TECHNOLOGY BRIEF: CA SITEMINDER

CA SiteMinder® Prepares You for What's Ahead

Table of Contents

Executive Summary

Challenge

Today's business environment requires the secure delivery of information and applications over the Web. Web Access Management (WAM) systems are central to this evolution. While WAM systems are not new, pressures around cost control, compliance, and growth — and emerging technologies such as Web Services, Federation, and user-centric identity — are causing organizations to rethink and often dramatically expand their WAM strategies.

Organizations must adopt new and more advanced authentication systems, implement risk-based security policies, and federate identities with other organizations to compete effectively in the Web-enabled world. At the same time a better user experience, simplified administration, and unprecedented reliability and scalability will be required as the Web solidifies its place at the center of application strategies.

Opportunity

CA SiteMinder® is the most widely deployed WAM solution available and can provide you with a proven security platform that both addresses your challenges with today's Web-enabled world and positions your organization for further change and expansion. CA SiteMinder delivers:

- Unparalleled platform support
- Advanced authentication and authorization capabilities
- Enterprise-class administration and management capabilities, including administrative scoping and multilevel delegation — an industry first
- A new extensible architecture that simplifies upgrades while providing a unified platform for enterprise policy management
- The best performing and most scalable WAM solution available

Benefits

CA SiteMinder can handle your secure Web-enablement challenges and enhance your enterprise identity and access management strategy. This WAM solution helps you:

- Create a seamless experience for users, including access to partner systems
- Reduce costs with delegated administration and simplified management
- Respond to business needs with the latest features, including strong authentication
- Move beyond retroactive audits and toward continuous compliance

CA SiteMinder addresses all of your security management concerns so you can stay focused on your important business challenges.

The Objectives of Web Access Management

WAM systems are the key to enabling business over the Web while limiting your security risk. A WAM system protects and controls access to your Web applications, records user and administrator activities, and is responsible for creating a seamless single sign-on experience for any user including employees, partners, and customers.

An effective WAM system must be a shared security service for applications throughout the enterprise. It's not enough to simply meet basic requirements — enterprise WAM deployments need to support complex single sign-on scenarios and non stop operations. They must be easy to administer, monitor, and manage. Deployment alternatives are necessary so that the system can be adapted to an organization's specific requirements. In addition, the system needs to be extensible and pervasive in terms of its platform coverage and capabilities.

What Does a WAM System Need to Do?

From a business perspective, the WAM system needs to help organizations respond to many important questions, including:

- Are our Web resources adequately protected?
- How can we provide a seamless experience for users given our disparate application environments?
- How should we authenticate users and can different approaches be used based on criteria we define?
- Is it easy to create and manage access policies and does the system offer us the flexibility we require?
- Can the system help us reduce security administration and related operational costs?
- Will a company acquisition force us to rethink our deployment strategies?
- Can we tie the system into our existing auditing processes?
- As our usage increases, will the system continue to be responsive and easy to manage?
- Can the system itself be compromised and how reliable is it?
- Can we offer a secure and simple means of authenticating users without requiring them to remember passwords?

These are challenging questions. It is important to understand your requirements and compare them to the capabilities of a WAM system to allow you to make the right decision before committing to a WAM solution and a deployment strategy.

CA SiteMinder

CA SiteMinder is a comprehensive security management solution that addresses these important questions. This paper discusses how the component architecture of CA SiteMinder enforces security policy, why it performs so well, and how companies have scaled CA SiteMinder deployments to support thousands of Web applications and tens of millions of users.

The key WAM functions that CA SiteMinder supports, including authentication, single sign-on, authorization, and auditing are also discussed. Also, since you might be facing some challenging issues as WAM deployments move to enterprise-scale, some of the advanced capabilities built in to CA SiteMinder will also be reviewed.

CA SiteMinder r12 introduced innovative administration features designed to engage a wider population in the creation, management, and auditing of security policies. Couple that with the fact that CA SiteMinder administrative tasks can now be assigned with an unprecedented level of control and you have an opportunity to deploy WAM capabilities faster and more broadly than ever before.

CA SiteMinder is certified with more than 450 specifically tested combinations of Web and application servers, ERP systems, directories, databases, and operating systems. Thus, it can support the breadth of platform combinations found in today's organizations.

In addition, more than 150 companies have joined the CA Partner Program to offer add-on capabilities and services to CA SiteMinder customers. And thousands of CA SiteMinder customers around the world share ideas and experiences through their interaction in user groups, forums, and trade shows.

The Basic Architecture of CA SiteMinder

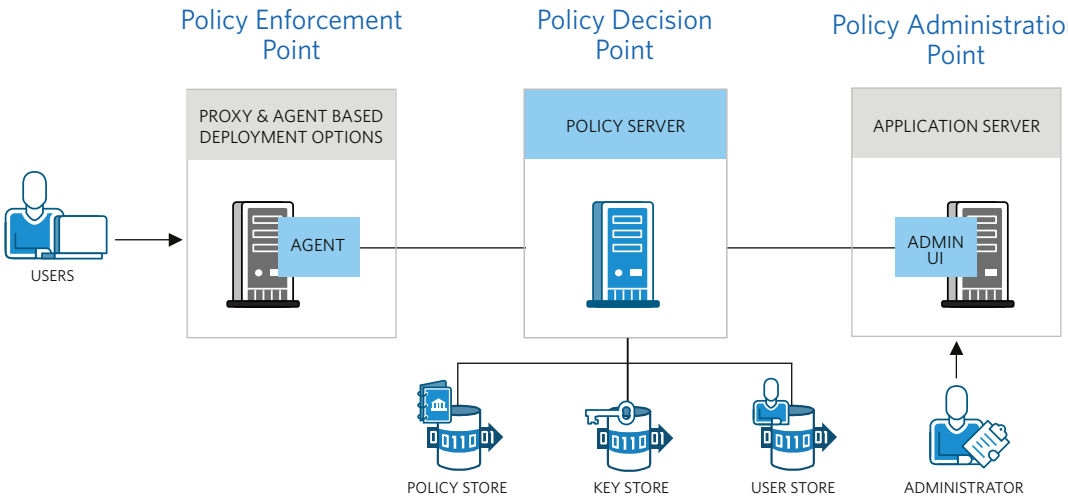
CA SiteMinder consists of two basic run-time components and an administration component.

FIGURE A

CA SiteMinder enforces security policies with agent-based and proxy-based PEPs to suit the requirements of each organization.

The CA SiteMinder Policy Server is a high performance and reliable PDP.

CA SITEMINDER REFERENCE ARCHITECTURE



A CA SITEMINDER AGENT acts as a *Policy Enforcement Point (PEP)* and also performs the services of authentication management and single sign-on. Agents can also support optional requirements such as securely passing user entitlements to protected business applications.

Agents come in several forms and each is tailored to the platform it protects. There are Agents for Web servers, J2EE servers, ERP systems, Proxy servers, and more. These options are described in more detail later.

A CA SITEMINDER POLICY SERVER acts as the *Policy Decision Point (PDP)*. The Policy Server authenticates users on behalf of the PEP, evaluates security policies, and makes authorization decisions that are communicated back to the PEP. The Policy Server also audits each of these events.

The Policy Server supports various providers and platforms for the user directory and for its policy and key stores. As Policy Servers are added for increased capacity and high availability, they connect to a common policy store to determine available infrastructure and the security policies they need to enforce. They also connect to a common key store to enable secure single sign-on.

THE CA SITEMINDER ADMINISTRATIVE UI serves as a secure *Policy Administration Point (PAP)*. One instance of the Administrative UI server can connect to and manage multiple Policy Servers.

Authentication

User authentication is the first step in securing Web applications, establishing a user identity, personalizing the user's experience, and determining what each individual can do. CA SiteMinder supports and manages the use of a broad range of authentication methods including passwords, tokens, X.509 certificates, smart cards, custom forms, and biometric devices. Authentication methods can also be combined for stronger authentication, for example, a certificate can be required in addition to a password.

Authentication methods can be designated a protection level, and minimum protection levels can be associated with applications to provide greater assurance of the user's identity where sensitive applications and information are exposed.

Risk-based capabilities allow for the context of the user's login request to be evaluated. For example, an HTML forms-based login over SSL originating from an unrecognized machine on the Internet represents a higher risk compared with the same forms-based login taking place over the company's virtual private network (VPN).

AVAILABLE AUTHENTICATION METHODS AND CAPABILITIES

- Basic Authentication
- Form-based User Id and Password
- X.509 Certificate (CRL and OCSP support)
- Integrated Windows Authentication (IWA, including Negotiate/Kerberos and NTLM)
- MIT Kerberos
- RSA SecurID Token Device
- Entrust IdentityGaurd
- One-time Passwords
- Smart Card
- Information Card / Microsoft CardSpace
- Arcot Webfort (software two factor system)
- Biometric Devices
- Third Party Integrations including: Tricipher and SafeWord
- Audited impersonation
- SSL to protect Basic and Form-based
- Combinations of methods (e.g. Forms and Certificate)
- Step-up based on Protection Levels
- Risk-based
- Knowledge-based
- Login Sequence Control
- Machine Address Verification
- Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)
- Security Assertion Markup Language (SAML)
- WS-Federation / Microsoft ADFS
- Custom methods created with the CA SiteMinder Authentication API

Directory Chaining

It is unrealistic and unnecessary to expect that all of the applications protected by a WAM system will be authenticating users to a single user directory. But today even a single application may need to authenticate users to two or more directories.

CA SiteMinder supports Directory Chaining, which means that a single security policy can support an application even when its user community is spread across multiple directories. This includes scenarios where the directories reside on dissimilar platforms such as an LDAP directory, Microsoft Active Directory, a mainframe, or a relational DBMS.

Password Services

Password Services encompasses a range of topics, including password policies, changing passwords, password expiration, password recovery, and account disablement. Password services are provided by some user directories and by some WAM systems.

CA SiteMinder provides a centralized approach to password services that supports LDAP directories, Microsoft Active Directory, and relational databases. This makes it easier to create common password policies that define rules and restrictions governing password expiration, composition, and usage and apply them across the enterprise.

When configured, CA SiteMinder invokes a password policy whenever a user attempts to access a protected resource. If the user's password has expired based on criteria defined in the password policy, the user's account can be disabled or the user can be forced to change the password.

Password policies can be associated with an entire user directory or a subset. Multiple password policies can be configured for the same user directory, in which case they are applied according to priorities that you can specify for them.

Impersonation

CA SiteMinder supports user impersonation, a feature whereby a privileged user can assume the identity of another user. This can be useful when a helpdesk or customer service representative needs to investigate application access problems for a particular user.

The impersonation support of CA SiteMinder is more secure than other approaches to these problems, such as sharing user credentials over the phone, which is a practice that is generally prohibited by company policy.

CA SiteMinder impersonation is a secure operation that allows only authorized users to impersonate other users. This is accomplished in the following ways:

- Security administrators set up impersonation rules in the security policy. This provides control over who can impersonate, who can be impersonated, and which resources can be accessed.
- Impersonation sessions are audited for record keeping and non-repudiation. Information from both the user who is impersonating and the user who is being impersonated is recorded.
- CA SiteMinder can set a secure header variable that the application can use to hide private information from the impersonating subject as necessary to protect the user's privacy.

Increasing Business Agility with Simplified Sign-on

BT is one of the world's leading providers of communications solutions and services and operates in 170 countries. With more than 8 million customers and 100,000 staff members and suppliers using Web-based applications everyday, the communications giant needs to ensure secure and efficient access to its online services.

Using CA SiteMinder, BT has been able to centralize the authentication and authorization of staff, suppliers and customers. This has enabled BT to rationalize 80 point security solutions, reduce the number of passwords needed by an employee, and support a throughput of over 40 million transactions a day.

Once an individual has gained access to a BT portal, they can easily move between different service and product areas, which is key for ensuring customer loyalty and satisfaction. With fewer passwords to remember and manage, BT staff members are also more productive every day.

Single Sign-On

Seamless Single Sign-On (SSO) across Web applications is one of the most visible features of a well-designed WAM system. Most WAM systems address basic SSO requirements through the use of an HTTP session cookie. But challenges emerge as the deployment scale grows or as the Information Technology (IT) infrastructure from different organizations is combined.

CA SiteMinder includes three additional SSO features to address these challenges: *Security Zones, Cookie Providers,* and *Identity Mapping*.

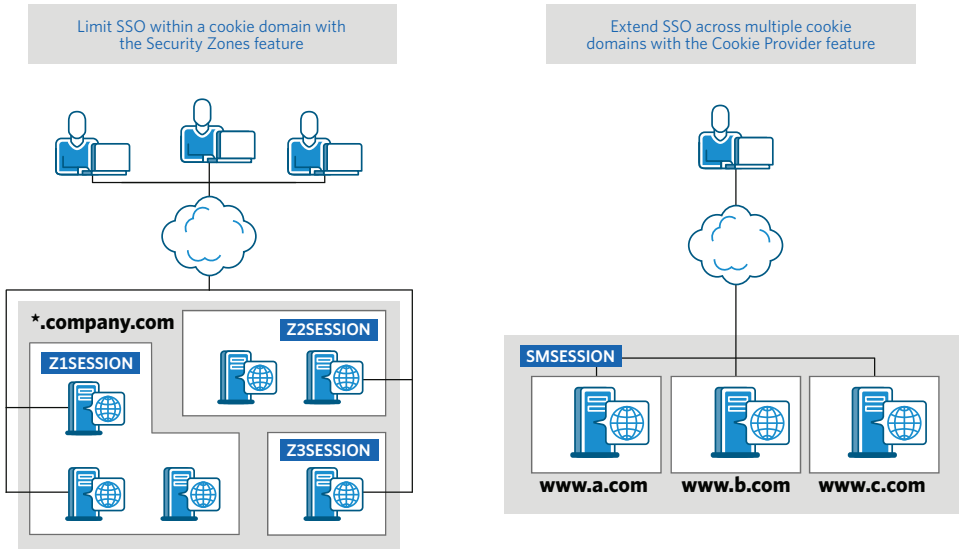
FIGURE B

CA SiteMinder includes three features that extend traditional Web SSO to enterprise scenarios.

Security Zones allows you to restrict SSO across applications within a single cookie domain. The *Cookie Provider* feature extends SSO across cookie domains.

Identity Mapping (not shown) extends SSO across independent CA SiteMinder deployments, a situation that could arise as the result of an acquisition.

ADVANCED SINGLE SIGN-ON SCENARIOS



Security Zones

SSO across applications within a common cookie domain can be restricted through the use of CA SiteMinder Security Zones. This allows a single cookie domain to be partitioned to allow for different security policies without a requirement to establish Domain Name System (DNS) subdomains.

Administrators first organize applications into groups (or zones) with similar SSO requirements. Then, CA SiteMinder generates a separate session cookie for each zone. End users benefit from SSO within each zone and administrators are able to enforce different security policies for applications in different zones.

Security Zones make it possible to have:

- Different session time-out settings for applications in each zone
- Different user directories for authentication in each zone
- Different authentication methods and protection levels in each zone

Cookie Provider

SSO can be extended across multiple DNS domains with the CA SiteMinder Cookie Provider feature. In this configuration, CA SiteMinder challenges the user to authenticate in the first DNS domain (company.com) but does not challenge the user when they navigate to subsequent domains (subsidiary.com).

The Cookie Provider feature is popular for cross-domain SSO where a single CA SiteMinder environment is protecting resources in each domain. The federation capabilities of CA SiteMinder provide a better solution when there are many different domains or when there is no CA SiteMinder infrastructure in the other environments.

Identity Mapping

CA SiteMinder Identity Mapping can be used to extend SSO across independent CA SiteMinder deployments. This might be useful when two organizations merge and each was previously running different CA SiteMinder systems (and different user directories) and it is not possible or desirable to merge the infrastructure.

Also known as auth-validate mapping, Identity Mapping makes it possible for a user to be authenticated to a user directory in one CA SiteMinder system and be mapped to the same user identity in a different authentication store on another CA SiteMinder system. The two systems need only share or synchronize their CA SiteMinder key stores. The federation capabilities of CA SiteMinder can also be used for this prupose.

Extending SSO to Non-Web Applications

CA Single Sign-On is a complementary product that can be used to extend SSO to non Web-based applications including those deployed on the desktop or on legacy systems.

Authorization

Organizations need flexible security policies that can be easily leveraged over multiple applications and services. They need to implement a single shared security service to simplify administration, ease compliance-related reporting, and reduce the security-related burden on application developers.

Without WAM, systems developers must implement security logic entirely inside their applications. This leads to compliance exposures and development challenges. For example, the required security development skills would depend on the type of Web server, operating system, and programming language used for the application.

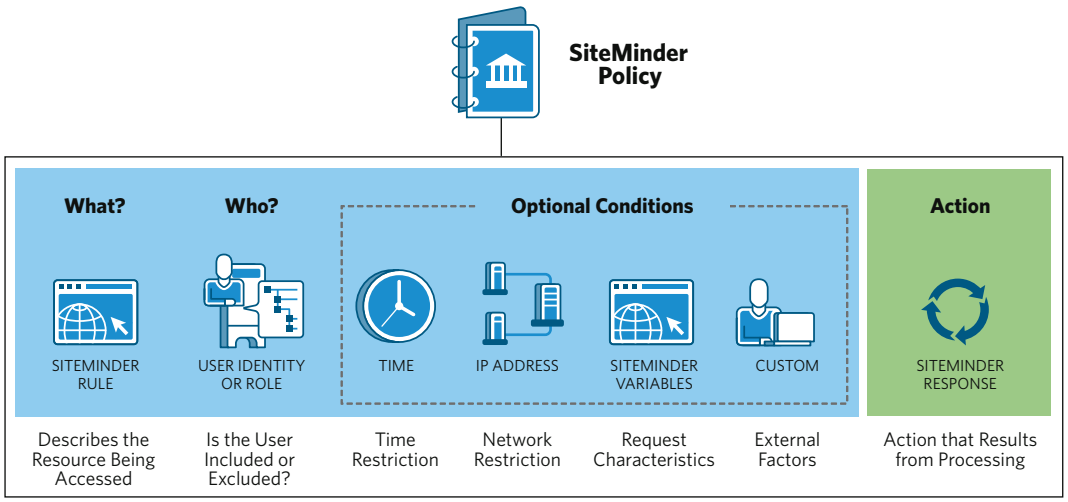
CA SiteMinder centralizes the management of user entitlements for customers, partners and employees across all web applications through a shared service. Centralized authorization greatly reduces development costs by allowing developers to focus on the application's business logic instead of programming security policies. In addition, CA SiteMinder provides the ability to enforce security policies across the enterprise, which eliminates the need for redundant user directories and application specific security logic.

FIGURE C

A CA SiteMinder policy consists of a number of components that associate users with resources and grant or deny access.

The policy can also trigger actions on various events, such as securely delivering user attribute or role data to the protected application.

CA SITEMINDER SECURITY POLICY COMPONENTS



CA SiteMinder Policies

CA SiteMinder policies are designed to accommodate the user and the user's relationship to the protected resource. A policy protects resources by explicitly allowing or denying user access. It specifies: the resources that are protected; the users, groups or roles that have access to these resources; the conditions under which this access should be granted; and the delivery method of those resources to authorized users. If a user is denied access to a resource, the policy can also determine how that user should be handled.

Policy components can be created within a policy domain and also globally, where they apply across all policy domains.

- Rules are a key component of the security policy because they grant or deny access to a specific resource or resources that are included within the policy. A rule describes the resource being protected, whether it is an entire application, a portion of an application, or a specific component of the application. Dynamic rules can also be defined to determine whether or not the resource being accessed should be covered by the access policy.

  Web resources can be restricted using regular expressions, and wildcards and query strings can be controlled as well. Rules can also be defined for an event, such as authentication success (or failure), session time-out, and access denial.

  Rules are associated with *Realms* or *Components* (which can be nested inside other Realms or Components). Components & Realms provide a convenient collecting point for Rules to define common policy requirements such as authentication levels and session time-outs.

- **User Identity or Role** connects authenticated users with the access policy. This association can be defined in many ways, including group membership, LDAP organizational structure and search filters, or as a SQL query to a relational database.

  In CA SiteMinder r12, access can also be determined via expression-based roles that provide greater flexibility and benefits, including a level of abstraction from the technology of the underlying user directory. For more information see the Enterprise Policy Management section under *Innovations Delivered in r12* in this paper.

- **Time** restrictions can be applied at the policy level and on the resource access rules themselves to provide greater flexibility as to when access should be allowed (or disallowed). For example, restrictions can be set to allow: *Mondays from 8-10 a.m. or Entire Weekend.*

- **IP Address** restrictions make it possible to constrain policies based on the network address associated with the client.

- **Variables** allow you to include business logic in policies by capturing a wide range of dynamic data that can be built into policy expressions. For example, a policy may depend on a piece of POST data submitted with the request or the user's credit rating, which is retrieved via a Web service call.

- **Custom** conditions can be evaluated using Active Policies to achieve even more fine-grained control over authorization. For example, a policy could deny access to an order entry page for customers with an overdue balance in an accounting database.

- **Responses** are configurable actions that result from the processing of a policy. Responses can deliver user profile data and entitlements to the application when access is granted. With this information, the application can present a personalized interface and determine which capabilities to offer the user. Responses can also be used to tailor what the user sees when access is denied or the user's session times out.

  Responses accomplish these things by securely setting HTTP session variables for the application, issuing redirects, setting HTTP cookies in the user's Web browser, and more.

  Active Responses allow custom code to retrieve or generate data for the application, or to trigger external actions as a result of a policy decision.

Authorization Mapping

CA SiteMinder supports Authorization Mapping, which allows administrators to relate users in an authenticaton directory to their corresponding identities in a different directory being used for authorization.

Potential uses of Authorization Mapping include:

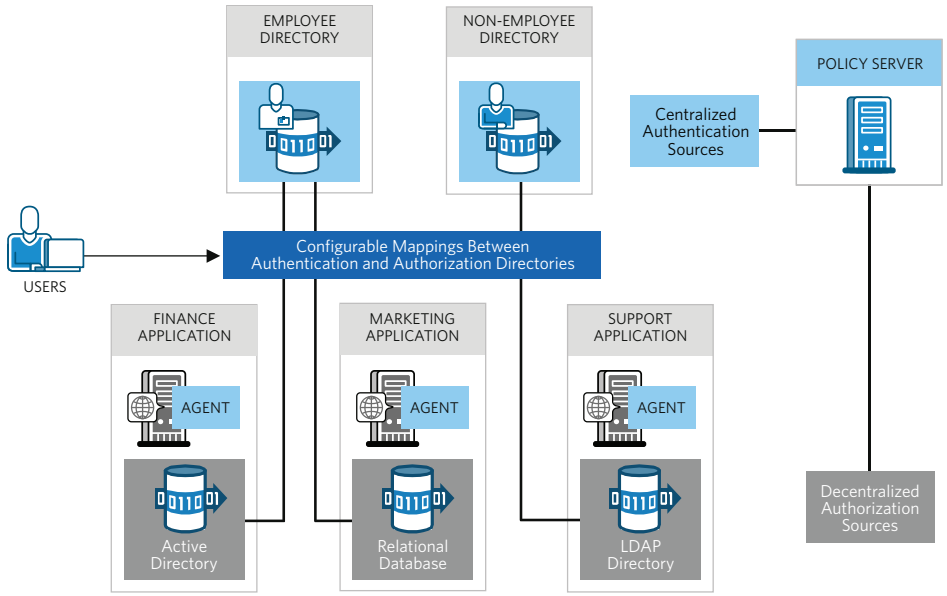
- Moving authentication from a legacy or stand-alone application to a centralized user directory. This makes it possible to introduce SSO and stronger authentication, even though authorization may need to remain located with the application.
- A way to enable CA SiteMinder Windows authentication to Microsoft Active Directory, while supporting authorizing to an alternate directory with a more flexible schema (e.g., Microsoft AD/AM), in order to leverage custom attributes such as roles and user entitlements.

The Administrative UI lets you choose how to map a user's identity between authentication and authorization stores, even when they are based on different technologies such as LDAP and relational database.

FIGURE D

CA SiteMinder provides an Authorization Mapping feature so organizations can leverage centralized authentication stores even when the authorization data remains distributed with the application.

AUTHORIZATION MAPPING HELPS ORGANIZATIONS DECOMISSION SECURITY SILOS



Directory Virtualization

Organizations often find themselves in a situation where they need to accommodate multiple user directories. This can happen for a variety of reasons including distributed development, lack of security standards, organizational politics, deployment of commercially available applications, and as the result of acquisitions or consolidations.

These directories may be used by different applications and a single application may use two or more directories. In some cases, user profile data may need to be combined from two directories in order to establish the required set of entitlement data needed by the application.

Virtual Directory Server (VDS) products have emerged to address these requirements. VDS products serve as an abstraction layer between supported user directories (which typically include LDAP directories, Active Directory, and relational databases) and the applications requiring their services. A VDS simplifies application configuration because to the application, for example, CA SiteMinder, there appears to be only a single user directory.

But these benefits come with additional cost including VDS software, deployment services, and hardware. A VDS product also represents a new layer of infrastructure, which requires new considerations related to capacity planning, failover, and management. These products also represent a new administration layer that requires thinking about how policy administration and runtime behavior should be managed and audited.

Directory Virtualization Capabilities

CA SiteMinder is not a VDS and there are many scenarios where VDS technology is appropriate. However, CA SiteMinder does offer some directory virtualization capabilities not found in other WAM systems. And because CA SiteMinder already offers a high performance nonstop environment with excellent administration and management characteristics, it may be advantageous to forgo the introduction of VDS technology in some cases.

CA SiteMinder provides a Directory Chaining feature, for example, that allows it to easily search two or more user directories in a configurable order to authenticate the user. CA SiteMinder r12 includes additional directory virtualization capabilities. Authenticated users can be authorized against more than one directory through Enterprise Policy Management (EPM) Roles. These roles are described in the Enterprise Policy Management section in this paper. EPM roles can be used to map an identity across authorization directories, in effect presenting a virtualized user directory from the perspective of policy administrators and audit reporting.

So while virtual directory server (VDS) technology has many benefits, it may not be practical or cost effective to bring in a VDS platform solely for the purpose of authenticating and authorizing users in two or more directories.

Auditing

Organizations must closely track how applications and data are used, and how the security system is helping to provide controls. System administrators need detailed system data to fine tune performance. Business managers need activity data to demonstrate compliance with security policies and regulations.

CA SiteMinder includes comprehensive auditing capabilities including:

- Auditing to relational database and flat files.
- Auditing of user, administrator, and system activity within CA SiteMinder and also in custom modules or command line utilities.
- Auditing of impersonation events, where a privileged user takes on the identity of another user (for example, a help desk professional helping a user with a secured application).
- Flexibility to configure the kinds of events that will be recorded (for example, failed authorization attempts only).
- Integration with event aggregation and correlation systems including CA Security Command Center. This enables policy-based event filtering and correlation with enterprise-wide network, system and application events.
- A powerful event API that allows you to write custom event handlers that can trigger activities in external applications. For example, a custom event handler can be written to trigger an email notification to be sent when a security policy is modified.

Flexible Deployment Options

CA SiteMinder includes several complementary deployment options. A number of agents (distributed PEPs) are available for popular Web servers, application servers, and enterprise resource planning (ERP) systems. A proxy-based alternative is also available where a centralized PEP model is desirable. Some of these deployment options are depicted in Figure E.

WEB SERVER AGENTS are implemented as plug-ins for Web servers. The agent intercepts all HTTP and HTTPS traffic coming into the Web server and provides comprehensive protection for Web server resources including HTML pages, scripts, CGI programs, and Active Server Pages.

Web Server Agents are also used to provide perimeter protection and single sign-on for business applications behind the Web server, including Java Server Pages running inside a servlet container.

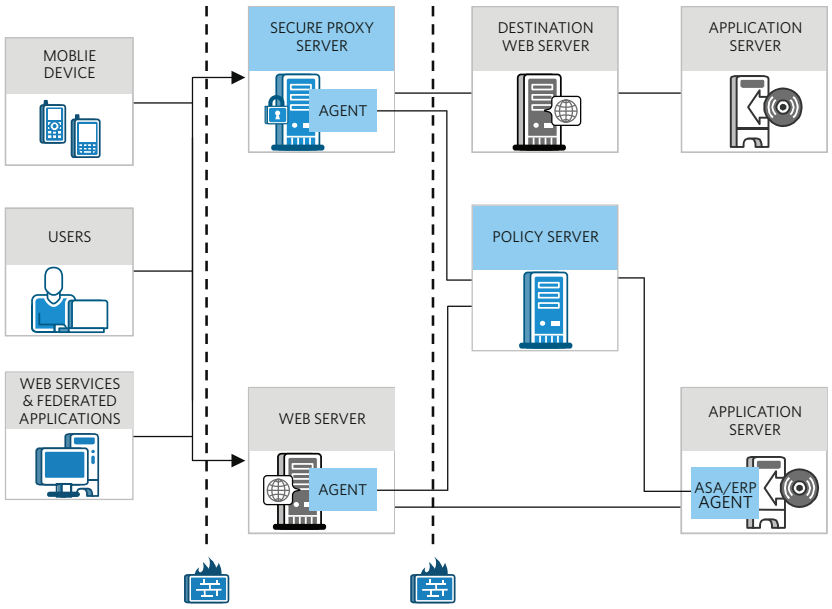
Web Server Agents are available for Microsoft Internet Information Server, Sun Java System Web Server, Apache, Red Hat Apache, IBM HTTP Server, Domino, Oracle HTTP Server, and HP Apache.

FIGURE E

CA SiteMinder supports two deployment strategies: a proxy-based PEP where application infrastructure cannot be disrupted and an Agent-based PEP where protection of local resources is a requirement.

The two approaches can also be used together.

DEPLOYMENT ALTERNATIVES MAXIMIZE FLEXIBILITY



CA SITEMINDER AGENT FOR SHAREPOINT® allows you to incorporate SharePoint into your SiteMinder single sign-on experience (including any SiteMinder supported authentication scheme). This results in a better user experience and the consistent enforcement of security policies and password rules. As SharePoint usage grows and you look to extend access to contractors, partners and customers, you can make it part of their SSO experience as well. The CA SiteMinder Agent for SharePoint can integrate with a variety of directories such as an LDAP directory, Microsoft Active Directory, a mainframe, or even a relational DBMS. All users

can then be administered from a central location which enables consistent access for internal, external and federated users.

APPLICATION SERVER AGENTS (ASA) are implemented as plug-ins for J2EE application servers. Typically an ASA is deployed in conjunction with a Web Agent, where the Web Agent provides perimeter protection and SSO, and the ASA enforces authorization policies.

The ASA also binds the CA SiteMinder and J2EE sessions together for a seamless and more secure experience for the user. ASA Agents are available for IBM WebSphere, Oracle WebLogic and RedHat JBoss EAP.

ENTERPRISE RESOURCE PLANNING (ERP) AGENTS are available to extend the single sign-on experience and policy-based protection to ERP systems including SAP, Oracle, PeopleSoft and Siebel.

SECURE PROXY SERVER (SPS) is a high performance reverse proxy gateway that provides out-of-the-box policy enforcement without access to the business application's Web platform. SPS is generally used to protect a number of different applications from a single centralized PEP.

SPS also offers:

- Mobile Device Support through specialized session schemes including mini-cookies, device ID, URL rewriting, SSL session ID, and custom solutions based on the Java Session Scheme API included with SPS.
- Credential Vaulting to provide single sign-on for legacy Web systems that cannot be remediated for sign-on integration.

An SPS deployment can be combined with Web Agents, which provide tighter control of local resources.

CUSTOM AGENTS can be built or embedded with the CA SiteMinder Agent API to secure many other types of applications (including non-Web applications). Using the Cookie API, custom agents can also create CA SiteMinder session cookies so these applications are able to participate in a CA SiteMinder-enabled SSO environment.

WEB SERVICES can be protected with CA SOA Security Manager, a complementary product which contains a specialized agent layered upon CA SiteMinder. CA SOA Security Manager provides identity-based Web services security and XML threat mitigation in a single integrated solution.

IDENTITY FEDERATION services are available to CA SiteMinder deployments using CA SiteMinder Federation Security Services, soon to be called CA Federation Manager. In a browser-based federation scenario, CA SiteMinder Federation Security Services enables users to securely traverse between a home site where they are initially authenticated (the Identity Provider), to an application on a target site (the Service provider). CA SiteMinder Federation Security Services enables CA SiteMinder deployed sites to be the Identity Provider, Service Provider, or both based on standards such as SAML 1.x/2.0 and WS-Federation.

NETWORK ACCESS SERVER (NAS) DEVICES such as proxy servers, firewalls, and corporate dial-up services can be supported by the authentication and security policy infrastructure of CA SiteMinder. NAS devices can use the Remote Authentication Dial-In User Service (RADIUS) protocol to exchange session authentication and configuration information with the Policy Server's built-in RADIUS service.

Extensible Policy Store

CA SiteMinder r12 is built on a new Extensible Policy Store (XPS) architecture that makes it possible for features and functionality to expand without requiring costly migration steps during an upgrade or the installation of additional products.

XPS employs a data dictionary-driven model to manage, validate, migrate, and secure objects allowing new object types to be introduced without requiring changes to the traditional Policy Store schema.

To illustrate the power of this feature, CA SiteMinder 6.0 SP5 customers can begin using the new Administrative UI without a requirement to upgrade the entire Policy Server infrastructure to r12. This allows organizations to take advantage of the new Enterprise Policy Management and advanced administration features built into CA SiteMinder r12 sooner and with less effort and less cost.

Administering Large Scale Deployments

CA SiteMinder r12 introduces a new administrative platform and a new administrative model, both designed to support secure application deployment on an enterprise scale.

The new Administrative UI can connect to multiple Policy Servers so you can manage all of your environments from a single shared administration server. The Administrative UI also integrates with a new security model that offers fine-grained control over assignment, scoping, and delegation of policy administration rights.

With these capabilities, security management teams can reduce administration costs, be more responsive to application owners, and continue to retain centralized control.

FINE-GRAINED PERMISSION ASSIGNMENT makes it possible to grant only those capabilities necessary for each individual to do their job. For example, this means that:

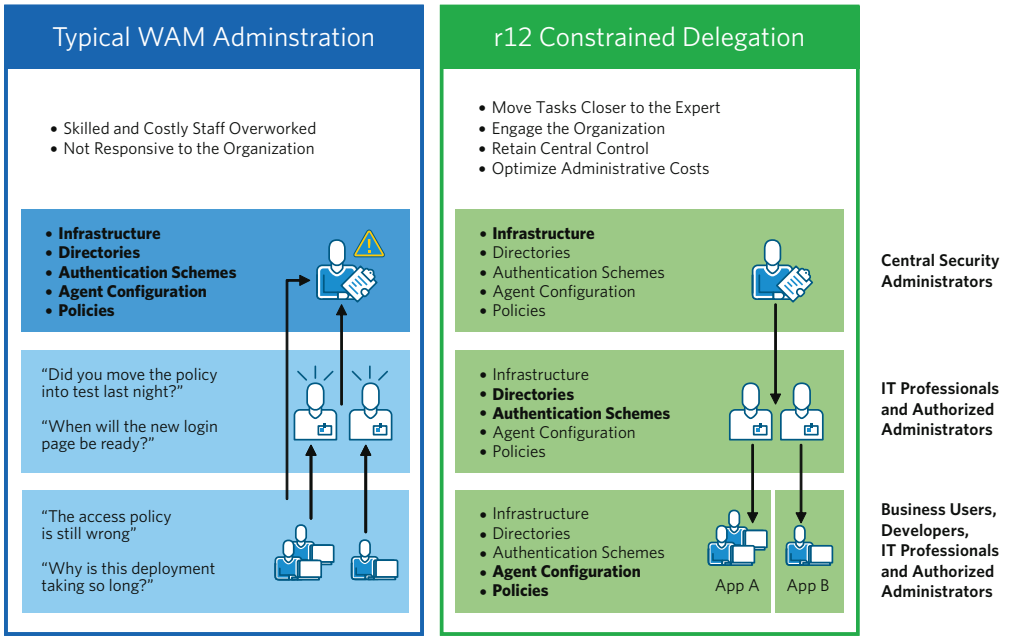
- An auditor can be granted view-only access to CA SiteMinder policy definitions.
- An administrator can assign view privileges for Agent settings to a team and manage privileges (create, update, delete) only to a trusted member of that team.
- Operations personnel can deploy and configure new Agents or user directories, without having access to application security policies.
- A service account can be defined for the purpose of moving policy objects from development to test. This account can be granted import privileges but denied access to the Administrative UI, in support of compliance policies.

There are over 30 administration categories that can be assigned. Each category can be granted with the necessary combination of view, manage, propagate, and execute (applies only to reports) permissions.

FIGURE F

The CA SiteMinder Administrative UI supports fine-grained permission assignment, multilevel delegation, and privilege scoping. This enables organizations to simultaneously distribute administrative authority, while retaining centralized management over the entire process.

CONSTRAINED DELEGATION SUPPORTS ENTERPRISE WAM DEPLOYMENT



Access methods can be granted or denied to specific individuals, including whether access to the Administrative UI, local API, remote API, or report server is allowed. Access can also be restricted to import, export, agent registration, and to specific command line tools.

Command line tools now respect operating system authentication, in addition to administrator ID and password, which means that credentials are not required in customized scripts built by customers to automate administration tasks.

CONSTRAINED DELEGATION is integral to the new security model and addresses transferability of administrative responsibilities — a key requirement in enterprise WAM deployments. In the Administrative UI, an administrator can decide if the individual assigned a given privilege can themselves further delegate that privilege to others. This special permission is referred to as Propagate in the Administrative UI.

Support for delegation, and the ability to control who can delegate which privileges is critical to the success of a large-scale enterprise WAM system. Multilevel delegation makes it possible for each organization to decide how to manage their responsibilities. Because the propagation

privilege can be granted to specific individuals for specific privileges and scope, organizations have the flexibility to distribute administrative authority, while retaining centralized management over the entire process.

ADMINISTRATIVE SCOPING allows the administrator to grant privileges for some — but not all — of the objects those privileges apply to. With scoping, an administrator can:

- Grant specific individuals or teams management permission to manage security policies for finance applications but not for other applications.
- Grant an auditor view access to all security policies, except for one associated with a confidential project.

Enterprise Policy Management

CA SiteMinder r12 introduces Enterprise Policy Management (EPM), a new access management model that enables business users to create security policies using terms they understand.

EPM APPLICATIONS combine all of the elements of a security domain into a simple concept that is easy to understand and manage. Protecting a business application is as easy as:

- Describing the resources to be protected. This may include a URL for a Web application or a component for a J2EE application.
- Describing the users who have access by creating EPM Roles.
- Creating the security policy by associating the roles and resources.

You also have the option to add responses to the policy, which may include sending entitlements to the business application or redirecting the user to another page.

Additionally, application administration can be delegated to the individuals best suited to this task. This may include application developers, business owners, or members of the administration staff.

Administrators can also scope which applications, and which aspects of applications, an individual can manage. For example, one team can manage financial applications, while another team can manage roles for intranet applications.

EPM ROLES let you describe which users will have access to the application based on your business requirements, rather than being driven by the technical implementation of a particular user directory. This is possible because a user's participation in a role is described to CA SiteMinder as an expression that provides an abstraction from the specific characteristics of the underlying user directory.

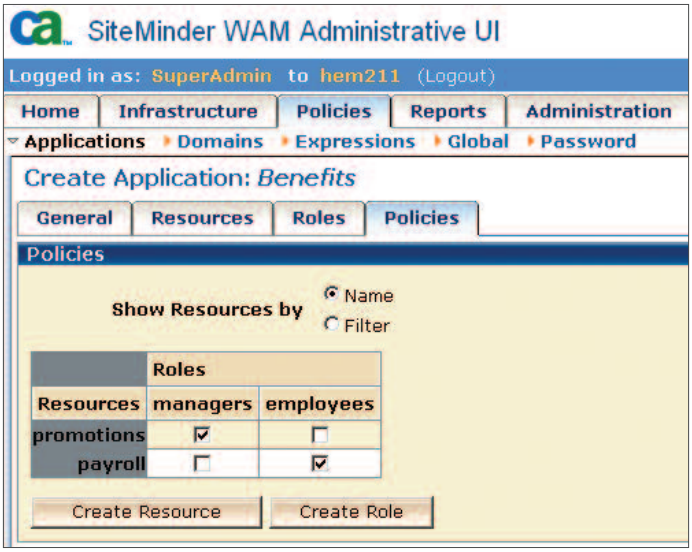
Expressions are defined in the Administrative UI and attach business meaning to directory-specific concepts such as group membership, user profile attributes, and SQL query syntax. Administrators can then name these expressions so that others can use them to build roles.

FIGURE G

In order to expand WAM to the enterprise, organizations need an easier way to build and manage security policies.

EPM includes an innovative and easy-to-use approach to define security policies. This enables organizations to fully exploit the built-in delegation capabilities of CA SiteMinder.

AN EASIER WAY TO DEFINE SECURITY POLICIES



This abstraction between directory-specific features and application security policy enables organizations to fully leverage the benefits of multilevel delegation. Those who understand the directory's organization and schema can define expressions. Others who understand the application's access requirements, but are not familiar with the underlying directory implementation, can use these named expressions to create roles.

This expression-based approach also allows roles to span user directories, essentially virtualizing directory infrastructure from the standpoint of authorization. The capability includes support for spanning directories on dissimilar platforms such as LDAP and RDBMS. This may be useful in cases where an organization is incorporating new directories obtained through acquisitions or transitioning to a new directory platform.

EPM IS A LAYERED FEATURE built on top of traditional CA SiteMinder policy components. This enables EPM to deliver a new delegation-friendly administrative model, while preserving the performance characteristics of the core policy engine.

Administrators familiar with traditional CA SiteMinder policy components can continue to secure applications with this approach, and both the EPM and traditional approaches can be used within the same deployment.

CA Report Server

CA SiteMinder r12 is integrated with CA's new enterprise reporting platform, CA Report Server. CA Report Server is a robust enterprise-class reporting system that is built on top of Business Objects XI R2.

CA Report Server is used with CA SiteMinder in two ways:

- Audit reporting, via ODBC to the standard audit store in CA SiteMinder
- Policy analysis reporting, via a direct connection to the Policy Server.

As with other products in the CA Identity & Access Management (IAM) suite, CA Report Server is included with CA SiteMinder as an optionally deployed shared component.

Performance

There are a number of features built in to the CA SiteMinder architecture that contribute to its industry-leading performance characteristics.

WEB AGENTS filter Web requests and support a number of functions including authentication, authorization, single sign-on, and application personalization. Because agents are deployed between the users and the business applications, agent processing must be extremely efficient and reliable.

- Auto Authorization is a configurable feature that enables agents to bypass policy evaluation based on file extensions or URI matching. This feature is commonly used to exclude content such as images and style sheets that may not be governed by an organization's security policy.
- Caching improves throughput by avoiding unnecessary calls to the Policy Server
  - The *Agent Resource Cache* tracks whether or not a particular resource is protected.
  - The *Agent Response Cache* improves performance when entitlement data is being passed to the business application.
  - The *Agent Session Cache* tracks user session state and the resources each user session has been authorized for.

  A *least recently used* algorithm and settings to govern cache size favor active user sessions and make efficient use of system resources, even in multimillion user deployments.

  Agents regularly poll Policy Servers for changes that might invalidate cache entries. This polling behavior is configurable and enables organizations to balance performance and policy consistency. Cached data can also be purged for specific users, realms, and agents through the Administrative UI.

POLICY SERVER is a highly-optimized, multithreaded policy decision engine that runs four key service functions: authentication, authorization, administration and auditing. These optimizations are supported by additional features to improve performance:

- A highly efficient threading model matched with a uniquely configurable thread pool allows the dispatcher to take maximum advantage of multiprocessor hardware including 4-way, 6-way, 8-way and 16-way symmetric multiprocessor systems.
- Caching is used in many areas:
  - An *Object Store Cache* maintains entries retrieved from the policy store and is preloaded to improve performance.
  - A *Two-level Memory Cache* links resources to their associated policy objects and can be sized to optimize performance.
  - The *User Authorization Cache* allows the Policy Server to quickly evaluate which policy belongs to which user and can be sized to optimize performance.
  - The *Expression Cache* holds precompiled expressions.
  - The *User Sub-expression Cache* eliminates common sub-expression evaluation where the same expression clause is used more than once for the same user, even if not in the same master expression.
- Connection pooling is used for policy store and user directory access to make efficient use of system and network resources.
- High Performance Auditing capabilities optimize performance:
  - Optional *Asynchronous Auditing* improves throughput by separating decisions related to authentication and authorization from the task of recording the decision.
  - Control over which types of events are audited, for example, all events versus rejection events, and whether or not to audit Web Agent cache hit events.
  - Availability of file-based and RDBMS-based auditing, including a high-performance bulk update SQL transaction design.

Proven Scalability and Availability

High-performance alone is not enough to support large-scale enterprise and global WAM. These systems require horizontal and vertical scaling, efficient use of resources, and a fault-tolerant architecture. CA SiteMinder includes a number of built-in features designed to complement its high performance architecture and support global scale deployments.

WEB AGENT CLUSTERING is supported through the use of popular third-party load balancers in order to establish the desired capacity and fault-tolerance at the Web tier. The session model in CA SiteMinder does not impose special configuration requirements on the load balancer. Users can flow seamlessly from one Web agent to another as dictated by the load balancer.

POLICY SERVER CLUSTERING is key requirement of a scalable WAM system and is built-in to CA SiteMinder. With Policy Server clusters, administrators can organize processing capacity by application, geography, or service level.

In a cluster, each Policy Server connects to the same logical, replicated, Policy Store so that it has a common view of infrastructure and policy information. Cluster capacity scales linearly

with the addition of new Policy Servers because there is no replication taking place between Policy Servers, except in the policy store itself.

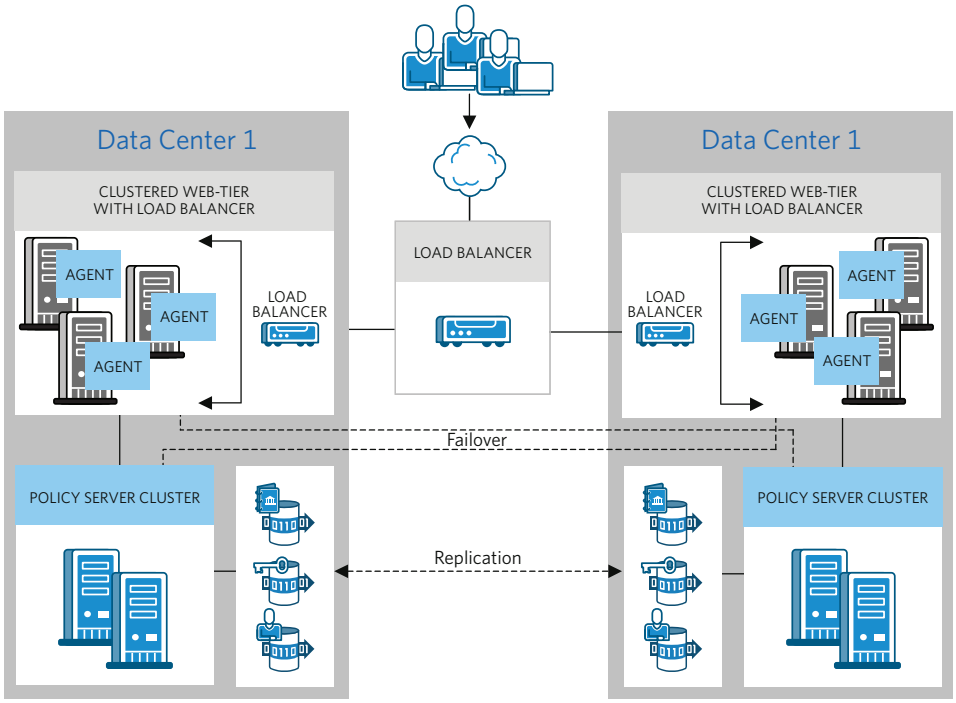
Clustering is desirable because:

- Agent connections are made based on real-time response data from each Policy Server. Less busy or higher capacity Policy Servers are automatically assigned a larger proportion of the load. This ensures efficient use of system resources, without intervention or monitoring.
- Agents can failover from one Policy Server cluster to another based on configurable criteria.
- Software maintenance is simplified because servers can be more easily taken down, upgraded, and brought back online without service interruption.
- Capacity can also be expanded without additional administrative requirements such as updating Agents with information about the new server.

FIGURE H

It's important that your business critical Web applications are secured with a scalable and fault-tolerant system. CA SiteMinder includes built-in support for clustering and cluster failover — building blocks for global deployment of Web applications.

LARGE SCALE DEPLOYMENTS REQUIRE SPECIALIZED FEATURES



FAILOVER AND LOAD BALANCING FOR BACKEND SYSTEMS is also critical to the 24 hours per day, 7 days a week operation of a large-scale WAM deployment. There are a number of CA SiteMinder features, best practices, and third-party capabilities that are used to ensure operational continuity during failure of a user directory, policy store, key store or session store.

- Failover is provided for the Key Store and Policy Store so that maintenance can be performed on these databases or LDAP servers without requiring a scheduled outage of CA SiteMinder and the applications for which it manages access.

- Replication of Key Store and Policy Store data across data centers is accomplished with third-party replication systems or by the underlying store technology itself (for example, Oracle RAC).
- User directory failover and load balancing is supported through settings in the Administrative UI.

Secure Platform

Layers of security, advanced features and strong encryption technology make it easy to operate CA SiteMinder in a highly secure manner.

ADVANCED ENCRYPTION STANDARD (AES) is an option in CA SiteMinder r12 and when selected is used throughout the system. This encryption covers session cookies, agent communications, and sensitive data in policy export files.

The r12 AES implementation uses a number of high-security options, including:

- AES OFB (Output Feedback) with HMAC-SHA256 to establish encrypted pipes between Agents and Policy Servers.
- AES CBC (Cipher Block Chaining) mode with 228-truncated HMAC-SHA256 for cookie encryption.
- AESKW (AES Key Wrap) for key storage, key transport, and secure data export.

The AES implementation of CA SiteMinder r12 supports the FIPS 140-2 standard and provides any organization with a very secure WAM platform.

AGENT REGISTRATION ensures that new agent installations are authorized and gathers the information necessary to establish a cryptographic trust relationship between the CA SiteMinder Agent and Policy Server. This mutual authentication process between components ensures that agent registration and initialization cannot be compromised.

Multiple Web servers on a single host can share a single trust registration, but separate trust registrations can also be established for greater control. The shared secret, which this trust is bound to, can be changed at any time through the Administrative UI. There is also an option for CA SiteMinder to automatically change the shared secret periodically.

- Dynamic Key Rollover is a built-in feature designed to increase the security of CA SiteMinder session cookies by rotating the symmetric key used for encryption and decryption. The feature is designed to work in large deployments and includes grace periods to compensate for the latency associated with processing key update requests across thousands of agents.

- Secure Attribute Passing is supported with CA SiteMinder responses. When responses are configured and triggered by a policy, the Policy Server retrieves one or more attributes (a group or role identifier, a user profile attribute, a credential, etc.) and sends them back to the Web Agent via an encrypted tunnel. Web Agents then inject the retrieved information into the user's Web request as a series of named HTTP headers. Other agent types present responses using mechanisms appropriate to their type.

  These headers are added to the user's HTTP request by Web Agent and are therefore not seen by the user or an observer in the DMZ. Additionally, these headers supersede forged headers that might be sent up from the client to attempt to break into an application.
- Cache Control enables administrators to selectively purge the Agent authorization cache to ensure that a user's session is no longer valid even if they do not logoff.

Vulnerability Testing

Additionally, CA SiteMinder has undergone third-party vulnerability analysis that includes source code review and penetration testing based on over 96 categories of vulnerability patterns.

These tests include whether Web browser client inputs are properly handled, whether sensitive data is properly protected, and whether authentication, authorization, and session management functions are properly performed. To obtain a copy of the report, please contact your CA representative.

Enterprise-Class Management Capabilities

Operating Web-enabled applications on a large scale also requires specialized tools and management infrastructure. CA SiteMinder includes tools for policy lifecycle management, monitoring, tuning, and debugging. CA SiteMinder also offers flexibility in terms of centralized agent configuration, local agent configuration, and combinations of both approaches.

POLICY LIFECYCLE MANAGEMENT tools are included to move security policy and infrastructure objects across development, test, and production environments. These tools have been updated in r12 to include:

- A standards-based XML format for exported data.
- Encryption of sensitive data in export files.
- Settings to govern import behavior including add, replace, and overlay options.

A COMMAND LINE INTERFACE is available to leverage the power of Perl scripting to dynamically control the CA SiteMinder system.

ONEVIEW MONITOR is a centralized monitoring tool included with CA SiteMinder that provides information about resource usage in order to help identify performance bottlenecks. OneView Monitor collects operational data from both Agents and Policy Servers and can display alerts when certain events occur, such as component failure.

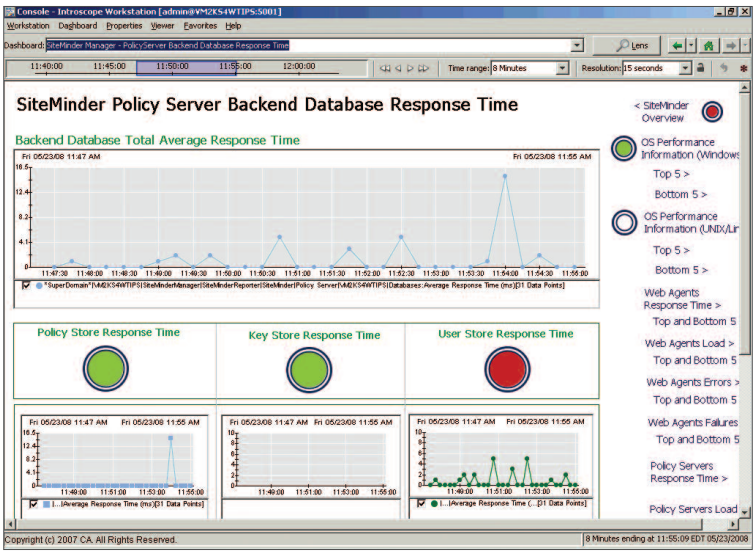
CA WILY MANAGER FOR CA SITEMINDER is a complementary product that provides support teams with an early warning system, enabling them to quickly detect, triage, and diagnose issues affecting CA SiteMinder operation before end users are impacted. CA Wily Manager for CA SiteMinder gathers evidence that can be used to pinpoint problems that may at first appear to be caused by CA SiteMinder but may actually related to the user directory platform, network, or Web server.

FIGURE I

CA Wily Manager for CA SiteMinder monitors your WAM system 24 hours a day, 7 days a week to proactively detect problems and enable quick analysis when performance issues arise.

History is preserved and the event window can be easily shifted to focus on specific time periods.

REAL-TIME PERFORMANCE MONITORING WITH BUILT-IN HISTORY



By aggregating data from all Policy Servers and agents, CA Wily Manager for CA SiteMinder allows IT teams to monitor comprehensive, real-time performance metrics from CA SiteMinder, including average response time for login; successes, failures, and errors per measurement period; and socket availability for CA SiteMinder processes.

CA Wily Manager for CA SiteMinder automatically identifies problematic transactions and displays those transactions with correlated metrics from the CA SiteMinder environment to speed problem resolution.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) SUPPORT enables monitoring from SNMP management applications such as CA Unicenter® and HP OpenView. CA SiteMinder includes an SNMPv2-compliant Management Information Base (MIB), an SNMP Agent, and an Event SNMP Trap library. The SNMP Agent enables monitoring applications to retrieve operational data from CA SiteMinder OneView Monitor. The SNMP Agent sends data to the SNMP manager and supports SNMP request handling.

FLEXIBLE ALTERNATIVES FOR AGENT CONFIGURATION AND MONITORING are available so customers can choose whether to manage agent configuration centrally with the Administrative UI, locally via a configuration file on the agent platform, or with a combination of the two approaches.

The CA SiteMinder central agent management model is generally preferred because it simplifies administration of large deployments. As new Web servers are added to meet demand, new Web agents can be deployed with a minimum of administrative effort.

Sometimes it is also desirable to allow operations personnel or developers to control some of the Web agent's settings such as where to write trace files or which URL characters to block on incoming requests. These settings can be modified via the Administrative UI; CA SiteMinder also allows these settings to be defined in a local configuration file on the Web tier. Control over which options are available is managed by an administrator in the Administrative UI on a per agent basis.

ADVANCED LOGGING AND TRACING capabilities are built in to troubleshoot configuration and runtime problems. Key features include:

- Run-time profiling let's you limit tracing to specific processing components and data elements. You can also specify filters to further refine trace output. Profile changes are loaded dynamically, which means you don't need to restart the Policy Server to alter the data being logged.
- Transaction correlation lets you track events on both the Agent and Policy Server through an auto-generated and unique transaction ID that is common to each event.
- Available settings let you control log file retention and rollover behavior, including rollover based on file size or time of day
- Control over log format including XML, delimited, and fixed width.

With these features, it is much easier to troubleshoot problems on busy servers.

A TEST TOOL is available to simulate the interaction between Agents and Policy Servers. Policy administrators can use this tool to quickly test policy evaluation and to help troubleshoot policy design problems.

THE POLICY SERVER PUBLISH COMMAND can be used to capture a snapshot of a CA SiteMinder runtime environment, including information about Policy Server configuration, connected Agents, user and policy stores, and custom modules in use. Should it be required, the information collected enables CA Support engineers to more quickly reproduce and resolve critical production problems.

Software Development Kit (SDK)

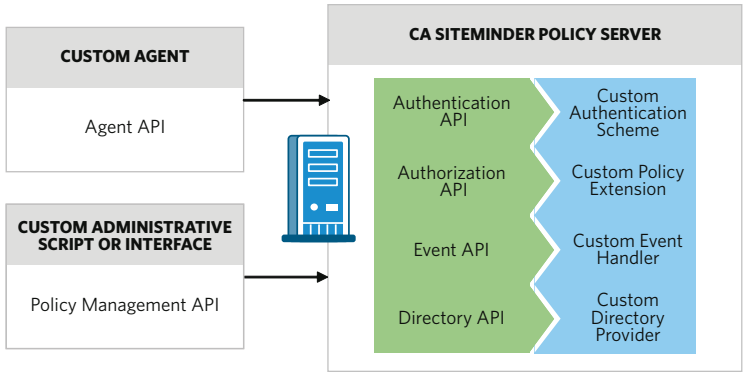
The CA SiteMinder SDK includes a set of documented application programming interfaces (APIs) that let you integrate and extend the capabilities of CA SiteMinder within your specific environment.

THE POLICY MANAGEMENT API is used to manipulate objects in the CA SiteMinder Policy Store. Using the Policy Management API, you can develop a custom administrative interface for managing policy and infrastructure objects, including movement of policies across environments and bulk load of policy objects. Both programming and command line interfaces (CLI) are available.

FIGURE J

Programming APIs are available in C, Java, and Perl to develop custom integrations with CA SiteMinder.

AVAILABLE APPLICATION PROGRAMMING INTERFACES



THE AGENT API is used to build custom agents that enforce access control and manage user sessions. Enforcing access control consists of authentication, authorization, and auditing. Additional services provided by the Agent API include:

- Session management, including the ability to store and retrieve variables.
- Load balancing, failover, and encryption for Policy Server communications.
- Detection of configuration changes, cache flushes, and key rollover events.
- Ability to execute custom code on the Policy Server via a secure channel. This is useful for integrating legacy systems with the policy evaluation process and as a secure way of communicating through a firewall.

Custom agents can participate in a single sign-on environment with standard CA SiteMinder Web agents using a set of cookie APIs. These interfaces can be used to create third-party SiteMinder session cookies that can be optionally accepted by CA SiteMinder Web agents.

THE AUTHENTICATION API is used to develop plug-in modules that define new authentication schemes or customize out-of-the-box authentication schemes. Modules developed using this API are implemented as shared libraries and can be configured using the Administrative UI. Custom authentication schemes can assist with user disambiguation as well as with authentication.

THE AUTHORIZATION API is used to develop plug-in modules that perform custom authorization functions. The modules can be configured using the Administrative UI to define active rules, active policies, and active responses.

Active rules and policies are custom code that modify or enhance the basic rules and policy functions of CA SiteMinder. Active Responses allow custom code to retrieve or generate data for the business application or trigger external actions as a result of a policy decision.

THE DIRECTORY API is used to develop a directory provider for a custom user directory.

THE EVENT API is used to build a custom handler that can log events using outside sources, providers, or applications. For example, a developer could build an event handler that sends an email to the administrator when the accounting server starts or when someone creates a new security policy.

CA SiteMinder Partner Programs

CA provides a comprehensive set of programs that enable the partner community to develop, market, deliver, and implement CA SiteMinder-based solutions and services for our customers. CA's extensive partner community covers a broad range of models including systems integrators, consulting service providers, resellers and technology partners.

Global Systems Integrators

CA has formed strategic alliances with a number of the world's leading Global System Integrators (GSI). These alliances enhance CA SiteMinder with the GSI's industry-recognized consulting services and thought leadership to deliver exceptional value to CA's customers. CA's GSI partners include Accenture, BearingPoint, Cap Gemini, Deloitte, Infosys, PwC and Satyam, TCS and Wipro.

Independent Software Vendors

CA also encourages technology partnerships related to CA SiteMinder. Independent Software Vendors (ISVs) provide applications that are either built on or integrate with CA SiteMinder to extend the value for our customers. The robust SDK and mature APIs in CA SiteMinder have enabled hundreds of partners to address our mutual customer's needs with integrated and industry-leading solutions.

CA works closely with its CA SiteMinder partners to address the unique needs and requirements of the CA SiteMinder community.

For more information, please visit http://www.ca.com/partners

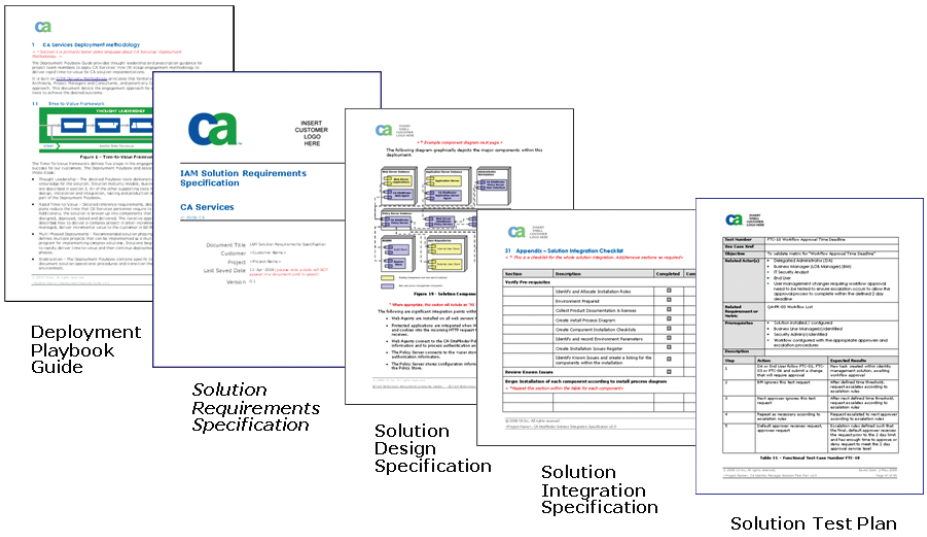
CA Services

There is no replacement for knowledgeable security experts and a detailed design when it comes to ensuring the efficient and secure deployment of an enterprise WAM system.

FIGURE K

The CA SiteMinder Rapid Implementation Service provides WAM experts that work with you to develop a plan to get you operational quickly by focusing on an initial, bounded deployment.

LEVERAGE THE EXPERIENCE OF EXPERTS



CA SITEMINDER RAPID IMPLEMENTATION SERVICE provides WAM experts to work with you to develop a plan to get you operational quickly by focusing on an initial, bounded deployment. The plans are built to extend and enhance your existing capabilities in Web access administration, application integration, user or system authentication, and user password policy management.

Once the design and specification is validated, CA SiteMinder experts install, configure, integrate, test and document the workflows, features and functions defined in the detailed design.

The CA SiteMinder Rapid Implementation service provides the following benefits:

- Accelerates time-to-value with a bounded deployment.
- Reduces the risk of deployment mistakes with WAM infrastructure.
- Delivers achievable, custom-built implementation and test plans.
- Improves efficiency through application of best practices methodologies.
- Matching CA SiteMinder features and functions to your business and security requirements and goals.
- Speeds deployment and staff learning curves.

CA Global Solution Engineering

CA Global Solutions Engineering (GSE) is a team within CA Services whose mission is to help achieve faster time-to-value for CA product implementations by providing centralized delivery of high-quality, supportable and cost-effective accelerators and components.

GSE components are:

- High Quality GSE uses consistent methodologies and testing standards to produce each component. Our components are well-documented and easy to integrate into a CA environment.
- Supportable All work is supported by GSE, either on a time and materials basis or as part of a support contract.
- Cost Effective GSE uses a blended onshore/offshore delivery model that combines the business and technical skills of our architects with the development, testing, and documentation offerings of our offshore development teams.
- Partner-Leveraged To meet the customers' specific needs, GSE leverages relationships with key partners to provide additional capacity and expertise.

GSE provides a comprehensive catalog of pre-built accelerators and components which are available to enhance and extend SiteMinder and other products in CA's Identity and Access Management suite.

GSE develops integrated solutions for SiteMinder using the SiteMinder Software Development Kit (SDK) supplied with these products. GSE works with CA Services, CA product engineering, and CA product management to develop solutions for customers that are high-value and consistent with CA product direction.

Platform Support

CA's certification team is dedicated to porting and testing CA SiteMinder with the latest hardware and software according to the priorities of our customers. SiteMinder is currently certified with more than 450 specifically tested combinations of Web and application servers, ERP systems, directories, databases, and operating systems.

POLICY SERVER & WEB AGENT OPERATING SYSTEMS	AGENT PLATFORMS	USER DIRECTORIES
• Microsoft Windows • Sun Solaris • Red Hat Enterprise Linux • SUSE Linux • HP-UX • IBM AIX • IBM Z/OS **Other Standards** • SAML 1.x/2.0 • WS-Security • WS-Federation • SNMP • IPv6 • AES • FIPS 140-2 • RADIUS • Common Criteria (evaluated)	**Web/Application Servers** • Apache HTTP Server • Apache Tomcat • Oracle WebLogic • HP Apache • RedHat JBoss EAP • IBM HTTP Server • IBM WebSphere • Lotus Domino • Microsoft IIS • Microsoft SharePoint • Oracle HTTP Server • Red Hat Apache • Sun Java System **ERP Systems** • Oracle • PeopleSoft • SAP • Siebel	• CA Directory • Critical Path Directory Server • IBM DB2 • IBM Directory Server • Lotus Domino LDAP • Microsoft Active Directory • Microsoft AD/AM • Microsoft SQL Server • MySQL • Novell eDirectory • Oracle Internet Directory • Oracle RDBMS • Oracle RAC • Open LDAP • OpenWave • Radiant One Virtual Directory Server • Red Hat Directory Server • Siemens DirX • Sun Java System Directory Server • SunOne Directory Server

For the latest certification information, refer to the CA SiteMinder Platform Support Matrix and Certification Roadmap documentation found on the CA support site.

SECTION 5: **CONCLUSIONS**

WAM systems perform a vital role in today's business environment by securing the delivery of information and applications over the Web. At first glance, there may appear to be a number of WAM solutions available with similar features and capabilities. However, a closer look reveals why CA SiteMinder remains the gold standard for WAM systems worldwide.

CA SiteMinder has the best performing and most scalable architecture available today to secure all of your Web applications, even those destined for global scale deployment and tens of millions of users. Advanced authentication and single sign-on features, flexible deployment and auditing options, and broad platform support make it possible to optimize a CA SiteMinder deployment to your organization's specific requirements.

CA SiteMinder r12 introduces a new Enterprise Policy Management model and the industry's most advanced administration capabilities. This makes is possible to engage a broader set of individuals in the process of securing your Web applications, freeing up security experts and compressing project schedules. The r12 release is also based on a new extensible architecture that can coexist with the previous r6 release, while enabling CA to deliver important new features even faster and without the migration hassles typically associated with software upgrades

Finally, CA's Identity and Access Management suite includes complementary products that when used with CA SiteMinder can extend your benefits. These products address the issues of federated identity and SOA/Web Services management, legacy system single sign-on, security compliance management, and identity lifecycle management.

CA SiteMinder addresses today's WAM challenges and prepares you for the ever-changing and growing capabilities that lie ahead on the Web.

To learn more about CA SiteMinder, a key component of CA's Security Management portfolio, visit **ca.com/security**.

CA (NSD: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

1683_0310

Learn more about how CA can help you transform your business at **ca.com**