Integrating SAP Applications into your SSO Environment

Netegrity White Paper

Published: January, 2002

Table of Contents

INTRODUCTION

Note: This paper assumes a working knowledge of Netegrity SiteMinder. For an introduction to SiteMinder, please refer to the Netegrity white paper, "How to Secure Access for e-Business Websites."

SAP provides a web-based interface to many of their applications through a web server component known as Internet Transaction Server (ITS). ITS is the primary component for mySAP and mySAPWorkplace, and can provide single sign-on (SSO) for all the SAP applications. However, ITS cannot extend this support to non-SAP applications, thus creating a SAP single sign-on silo within your security infrastructure, as shown in the following figure.

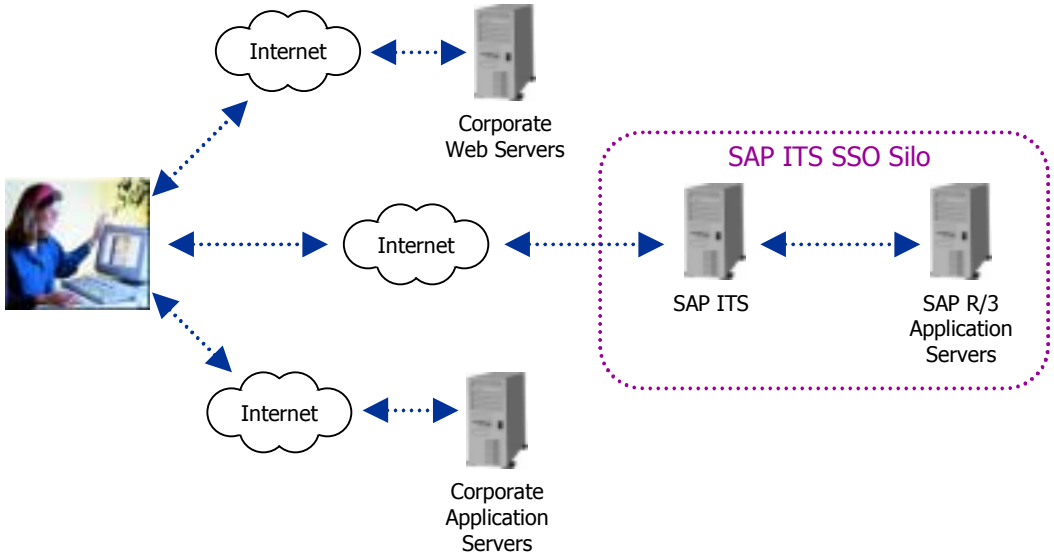


FIGURE 1 – SAP ITS SSO SILO

This white paper discusses how Netegrity has integrated its flagship security management product, SiteMinder, with SAP ITS so that customers can realize SSO across all their web-based applications. In addition, the Netegrity SiteMinder solution can also provide SAP customers the following benefits:

- Extended SSO;
- Enhanced Security Options;
- Increased Security (Tier 2 Integration);
- Reduced Portal Integration Costs / Time.

Each of these benefits will be discussed in greater detail in the following paragraphs.

EXTENDED SSO

SiteMinder can implement single sign-on within a single domain, across multiple Internet domains, or to affiliate sites. A single domain environment is one in which all resources exist in the same cookie domain. Multiple Web Agents within the same cookie domain can

be configured for SSO provided that you specify the same cookie domain in each Web Agent's configuration.

If SSO is enabled, the Web Agent caches the successful authentication, and issues an encrypted SSO session ticket to the user's browser. When the user accesses protected resources in other realms with the same protection level, they do not have to re-authenticate. Also, if the user moves to another Web server within this domain, then the SSO session ticket provides the appropriate session information to allow the user access, provided that the protection level rules were maintained.

In an environment that includes resources located across multiple domains, SiteMinder supports SSO across applications running on heterogeneous Web and application server platforms.

SiteMinder implements SSO across multiple domains by using a cookie provider. The cookie provider, which is a specifically configured SiteMinder Agent, passes a session ticket that contains the user's identity and session information to other domains in the SSO site. The user can then authenticate across the entire site. If the user's browser is missing this session ticket, the cookie provider sets it.

In addition to single and multiple domains, SiteMinder can provide SSO to an affiliate site via an Affiliate Agent. A SiteMinder Affiliate Agent provides a seamless connection from a main portal to an affiliate site without requiring a user to re-authenticate or provide additional information at the affiliate site. The Affiliate Agent extends the single sign-on and personalization capabilities provided by SiteMinder at the portal site to the affiliate site.

At the affiliate site, a small plug in called an Affiliate Agent is installed; there is no Policy Server. The affiliate site does not require a full installation because an Affiliate Agent does not protect resources in the same way as a Web Agent. It simply provides user information to a Web server for use with its Web applications, which use the information to personalize Web content for each user. The Affiliate Agent enables the affiliate to determine that the user has been authenticated at the main portal.

ENHANCED SECURITY OPTIONS

The SAP ITS allows for only basic authentication (i.e. username / password). With the SiteMinder SAP SSO solution, security administrators can implement a wide variety of authentication schemes. Currently, SiteMinder can support the following authentication schemes:

- Basic
- X509 Client Certificates
- HTML forms
- Tokens
- Proxy
- Digest
- NT LAN Manager (NTLM)
- Custom

In addition, SiteMinder allows administrators to assign protection levels to authentication schemes. With these protection levels, SiteMinder enables administrators to implement authentication schemes with additional measure of security and flexibility for an SSO environment. For example, a user who is authenticated in one realm can access a resource in another realm if the second is protected by an authentication scheme of an equal or lower protection level. As long as the protection level is the same or lower, that user does not need to re-authenticate. If a user tries to access a resource protected by an authentication scheme with a higher protection level, SiteMinder prompts the user to re-authenticate. In other words, enabling SSO does not provide blanket authorization to a user for all resources, if this is not desirable. Lastly, SiteMinder also supports the concept of authentication method chaining, which allows you to require multiple authentication methods in order to gain access to a specific resource.

INCREASED SECURITY (TIER 2 INTEGRATION)

One of the key security features and competitive advantages of the SiteMinder product is its ability to achieve Tier 2 integration with a variety of applications and products. Very few of our competitors can offer Tier 2 integration, and none can integrate at this level to as many products as Netegrity does. The differences between Tier 1 and Tier 2 integration are discussed in greater detail in the following paragraphs.

- Tier 1 integration typically describes the process in which an underlying application reads and interprets the authentication information passed by SiteMinder so the underlying application (Siebel, SAP, etc) can login the user and create its own session if necessary. Tier 1 integration is the minimum required to provide SSO. With Tier 1 integration, the underlying application fully trusts that the information was sent from SiteMinder and does no verification of that fact. In addition, Tier 1 leaves certain important integration issues untouched, such as session timeouts.
- With Tier 2 integration two important features are added to an integration. First, the capability for an underlying application to verify that the information passed in by SiteMinder was actually sent by our product vs. someone trying to hack the site. This capability is critical to ensuring that internal users are not attempting to compromise the application. Secondly, SiteMinder sessions and the underlying application's sessions are synchronized. If a user timeouts or logouts from SiteMinder, the underlying application's session does so as well. This capability avoids having open sessions in the underlying application when the user's session is no longer valid. This synchronization can increase security and reduce the resources necessary to run the application.

The SiteMinder Tier 2 integration with SAP ITS is discussed in greater detail in the Architecture section of this document.

REDUCED PORTAL INTEGRATION COSTS

Although many portal products can effectively integrate with SAP applications, the integration is typically Tier 1, which can have significant security and/or auditing consequences depending on how the integration is performed.

- Option 1: Portal stores user's credentials in its own database/directory, which may or may not be encrypted, and usually located on the web server, and thus wide open to a hacker attack;

- Option 2: Portal logs onto application as a super user, thus masking the identity of the true user. Therefore, the SAP audit logs will show the "portal" as the user, and the administrators must coordinate portal logs with SAP logs in order to determine who performed specific actions.

With SiteMinder, users can be authenticated at the main portal when they first login, and then move seamlessly to any SiteMinder protected resources and/or applications without being prompted for credentials. The portal itself would provide the presentation mechanism for the users, but SiteMinder would assume the responsibility for authenticating and/or authorizing the users. Because SiteMinder can natively integrate with most user directories and/or databases, there is no need to store user credentials in multiple locations.

In addition, SiteMinder can also provide increased Return on Investment for customers primarily through:

- Lower Cost of Application Deployment
- Lower Cost of support through SSO and Password Management
- Savings by leveraging existing infrastructure

Lower Cost of Application Deployment

By abstracting all security, personalization and entitlement logic out of the applications SiteMinder allows customers to realize an estimated 30% decrease in the cost of application development. In addition, applications are deployed more quickly allowing SiteMinder customers to realize additional returns through more timely delivery of applications and services to their end users.

Lower Cost through Single Sign-On and Password Management

With SiteMinder, users sign-on to a website once and gain access to all relevant information as defined by their user privileges. Single sign-on provides access to a personalized view of content residing on multiple applications which run on multiple servers, multiple platforms, and across multiple Internet domains. This benefits end-users by providing them with a high-quality user experience that is personalized to their needs and entitlements. The centralized security approach also minimizes the likelihood of a security breach by limiting the number of contact points. Analyst studies have shown that password management is estimated to save $75 per user per year.

Savings realized by Leveraging existing infrastructure

SiteMinder has been designed to support the platforms currently employed by companies, as well as new, emerging technologies. SiteMinder provides critical cost savings to IT departments by:

- Supporting the existing heterogeneous environments allowing clients to leverage their existing investments in technology while planning for the next generation of Internet technologies.
- Because SiteMinder can support both existing technologies and emerging standards in Internet technologies simultaneously, SiteMinder provides cost savings for clients as they migrate.

SiteMinder provides integration with all leading user directories, web servers, application servers and authentication technologies. SiteMinder also provides customers with support

for applications running on Microsoft, Apache, and iPlanet Web servers, as well as NT and UNIX platforms, making cross-platform development, deployment and migration easier.

BACKGROUND

SAP SSO OVERVIEW

SAP provides a web-based interface to many of their application offerings through a web server component known as Internet Transaction Server (ITS). ITS is the underlying architecture behind the more popular SAP products such as mySAP and mySAPWorkplace.

When a user attempts to execute an SAP transaction, ITS will prompt the user for their username, password, and language via an HTML form. Once authenticated, SAP will execute the requested transaction. Frequently, customers wish to have SSO across multiple transactions. SAP has two options to support this:

- Option 1 - SAP SSO Cookies
- Option 2 - SAP SSO2 Tickets

With Option 1, SAP R/3 will store the username and password in an encrypted cookie. This cookie is passed back to ITS, which in turn returns the cookie to the user's browser. SAP recommends this option only for legacy application support. With Option 2, SAP R/3 will generate a SSO2 Ticket, which offers significantly more flexibility, and is the preferred mechanism for achieving SSO. The SSO2 ticket is also stored in a cookie; however, instead of storing the username and password, the user's identity, session start time, and several other items are stored in the cookie by the SAP R/3 sever using standard public-key cryptographic routines. This design allows any SAP server to verify the user's identity without synchronizing passwords.

As mentioned previously, the SAP SSO extends only to those applications that are accessible via ITS (i.e., SAP applications). Many customers want to achieve SSO not only to SAP applications, but also across all their enterprise applications and resources. Therefore, Netegrity has worked closely with SAP to create a SiteMinder SSO solution to provide our mutual customers with this capability.

SITEMINDER OVERVIEW

Netegrity's flagship product, SiteMinder, makes e-business Web sites more secure and manageable. The SiteMinder platform provides companies with the ability to centrally manage user identity and entitlement information and to share this information across all of the applications on a site, greatly reducing the cost and complexity of administering these Web sites. The SiteMinder platform of shared services is managed through a rules based policy engine, which enables administrators to define policies that the SiteMinder platform will use to deliver services such as single sign-on, authentication management, entitlement management, and auditing. The SiteMinder platform is also used to manage B2B user driven transactions between companies that are putting transaction networks in place. From its inception, the SiteMinder platform was designed with full redundancy to allow for massive scalability and high reliability/availability.

A SiteMinder installation consists of two primary components:

- The SiteMinder Policy Server - The policy server is an NT or UNIX-based server that provides the following services: 1) Policy-based user management; 2) Secure portal management; 3) Authentication services; 4) Authorization services; 5) User registration services; 6) Password services; 7) Session management; and, 8) Auditing services.
- The SiteMinder Agent - The agent integrates with Web servers, Web application servers, or custom applications to enforce security and user management functions based on pre-defined policies. For RADIUS environments, the Agent is a Network Access Devices (NAS) device. SiteMinder supports the following types of Agents: Web Agents; Application Server Agents; Affiliate Agents; Custom Agents; and, RADIUS devices.

The following diagram illustrates different SiteMinder installations.

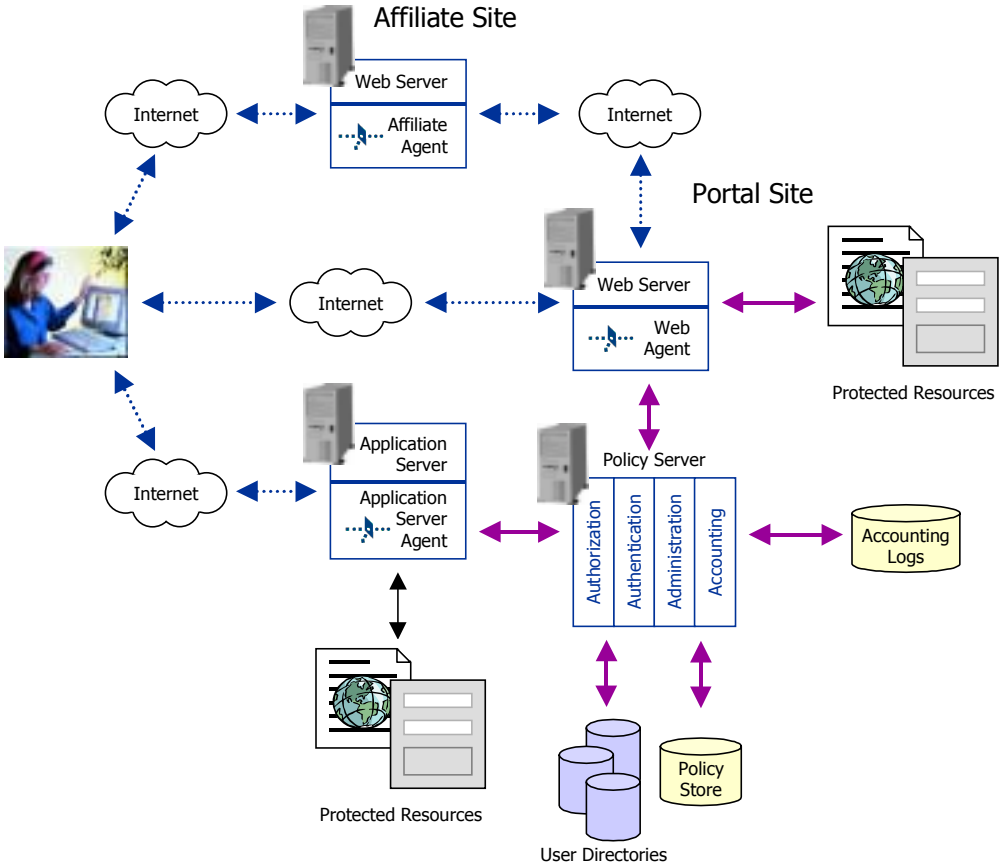


FIGURE – TYPICAL SITEMINDER INSTALLATIONS

SiteMinder provide four major services:

- Single Sign-On (SSO) - including SSO for single, multiple and affiliate cookie domains.
- Authentication Management – supporting basic, forms, X.509 certificate authentication with standard NT, LDAP and ODBC directories. This includes the ability

to define, choose, combine and relate authentication technologies to "ring levels" of protection.

- Entitlement Management – the ability to create and centrally manage models of access control for physical HTTP resources, as well as the ability to create and centrally manage application-specific authorizations on behalf of the user context.
- User Management – the ability to create and centrally manage a N-level model of delegation for LDAP directories. This includes the ability to create delegated administrators who can further create users that will map to specific contexts for pre-defined application authorization.

ARCHITECTURE

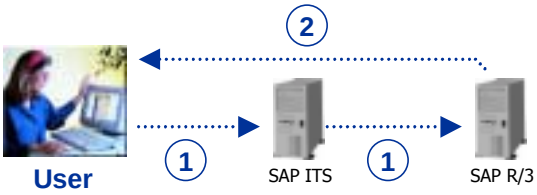
PREREQUISITES

In order to implement the SiteMinder SSO solution for SAP, customers would need the following hardware/software:

- SiteMinder
  - SiteMinder Policy Server v4.51 or higher
  - SiteMinder Connector for SAP Solutions
- Web Server
  - Microsoft IIS v4 or higher, OR
  - NES iPlanet Web Server, v3.6 or higher installed on Windows NT/Windows 2000
- SAP
  - mySAP v4.6D or higher; OR
  - mySAPWorkplace v2.10 or higher

SAP SSO ARCHITECTURE & PROCESS

Without the SiteMinder integration, a typical SAP environment including ITS appears as shown in the diagram below.



Actual Process Steps:

1. Access SAP transaction
2. Content + SSO cookie and/or SSO 2 ticket

FIGURE – SAP ITS SSO SOLUTION

As mentioned previously, this solution achieves SSO for SAP applications and/or resources, but does not allow for SSO beyond the SAP environment. In addition, ITS has limited support for authentication schemes.

SITEMINDER SSO ARCHITECTURE & PROCESS FOR SAP SOLUTIONS

Once the SiteMinder SSO solution for SAP is installed and enabled, the architecture and process become the following:

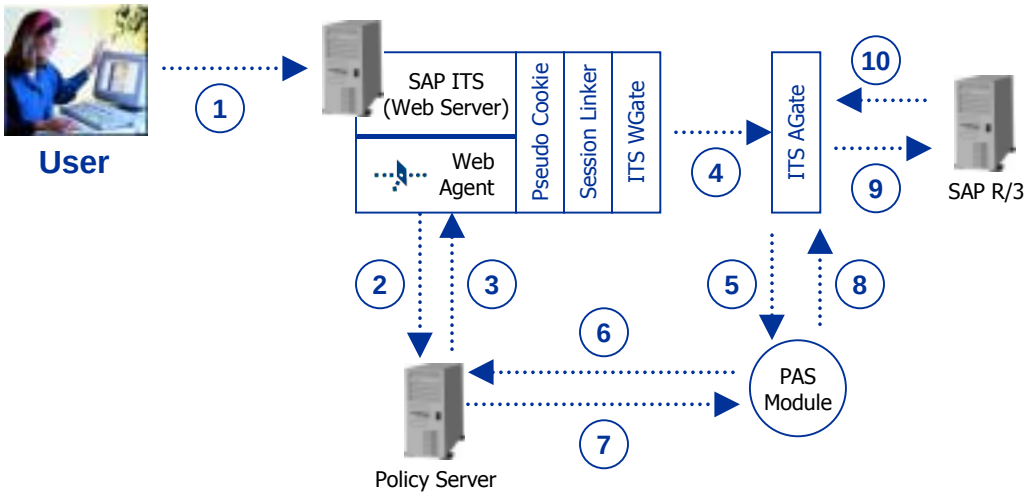


FIGURE – SITEMINDER SSO SOLUTION FOR SAP

The actual process steps are as follows:

1. User makes request to SAP application
2. Web Agent checks SiteMinder authentication & authorization
3. Result of active response is passed to Web Agent that in turn passes them as HTTP headers. A customized login page is loaded and processed by WGate
4. SAP WGate passes the login request to AGate
5. AGate calls the custom PAS module to verify username and SiteMinder session
6. PAS module passes data to Policy Server for verification
7. Policy Server returns result to PAS module
8. PAS module reports result to AGate
9. AGate requests an SAP SSO2 Login Ticket from SAP R/3
10. SAP R/3 returns SSO2 Ticket to Agate

CONCLUSION

With SAP ITS, the user can enjoy SSO within the SAP environment, but this capability does not extend beyond ITS or mySAPWorkplace. In addition, ITS is limited in the types of authentication schemes with which a user can be challenged. Netegrity's SiteMinder enables SAP customers to extend SSO to their corporate web and application servers, as well as to affiliate sites. Single sign-on across multiple platforms, applications, and Internet domains provides enhanced security, richer user experience, and decreased customer support costs due to lost passwords. The integration between SiteMinder and ITS provides a second level of authentication behind the DMZ in a trusted zone or corporate internal network. Two-tier authentication is critical for enterprise applications like SAP, which involve highly sensitive company information. The ability to provide a two-tier authentication model for SAP applications differentiates Netegrity from all of its competitors.