SiteMinder r12.5 new features

**Feature: Web 2.0 support**
SiteMinder r12.5 provides new Agent settings to better support modern web applications that make use of asynchronous JavaScript and XML (AJAX). You can configure SiteMinder to recognize requests coming from these applications and take special actions such as ignoring some requests (such as session heartbeats or polling requests) or returning special HTTP status codes and message bodies (when SiteMinder generates a response under a number of conditions, such as URL redirect at session timeout or a cookie provider redirect) that these applications can interpret. These options give organizations more flexibility for enabling interoperability between SiteMinder and rich, Web 2.0, internet applications.

**Feature: Open ID Authentication Scheme**
The OpenID authentication scheme is available in SiteMinder r12.5. You can use this to test the use of GoogleID, for example, as a means of authenticating users.

**Feature: Agent Discovery and Object Correlation**

SiteMinder 12.5 provides a centralized view of your connected Agent instances including how recently they have connected, their version, the type of agent they are, and environmental information such as the hostname and web server type they are installed on. You can also drill into the agent instance to more easily see which policies (policy objects), agent configuration objects, and host configuration objects are associated with the agent instance. This capability also enables you to identify unused agent object in your development environment in order to clean them up.

**Feature: Protecting the Administrative UI with SiteMinder**

In SiteMinder r12.5 the Administrative UI can be protected by a SiteMinder Web Agent deployed on a reverse proxy. The Administrative UI has a new step added to the Administrative Authentication wizard to simplify its configuration. This makes it possible to utilize advanced authentication and to audit access to the administrative UI.

**Feature: Administrative Workspaces**

In SiteMinder r12.5 administrators can setup administrative workspaces to delegate administration rights. The workspace defines which objects (e.g., agents, agent configuration objects, applications, policy domains, authentication schemes, and user directories) can be managed and what rights (e.g., read, read-write, delegation) are available to the scoped administrator. Using workspaces, centralized SiteMinder administration teams can delegate to distributed teams the ability to create their own agents, agent configurations, and policies using the scoped subset of authentication schemes, user directories, etc. This will provide distributed teams the autonomy they need while retaining the central control over the system.

**Feature: Enhanced Identity and Authorization mappings**

SiteMinder r12.5 supports a new kind of directory mapping that is more flexible than the auth-validate and authorization mapping capabilities currently included with the product. With the new functionality you can define validation or authorization mappings at the realm level. In addition, the new validation mappings can be created for the global realm. You will also be able to configure mappings between your authentication and authorization directories using any common attribute and each mapping can use a different attribute. For example, you can map between two LDAP directories using "uid" and map between LDAP and a RDBMS directory using "email".

**Feature: Central certificate store**

SiteMinder r12.5 includes a new central, shared certificate and key store that replaces smkeydatabase. With a centralized store it will no longer be necessary for the store to reside on each policy server or to execute manual synchronizations. During upgrade of SiteMinder, certificates found in smkeydatabase are automatically migrated to the new central store. In the first phase of the beta you will be able to manage the certificate store using the SiteMinder key tool utility. In the second phase of the beta you will be able to use the enhanced SiteMinder Administrative UI to upload and manage certificates in the new store. This capability will include ability to configure a grace period when enforcing a CRL.

**Feature: Support for hardware load balancers**

Hardware load balancers can now be used between Web Agents and Policy Servers to support IP address virtualization and simplify system management.

**Feature: Enhanced Active Directory password services**

SiteMinder r12.5 now supports better integration with Active Directory's native password services features. When a user attempts to change their AD password through SiteMinder password services and they supply a new password that was previously used and is not allowed because of AD's password history rules SiteMinder will display the message that they cannot reuse the password. Similarly when AD's policy is configured to force a user to change their password SiteMinder will now display the password must be changed page. And when the user's account is disabled in AD SiteMinder will display the user account disabled message. Finally, when a user changes their password in AD or LDAP through SiteMinder password services and mistypes their current password you can now set the DissalowForceLogin registry setting so that the user will be notified that they mistyped their current password.

**Feature: Removal of the smobjexport utility and replacement of smdiff with XML**

In SiteMinder r12.5 the smobjexport command will no longer be available and the SiteMinder Data Interchange Format Files (smdiff) files used to populate default policy stores will be replaced by XML files loaded by XPSImport. Customers will still have access to smobjimport to load smdiff files they may have but exports of r12.5 policy stores will be done exclusively with XPSExport. The XPS tools have benefits such as interchanging data easily between policy stores that use different encryption keys and a range of command line arguments that add flexibility. Use of the XPS tools is authorized based on the operating system user context rather than an ID/password making use of these tools with scripts more secure since the password doesn't have to be hardcoded or supplied at runtime.

**Feature: Upgrade from SiteMinder R6.x**

You can upgrade from SiteMinder r6.0 SP6 to SiteMinder r12.5 in order to test a number of things including: Policy Server upgrade, Policy Store upgrade, migration of certificates from the Policy Server's smkeydatabase to the new central key store, and Web Agent upgrade.

**Feature: Upgrade from SiteMinder r12.x**

You can upgrade from SiteMinder r12.0 SP2 and r12.0 SP3 to SiteMinder r12.5 in order to test a number of things including: Policy Server upgrade, Policy Store upgrade, migration of certificates from the Policy Server's smkeydatabase to the new central key store, and Web Agent upgrade.

**Feature: Content aware access policies (based on data classification) for Sharepoint 2010**

SiteMinder r12.5 will support a new Data Classification Service and you can use this with CA SiteMinder Agent for SharePoint to test the configuration and enforcement of access policies that take into account the classification of the data contained in SharePoint documents. For example, allow users to access documents in a site but block some users from accessing a subset of those documents that have been classified as having personally identifiable information or other type of sensitive data.

**Feature: Federation Management**

Federation services deployed on SiteMinder 12.5 will include a new UI wizard in the SiteMinder Administrative UI for managing the lifecycle of SAML 2.0 or SAML 1.1 federated partnerships. These enhancements will simplify the process of creating, duplicating, suspending, or deleting SAML 2.0 or SAML 1.1 partnerships as well as managing certificates and keys for your federation partnerships. [Note: The applet UI will still be available in 12.5.]

**Feature: Federation runtime enhancements**

Federation services deployed on SiteMinder 12.5 will include five new runtime capabilities:

1. Support for generating (as an Identity Provider) or consuming (as a Service Provider) authentication context requirements for user authentication in a federated transaction.

2. Support for generating (as an Identity Provider) user consent or checking that a user has consented (as a Service Provider) to a federated transaction.

3. Support for just-in-time user account provisioning

4. Support for being able to map assertion attributes from different Identity Providers to a common attribute on the Service Provider side of a federated transaction

Support for single logout over SOAP.

**Feature: Session store and authentication context enhancements**

SiteMinder r12.5 will support CA Directory DXGRID technology as a session store, introducing a number of advantages over current relational DBMS options, including: built-in replication for multi-data center support, and very high read-write performance. In addition, using SiteMinder r12.5 you will be able to capture information such as the SAML authentication level, SAML attributes, or information from the user's X.509 digital certificate (e.g. *subjectDN*, *issuerDN*, *serialNumber*, and *distributionPoint*), and store this data in the session store and retrieve it for use with authorization policies.

**Feature: Groups and OU support for EPM application policies**

In SiteMinder r12.5 will be able to easily configure Enterprise Policy Management (EPM) Roles, used with the EPM Application policy model by selecting groups and OUs from the user directory rather than having to first define expressions. This greatly simplifies policy creation based on the EPM Application model.