CA eTrust® SiteMinder®

Release Summary

r6.0 SP 5/6.x QMR 5

Second Edition

CA Product References

This document references the following CA products:

- CA eTrust® SiteMinder®
- CA eTrust® SiteMinder® Federation Security Services
- CA eTrust® SiteMinder® SAML Affiliate Agent
- CA eTrust® Audit iRecorder for SiteMinder®
- CA eTrust® Security Command Center

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 5: Changed Features for the SiteMinder Policy Server and Web Agent 21

Chapter 6: Changed Features for Federation Security Services 23

Chapter 1: Release Summary Overview

This section contains the following topics:

Finding Release Information

This release summary documents new and changed features for SiteMinder 6.0 SP 5/6.x QMR 5. For information on new features and fixes in cumulative releases (CRs) after 6.0 SP 5/6.x QMR 5, see the CR-specific product readme.txt file.

Chapter 2: New Features for the SiteMinder Policy Server and Web Agent

This section contains the following topics:

SharePoint 2007 Integration

SiteMinder may be configured to protect resources in a new or existing Microsoft SharePoint 2007 environment.

Note: More information on protecting resources in a SharePoint 2007 environment exists in the *Policy Design Guide*.

Kerberos Authentication

SiteMinder may be configured to use the Kerberos Authentication scheme to protect resources in a Kerberos domain.

Note: More information on using the Kerberos Authentication scheme exists in the *Policy Design Guide*.

Single Sign-On Security Zones for Strong Authorization

A security zone is a subset of single sign-on and it is a method of partitioning applications within a single cookie domain so that different security requirements can be configured for these applications. Security Zones is a method of further strengthening authorizations.

All applications in the same security zone allow single sign-on amongst themselves. Access across multiple security zones depends on the trust relationship between the zones. If a user has a valid session for any zone in a group of zones with a trusted relationship, the user has single sign-on when visiting any zone in this group.

Prior to the SSO Security Zones feature, the only way to group applications for single sign-on was to create different network domains and different cookie domains, such as CA1.COM, CA2.COM and use various multi-cookie domain configurations with cookie providers. This is not desirable in most enterprises, since using multiple network domains has certain IT maintenance and support consequences.

Note: For more information about security zones, see the *Web Agent Guide*.

Credentials Selector for Strong Authentication

The SiteMinder Credentials Selector lets you configure an authentication environment that presents an end user with a choice of credentials for logging in to a site to access a resource. The authorization decisions and user responses can be configured to depend on the end user's choice of authentication credentials.

For example, a user requests access to a protected application that provides him with a certain spending level for online purchases. A dialog box opens with a choice of basic authentication (Username and Password) or smart card authentication (SecureID or SafeWord).

If the user supplies only a valid Username and Password, the authentication level is 5 and his spending level is $1000. If the user supplies a valid Username and Password and checks the smart card authentication check box, he is prompted for his smart card PIN. Assuming that the PIN he provides is valid, the authentication level becomes 15, which allows the user a spending level of $5,000.

Note: For more information about the Credentials Selector, see the Credentials Selector technical note on the Technical Support site.

Sun Java System Web Agent is Now a Framework Agent

The framework architecture is now supported for any Web Agent installed on a Sun Java System Web server. The framework architecture provides support for dynamic central agent configuration and rolling log support on UNIX platforms.

The Sun Java System Web Server referred to in Web Agent documentation was formerly the Sun ONE Web Server.

Note: For a description of framework and traditional Web Agents, see the *Web Agent Guide*.

Improved User Experience When a SiteMinder Session Expires

When a user's SiteMinder session times out, the Web Agent can now redirect the user to a URL that displays a page explaining that the session has been terminated and how the session can be reestablished. If the user simply gets rechallenged after a session times out, that user may not understand why they have to provide credentials.

Note: For more information about this subject, see the *Web Agent Guide*.

Web Agent Parameter to Reduce Calls to the Policy Server During Forms Authentication

During forms authentication, the Web Agent makes an IsProtected call to the Policy Server to determine if the resource is protected. After this first call, the FCC typically makes an additional IsProtected call to the Policy Server to establish realm context so it can log a user in to access a protected resource. You can now control whether the FCC makes this additional call using the FCCForceIsProtected parameter.

Note: For more information about the FCCForceIsProtected parameter, see the *Web Agent Guide*.

Web Agent Parameters to Secure Session Cookies

Two new time-based session cookie parameters reduce the possibility of a SiteMinder session cookie being compromised by administrators or other users who have access to the following:

- Web server logs
- SiteMinder Web Agent logs
- Proxy servers sitting between domains in cross-domain single sign-on environments

These Web Agent parameters are as follows:

- CookieValidationPeriod – This parameter contains a value in seconds. If configured, the receiving Web Agent accepts the URL session cookie for only the number of seconds specified in this parameter. If not configured or set to 0, the cookie is valid until the Idle and Max Session Timeout values are met.
- ExpiredCookieURL – This parameter allows you to set an optional URL for the agent to redirect to if the URL session cookie has expired.

Note: For more information about these parameters, see the *Web Agent Guide*.

Web Agent Parameters to Prevent Unwanted Changes to SMSESSION Cookie

Outlook Web Access makes HTTP requests that update the SiteMinder SMSESSION cookie so that the session never expires. Web Agents can now skip the creation or update of existing SMSESSION cookies using the OverlookSessionForMethods and OverlookSessionForUrls parameters.

Note: For more information about these parameters, see the *Web Agent Guide*.

Improved Performance of the Forms Credential Collector

The form cache is a single repository for storing form template data. The form cache relieves the forms credential collector (FCC) by storing form template files in memory, where they can be read easily. Virtual memory access is faster than disk access, allowing FCC components to process forms more quickly with reduced strain on the host server. The improved processing time increases the FCC's capacity for serving requests for each web server and makes forms authentication more efficient.

Note: For more information about form cache, see the *Web Agent Guide*.

Solaris 10 Certification

The Policy Server and Web Agent are certified for global and non-global zones on systems running Solaris 10.

Note: For more information about Solaris 10 support, see the *Policy Server Installation Guide*.

Directory Mapping Configurations

Directory mapping now supports a configuration that lets SiteMinder authenticate users against one directory and validate users against another.

As a result, you can use the single sign-on (SSO) feature across multiple user directories in separate policy stores, even if the user directory name or user DN differs across individual user stores for the same user identity.

Note: For more information about configuring directory mappings, see the *Policy Server Design Guide*.

Oracle Support for iRecorder for eTrust SiteMinder

The eTrust Security Command Center (SCC) is now able to read security-related log data from the SiteMinder SQL Server and Oracle logs database.

Note: For more information about upgrading the 6.x audit log database schema to support the SiteMinder/eTrust SCC integration, see the *Policy Server Upgrade Guide*. For more information about the iRecorder, see the *eTrust Audit iRecorder Reference Guide*.

Resetting Policy Server Statistics

There is a new debugging option to troubleshoot the Policy Server. To use debugging options, run the Policy Server process, smpolicysrv, interactively in a command window with debugging options turned on.

The following command lets you log Policy Server statistics to the Policy Server log file:

```
smpolicysrv -stats
```

However, resetting the statistics required you to restart the Policy Server.

The following command now lets you reset Policy Server statistics without restarting the Policy Server:

```
smpolicysrv -resetstats
```

The -resetstats switch resets the following counters:

- Max Threads is reset to the Current Threads value.
- Max Depth of the message queue is reset to the Current Depth of the message queue.
- Max Connections is reset to Current Connections.
- Msgs, Waits, Misses, and Exceeded limit are reset to zero.

The -resetstats switch does not reset the following counters:

- Thread pool limit
- Current Threads
- Current Depth of the message queue
- Current Connections
- Connections Limit

Note: For more information about troubleshooting the Policy Server, see the *Policy Server Management Guide*.

Chapter 3: New Features for Federation Security Services

This section contains the following topics:

WS-Federation Support for Single Sign-on

SiteMinder's Federation Security Services now WS-Federation single sign-on (SSO) based the following specifications:

- Web Services Federation (WS-Federation)
- WS-Federation Passive Requester Profile (WS-F PRP)
- WS-Federation Passive Requester Interoperability Profile

Note: For more information about WS-Federation support in SiteMinder, see the *Federation Security Services Guide*.

User Authorizations Based on User Attributes

The SiteMinder Policy Server can now authorize a user based on user attributes provided by a SAML 2.0 Attribute Authority, which is an Identity Provider that adheres to the SAML 2.0 Assertion Query/Request profile.

When a user requests access to a protected resource, the authorizing entity, the SAML Requester, can request additional user attributes to determine whether access to the resource should be granted.

Note: For more information about user attribute authorizations, see the *Federation Security Services Guide*.

I18N Internationalization Support

Federation Security Services supports the following features for I18N internationalization:

- Federation Security Services configuration objects, Java and C++ code are encoded in UTF-8 format for the internationalization purposes.
- SiteMinder supports the creation and consumption of default and customized SAML 1.x, SAML 2.0, and WS-Federation assertions with multibyte user ids and attribute values.
- All target and redirect URLs are encoded per HTTP 1.1 RFC 2616 so multibyte path and file names are handled correctly.

Note: For more information, see the *Federation Security Services Guide*.

SAML 2.0 Metadata Utility For Efficient Configuration

SiteMinder provides a metadata tool to programmatically import and export SAML 2.0 metadata so you can efficiently exchange federation configurations between a site that uses SiteMinder and a partner that may use SiteMinder.

The two utilities that make up the metadata tool are:

- smfedexport
- smfedimport

Note: For more information about the metadata utility, see the *Federation Security Services Guide*.

Indexed Endpoints

SiteMinder Federation Security Services offers you the ability to configure indexed endpoints. An indexed endpoint is the site where assertions are consumed. In the context of SiteMinder, this endpoint is the Service Provider where the Assertion Consumer Service resides.

You can configure indexed endpoints for a SiteMinder Service Provider that has a federated relationship with a third party Identity Provider that supports indexed endpoints. You may also want to configure different protocol bindings (artifact vs. POST) for the Assertion Consumer Service by assigning more than one endpoint to the service.

Note: For more information about indexed endpoints, see the *Federation Security Services Guide*.

Federation Web Services Deployment on JBOSS

You can now deploy the Federation Web Services application on a JBoss Application Server.

Note: For more information about deploying on JBoss, see the *Federation Security Services Guide*.

Use of the Allow/Create Attribute for a New Identifier

As part of a single sign-on request, a Service Provider may request a particular user attribute for inclusion in an assertion that is not available in the user record at the Identity Provider.

To manage this situation, you can configure a SAML 2.0 Service Provider request to include the Allow/Create attribute, which instructs the Identity Provider to create a new identifier, provided the Policy Server at the Identity Provider is configured to do so.

Note: For more information about the Allow/Create attribute, see the *Federation Security Services Guide*.

SSO Security Zones to Improve Federation Deployment

A SiteMinder environment can be set up to include a Web application environment for web service protection and a federation environment for federated resource protection. This method can make a SiteMinder deployment more efficient.

Note: For more information about security zones, see the *Federation Security Services Guide* and the *Web Agent Guide*.

Chapter 4: New Features for the SiteMinder SDK

This section contains the following topics:

Pure Java Implementation of Java Agent API

The SiteMinder Java Agent API now has two implementations:

- The JNI Java Agent API, which relies on the native C/C++ Agent API libraries. It uses the interface presented in the SiteMinder SDK, versions 5.x and 6.0.
- The pure Java Agent API, which replaces the native code used in the JNI Java Agent API with pure Java components. The current version of this API uses the same interface as the JNI Java Agent API.

You can choose either implementation.

Note: For more information about the Java Agent API, see the *Developer's Guide for Java*.

API Support for WS-Federation

WS-Federation specifies a protocol for how passive clients (for example, Web browsers) implement the federation framework. Web SSO and sign-out are implemented using Account Partners and Resource Partners. You can define an Account Partner or Resource Partner using calls from the SiteMinder C Policy Management API and the Perl Policy Management API.

Note: For more information about code implementations of WS-Federation, see the *Developer's Guide for C* and the *Scripting Guide for Perl*.

API Support for SAML 2.0 Attribute Authority

SiteMinder now supports authorization for user access to a resource by requesting the value or values of predetermined user attributes from a remote site and then using those values as the basis for the authorization decision. The request contains no session information because the user is not necessarily authenticated on the remote site.

Note: For information about how the SiteMinder Policy Management APIs implement this kind of authorization decision, see the *Developer's Guide for C* and the *Scripting Guide for Perl*.

API Support for SAML 2.0 Indexed Endpoints

When configuring single sign-on at an Identity Provider, you can specify more than one endpoint for the Assertion Consumer Service. Each endpoint is assigned a unique index value, instead of a single, explicit reference to an Assertion Consumer Service URL. Using an assigned index enables you to use different Assertion Consumer Services for different protocol bindings.

Note: For information about specifying indexed endpoints programmatically, see the *Developer's Guide for C* and the *Scripting Guide for Perl*.

Chapter 5: Changed Features for the SiteMinder Policy Server and Web Agent

This section contains the following topics:

ODBC SQL Query Schemes

ODBC user directory SQL Query Schemes previously could only be configured to use literal queries. ODBC SQL Query Schemes can now be configured to use literal and bind-based parameters.

Note: For more information on creating bind-based queries, see the *Policy Design Guide*.

Policy Server Profiler Performance Improvement

Trace messages can now be buffered when written to the trace logs, which results in improved Policy Server performance.

Note: For more information on enabling buffered tracing, see the *Policy Server Management Guide*.

Mixed Policy and Key Store Configurations

The Policy Server now supports mixed LDAP/ODBC policy and key stores. The policy store can exist in an ODBC database, and the key store can exist in an LDAP Directory Server, or vice versa.

Note: For more information on configuring policy and key stores, see the *Policy Server Management Guide*.

Key Store Management and Policy Server Behavior

The Policy Server now behaves in the following ways when a key store becomes unavailable:

- When a key store that has been configured separately from the policy store becomes unavailable, the Policy Server goes in to a suspended state and refuses any new requests on established connections until the key store comes back online.
- A Policy Server in a suspended state remains up for the length of time specified in SuspendTimeout, at which point the Policy Server shuts down gracefully. If SuspendTimeout is equal to zero, the Policy Server remains in the suspended state until the key store connection is reestablished.
- When the Policy Server is started and the key store is unavailable, the Policy Server shuts down gracefully.

Note: For more information on key store management, see the *Policy Server Management Guide*.

Chapter 6: Changed Features for Federation Security Services

This section contains the following topics:

PKI Infrastructure and Usability Improvements

The following changes and improvements have been made to SiteMinder's PKI infrastructure:

- The AM.keystore, which resided at the consumer-side Web Agent, has been replaced by the smkeydatabase to improve the handling of certificates.
- There is a new migratekeystore utility to enable you to migrate the AM.keystore to an smkeydatabase.
- The smkeytool utility has been modified to use new command arguments.
- The Java keytool utility is no longer used to modify a key database.
- You can now assign alias names to each certificate in an smkeydatabase.

Note: For more information about these PKI changes, see the *Federation Security Services Guide*.

Removed Session Store Limitation

For artifact authentication, the total size of an assertion passed to an consumer could not exceed 4K because that was the size that could be stored in the session server.

This limit has been removed, enabling you to include a large number of attributes in an assertion.

Note: For more information about these changes, see the *Federation Security Services Guide*.