Mercury IT Governance Center™

Netegrity SiteMinder Integration

Executive Summary

This document addresses how to integrate Mercury IT Governance Center™ release 6.0 and Netegrity SiteMinder version 5.5 or 6.0. The integration allows Mercury IT Governance Center users to be authenticated through SiteMinder during the logon process. SiteMinder single sign-on is fully supported from both the standard and Workbench interfaces.

This document is intended for system administrators familiar with setting up and configuring Netegrity SiteMinder and Mercury IT Governance Center.

MERCURY™

Overview

Problem

Large enterprises often face the challenge of dealing with disparate authentication mechanisms for the applications that support their information technology (IT) infrastructure and business systems. Netegrity SiteMinder is an industry-leading product that addresses this challenge. It makes these systems more secure and manageable by providing a platform for centrally managing all applications. This results in a more scalable alternative to building proprietary user directories and access control systems into each individual application. The centralized approach to security management enables companies to reduce their administration cost and complexity.

SiteMinder also enables single sign-on mode to make application logon and logoff easy for large user bases. This also simplifies application integration when navigating from one application to another.

Solution

Mercury IT Governance Center can be configured to delegate user authentication to Netegrity SiteMinder for both the standard (Web) and Workbench interfaces. This configuration supports two authentication modes: mixed and Single Sign-on (SSO).

Mixed Mode

In this configuration, Mercury IT Governance users continue to log on using the Mercury IT Governance Logon page. Within the Mercury IT Governance Server, the integrated SiteMinder Authentication Module routes the login request to an existing SiteMinder Policy Server for authentication. This mode is referred to as mixed because Mercury IT Governance Center can be configured to use both SiteMinder and its own authentication simultaneously. In this case, each Mercury IT Governance Center user account must specify which authentication mode is to be used.

Single Sign-on Mode

In this configuration, Web requests are authenticated before being passed to Mercury IT Governance Center, bypassing the Mercury IT Governance Center Logon page. To enable SSO mode, the SiteMinder Web Agent must be plugged into any third-party Web server that Mercury IT Governance Center supports, and be configured to communicate with a SiteMinder Policy Server. The SiteMinder Web Agent intercepts Web requests and checks with the Policy Server to ensure they are authenticated before passing them to Mercury IT Governance Center.

Note that SiteMinder cannot be used to manage Mercury IT Governance Center application-level authorization, such as controlling access to various screens and functions. This type of access is controlled by the Mercury IT Governance Center security model, using security groups, access grants, product licensing, and so forth. Therefore, user accounts must exist in both Mercury IT Governance Center and the SiteMinder Policy Server, but their passwords do not have to be maintained by Mercury IT Governance Center.

High-Level Architecture

Single Sign-on Mode

This configuration requires that Mercury IT Governance Center be integrated with an external Web server that has both the SiteMinder Web Agent and Mercury IT Governance Web Server Module installed. The Mercury IT Governance Center internal Web server does not support SiteMinder SSO because Netegrity does not yet provide a compatible Web Agent or a suitable API to create one.

The SiteMinder Web Agent is the single access point for all Web clients. The SiteMinder Web Agent will intercept all incoming requests and ensure that they are authenticated before passing them to the Mercury IT Governance Web Server Module. The requests will then proceed to the Mercury IT Governance Server.

For Workbench clients, the SiteMinder Web Agent protects access to the Workbench Logon page. Once the Logon page is reached, the user authentication information is passed to the Workbench applet for automatic logon. Once launched, the applet communicates directly with the Mercury IT Governance Server.

Note

The Workbench does not support SSO mode when launched as an application (a less frequent scenario typically leveraged on UNIX clients). However, if Mercury IT Governance Center is launched as an application, it will still authenticate using SiteMinder. See the *Configuring the Workbench as a Java Application* section in Chapter 7 of the *System Administration Guide and Reference*.

A system diagram of the SiteMinder integration in SSO mode is shown in *Figure 1*.

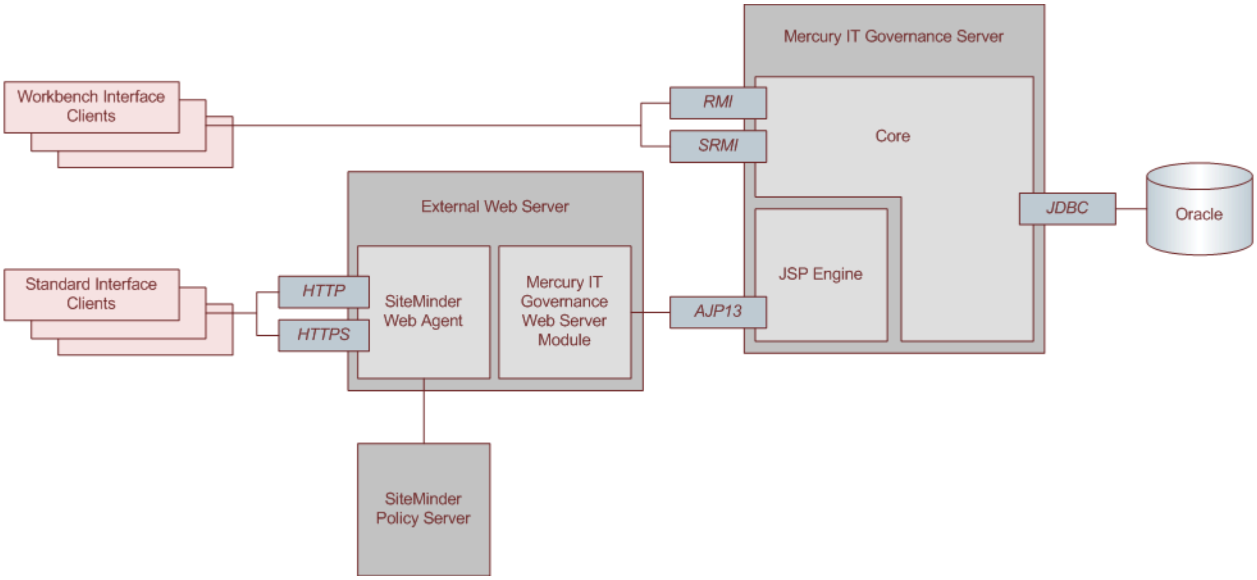

Mercury IT Governance Server
Workbench Interface Clients
RMI
SRMI
Core
External Web Server
JDBC
Oracle
Standard Interface Clients
HTTP
HTTPS
SiteMinder Web Agent
Mercury IT Governance Web Server Module
JSP Engine
AJP13
SiteMinder Policy Server

Figure 1. SiteMinder integration architecture for SSO mode

Mixed Mode

In this configurations, users log on directly to Mercury IT Governance Center, and the integrated SiteMinder Authentication Module passes logon information to the SiteMinder Policy Server for authentication.

To use mixed mode, the integrated SiteMinder Authentication Module must be properly configured. An external Web server can be used, but is not required.

For Workbench clients, once the Logon page is reached, the user authentication information is passed to the SiteMinder Policy Server for verification. Once validated, the information is passed to the Workbench applet for automatic logon. Once launched, the applet communicates directly with the Mercury IT Governance Server.

A system diagram of the SiteMinder integration in mixed mode is shown in *Figure 2*. The integration architecture with the optional Web server is shown in *Figure 3*.

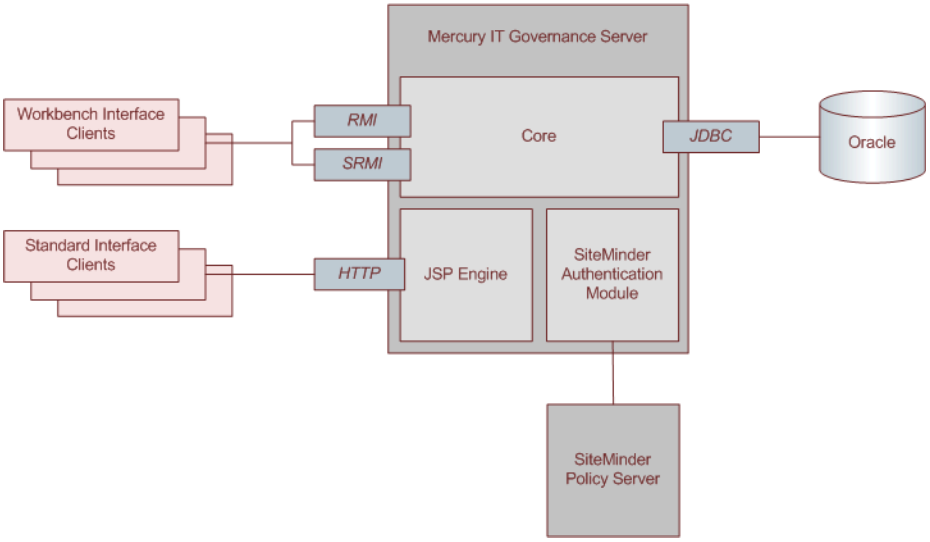

Mercury IT Governance Server
Workbench Interface Clients
RMI
SRMI
Core
JDBC
Oracle
Standard Interface Clients
HTTP
JSP Engine
SiteMinder Authentication Module
SiteMinder Policy Server

Figure 2. SiteMinder integration architecture for mixed mode

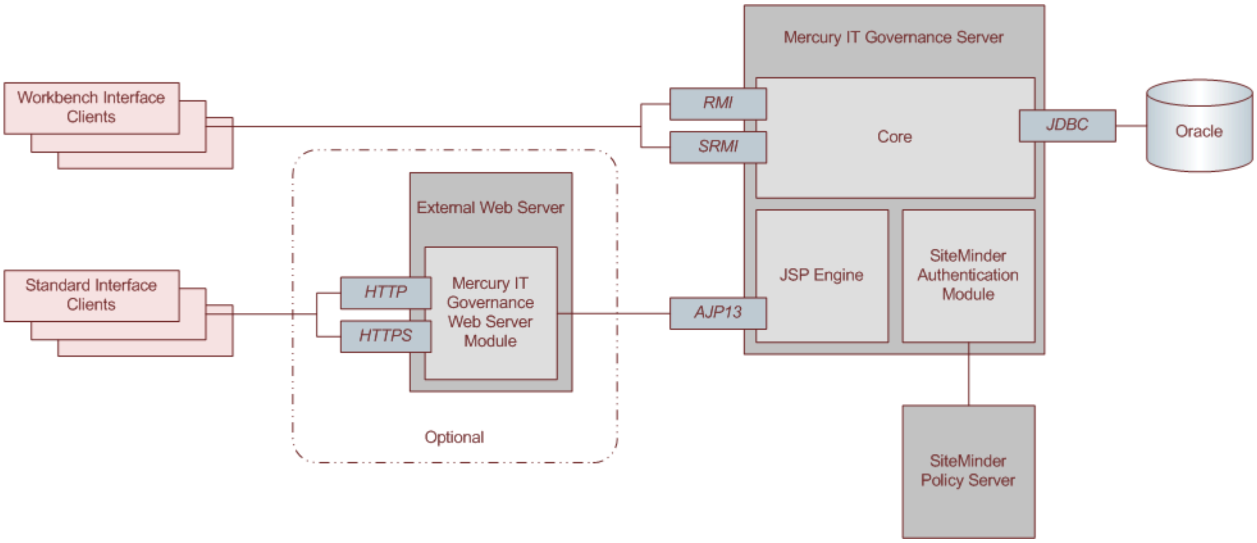

Mercury IT Governance Server
Workbench Interface Clients
RMI
SRMI
Core
JDBC
Oracle
External Web Server
Standard Interface Clients
HTTP
HTTPS
Mercury IT Governance Web Server Module
AJP13
JSP Engine
SiteMinder Authentication Module
Optional
SiteMinder Policy Server

Figure 3. SiteMinder integration architecture for mixed mode with optional Web server

Requirements

Software Requirements

A fully integrated system consists of the following software. Mercury-specific configuration information is detailed in the following section.

- Mercury IT Governance Center release 6.0
  (for both SSO and mixed modes)

  For installation information, see the *System Administration Guide and Reference*. Ensure that Mercury IT Governance Center is operating normally before it is configured for integration with SiteMinder.

- Netegrity SiteMinder version 5.5 or version 6.0
  (for both SSO and mixed modes)

  Refer to the Netegrity SiteMinder documentation for installation information. Ensure that SiteMinder is operating normally before it is configured for integration with Mercury IT Governance Center.

- External Web server with the following additional software
  (for SSO mode)

  Refer to the *System Requirements and Compatibility Matrix* guide for the complete list of supported Web servers.

  - Mercury IT Governance Web Server Module

    For installation information, see the *Configuring an External Web Server* section of the *System Administration Guide and Reference.*

  - SiteMinder Web Agent

    Refer to the Netegrity SiteMinder documentation for installation information and install the SiteMinder Web Agent on the same Web server as the Mercury IT Governance Web Server Module.

- External Web server with the following additional software
  (optional for mixed mode)

  Refer to the *System Requirements and Compatibility Matrix* guide for the complete list of supported Web servers.

  - Mercury IT Governance Web Server Module

    For installation information, see the *Configuring an External Web Server* section of the *System Administration Guide and Reference.*

Detailed Configuration

The SiteMinder integration process includes the following steps. Refer to the associated sections for details on each topic.

- *Step One: Configure Mercury IT Governance Center*
- *Step Two: Configure Mercury IT Governance Center Users*
- *Step Three: Configure Netegrity SiteMinder Policy Server*
- *Step Four: Restart SiteMinder*
- *Step Five: Restart Mercury IT Governance Center*

Note

In the following steps, these placeholders are used:

- `<ITG_HOME>` represents the installation path for Mercury IT Governance Center
- `<server.domain.port>` represents the base URL for the Mercury IT Governance Server

Step One: Configure Mercury IT Governance Center

To configure Mercury IT Governance Center to integrate with SiteMinder, complete the following steps:

1. Before customizing Mercury IT Governance Center for use with SiteMinder, verify that the installation is functioning properly.

2. Install the SiteMinder Java Agent API on the Mercury IT Governance Server.

   - For Windows

     Copy the `smjavaagentapi.jar` file to the `<ITG_HOME>\server\kintana\deploy\itg.war\WEB-INF\lib` folder.

   - For UNIX

     Copy the `smjavaagentapi.jar` file to the `<ITG_HOME>/server/kintana/deploy/itg.war/WEB-INF/lib` directory.

     This JAR file is available on the SiteMinder Developer SDK CD. The Mercury IT Governance Server will automatically include the JAR file in its CLASSPATH upon server startup.

3. Install the SiteMinder Agent native code.

   - For Windows

     Copy the `smjavaagent.dll` file to the `<ITG_HOME>\integration\siteminder` folder.

     If you with to place the `smjavaagent.dll` file in a different folder, ensure that the folder is included in the PATH system environment variable.

   - For UNIX

     Copy the `libsmjavaagent` API library file to the `<ITG_HOME>/integration/siteminder` directory.

     If you with to place the `libsmjavaagent` file in a different directory, ensure that the directory is included in the LD_LIBRARY_PATH environment variable.

4. Edit the SiteMinder configuration file and ensure that the settings match the SiteMinder setup.

   - For Windows

     The file can be found at `<ITG_HOME>\integration\siteminder\siteminder.conf`.

   - For UNIX

     The file can be found at `<ITG_HOME>/integration/siteminder/siteminder.conf`.

   The following is a copy of the default `siteminder.conf` file provided by Mercury IT Governance Center. Pay special attention to the value for `SM_AGENT_NAME`. If any SiteMinder settings are modified, this file must also be updated to reflect the changes.

```
# siteminder.conf

###################
# Global Settings #
###################

# The shared secret as defined in SiteMinder (case sensitive).
# The value can be optionally encrypted using
# ITG_HOME/bin/kEncrypt.sh
SM_SHARED_SECRET=12345

# Connection settings. Please refer to SiteMinder documentation for
# appropriate settings.
SM_CONNECTION_MIN=1
SM_CONNECTION_MAX=1
SM_CONNECTION_STEP=1
SM_CONNECTION_TIMEOUT=5

######################################
# Primary SiteMinder Server Settings #
######################################

# The hostname of the primary SiteMinder policy server.
```

```
SM_POLICY_SERVER=172.18.0.159
SM_AGENT_NAME=porsche

# Standard SiteMinder Ports
SM_AUTHORIZATION_PORT=44443
SM_AUTHENTICATION_PORT=44442
SM_ACCOUNTING_PORT=44441
SM_PROTECTED_URL=/itg/

# Optional Secondary SiteMinder Server Settings
# Create one @secondary block for each additional
# secondary server. The connection settings
# may be specified if desired. Otherwise, the global
# values will be used.

# @ secondary
# SM_POLICY_SERVER=
# SM_AUTHORIZATION_PORT=
# SM_AUTHENTICATION_PORT=
# SM_ACCOUNTING_PORT=

# @ secondary
# SM_POLICY_SERVER=
# SM_AUTHORIZATION_PORT=
# SM_AUTHENTICATION_PORT=
# SM_ACCOUNTING_PORT=
```

5. (Optional, although highly recommended) Create a backup copy of the Mercury IT Governance Center `server.conf` file.

6. For mixed mode:

   a. In the `server.conf` file, modify the authentication mode as shown below. This allows selection of SiteMinder or ITG authentication for the Mercury IT Governance Center users.

   ```
   com.kintana.core.server.AUTHENTICATION_MODE=ITG,SiteMinder
   ```

   b. Comment out the following setting in the `server.conf` file:

   ```
   com.kintana.core.server.SINGLE_SIGN_ON_PLUGIN=com.kintana.sc.security.au
   th.SiteMinderSingleSignOn
   ```

   c. Stop, then restart the Mercury IT Governance Server.

   d. Using the User Workbench, change the users' Authentication Mode to SiteMinder.

Note

You may want to have a few accounts set to use ITG Authentication Mode. This would permit access to Mercury IT Governance Center in the event that the SiteMinder Policy Server is unavailable.

7. For SSO mode:

   a. In the `server.conf` file, modify the authentication mode as shown below. This allows exclusive SiteMinder authentication for the Mercury IT Governance Center users.

   ```
   com.kintana.core.server.AUTHENTICATION_MODE=SiteMinder
   ```

   b. In the `server.conf` file, specify use of SSO as shown below:

   ```
   com.kintana.core.server.SINGLE_SIGN_ON_PLUGIN=com.kintana.sc.security.au
   th.SiteMinderSingleSignOn
   ```

   c. Stop, then restart the Mercury IT Governance Server.

Note

When both the SiteMinder Web Agent and Mercury IT Governance Web Server Module are installed on the external Web server, the SiteMinder Web Agent always takes precedence for requests in the form of `/itg/*`.

Step Two: Configure Mercury IT Governance Center Users

To configure Mercury IT Governance Center users to authenticate using SiteMinder, complete the following steps:

1. Ensure that the usernames for Mercury IT Governance Center users match those used by SiteMinder.

2. Ensure that Mercury IT Governance Center users have been set up to use SiteMinder authentication.

Warning

In SSO mode, users will be locked out of Mercury IT Governance Center if their authentication is set to anything other than SiteMinder.

If that situation arises, revert to the `server.conf` file created in step 5 on page 9. Then make the necessary changes to the user accounts before resetting the authentication mode in the `server.conf` file.

Step Three: Configure Netegrity SiteMinder Policy Server

Before configuring SiteMinder for use with Mercury IT Governance Center, ensure that the Policy Server is working correctly and the User Directory to be used for Mercury IT Governance Center authentication is properly configured. The SiteMinder Test Tool is useful for verifying that the installation is functioning properly.

Configuring SiteMinder for Mercury IT Governance Center is the same as configuring any other type of protected resource in SiteMinder. Use the SiteMinder Policy Server User Interface to update the SiteMinder configuration entities as necessary. For both mixed and SSO mode, the following standard SiteMinder configurations should exist: Host Configuration Object, User Directory, Policy Domain, and Policy.

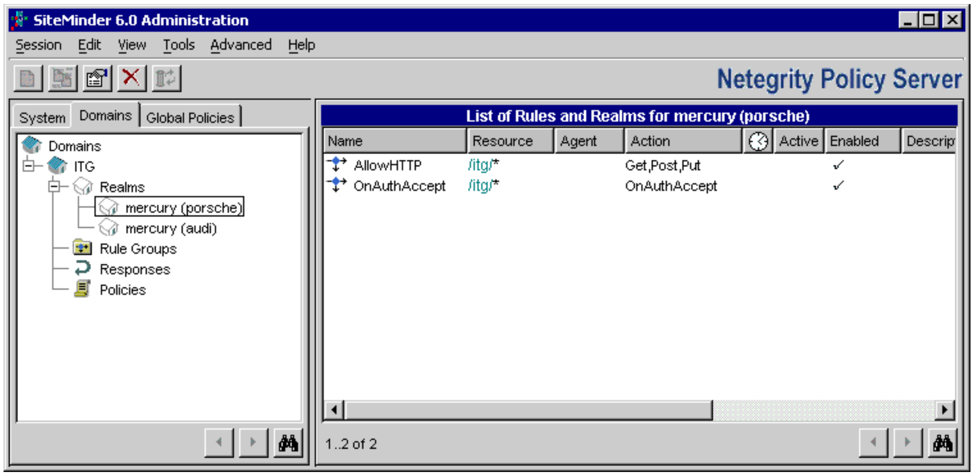
Additional Configuration for SSO Mode Only

For SSO mode, the following additional SiteMinder entities should be configured:

- A realm and associated rules for Mercury IT Governance Center
- Agent and Agent Conf Object

1. Configure a realm for Mercury IT Governance Center, and add two rules as shown in *Figure 4* below. This figure shows a SiteMinder Policy Domain configured for two different realms (for two different instances of Mercury IT Governance Center).

   Note that the resource being protected must be `/itg/*`.



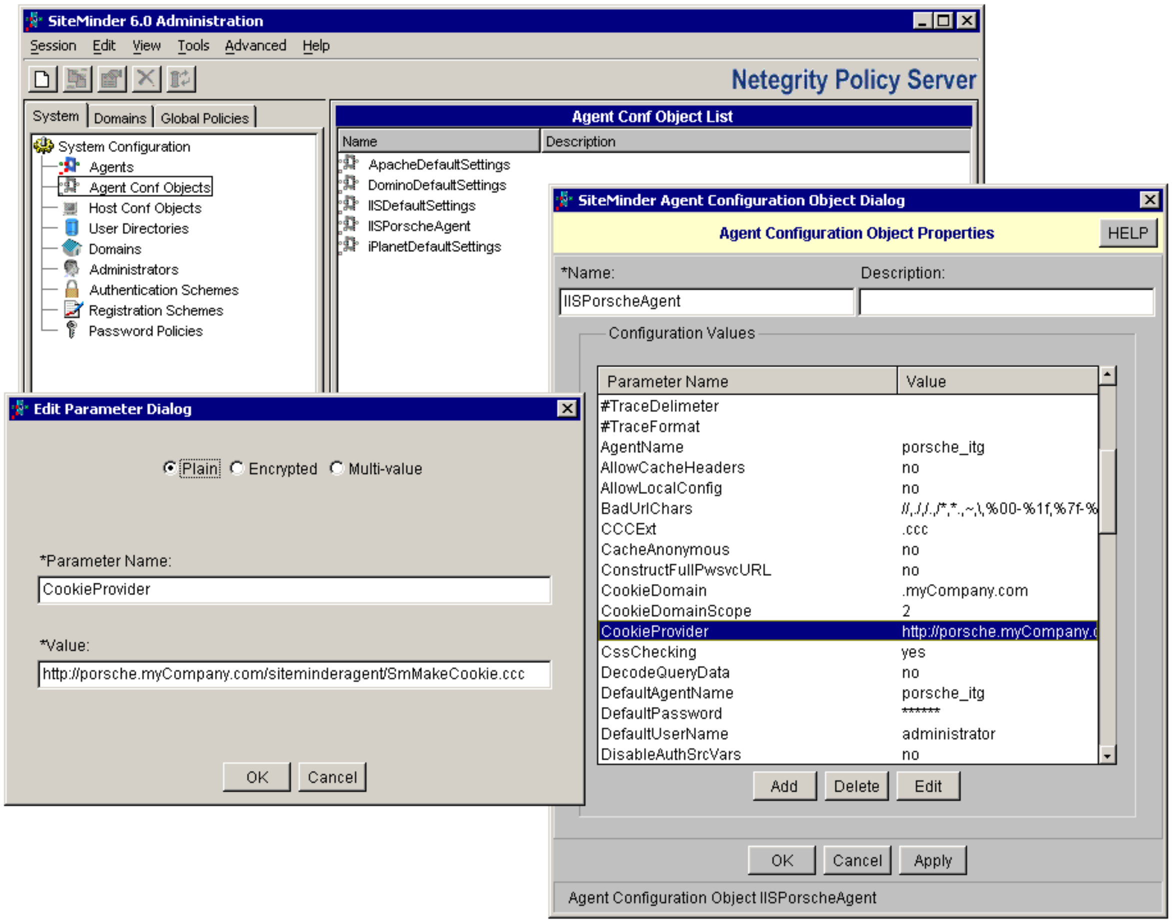
List of Rules and Realms for mercury (porsche)

Name	Resource	Agent	Action		Active	Enabled	Descrip
AllowHTTP	/itg/*		Get,Post,Put			✓	
OnAuthAccept	/itg/*		OnAuthAccept			✓	

1..2 of 2

Figure 4. SiteMinder policy domain

2. To enable SSO, the Cookie Domain and Cookie Provider URL must be defined in the Agent Conf Object for the SiteMinder Web Agent that will authenticate Mercury IT Governance Center Web requests. Cookies are used to track session and idle timeouts. The following figure shows an example agent configuration object for an agent named `porsche_itg`, integrated with Microsoft IIS on a host named `porsche.myCompany.com`.



Edit Parameter Dialog

● Plain ○ Encrypted ○ Multi-value

*Parameter Name: CookieProvider

*Value: http://porsche.myCompany.com/siteminderagent/SmMakeCookie.ccc

SiteMinder Agent Configuration Object Dialog

*Name: IISPorscheAgent

Description:

Configuration Values

Parameter Name	Value
#TraceDelimeter	
#TraceFormat	
AgentName	porsche_itg
AllowCacheHeaders	no
AllowLocalConfig	no
BadUrlChars	//,./,/.,/*,*.,~,\,%00-%1f,%7f-%
CCCExt	.ccc
CacheAnonymous	no
ConstructFullPwsvcURL	no
CookieDomain	.myCompany.com
CookieDomainScope	2
CookieProvider	http://porsche.myCompany.c
CssChecking	yes
DecodeQueryData	no
DefaultAgentName	porsche_itg
DefaultPassword	******
DefaultUserName	administrator
DisableAuthSrcVars	no

Agent Configuration Object IISPorscheAgent

For the CookieProvider, there are different syntaxes for different Web servers.

- For Microsoft IIS, Sun ONE, and Sun Java System:

  ```
  http://<server.domain:port>/siteminderagent/SmMakeCookie.ccc
  ```

- For Apache:

  ```
  http://<server.domain:port>/SmMakeCookie.ccc
  ```

3. Although no specialized responses are required, it is important to understand that Mercury IT Governance Center reads the information SiteMinder automatically injects into the HTTP Request header.

   Mercury IT Governance Center relies on the following user attributes:

   - SM_USER

     For an authenticated user, this is the user distinguished name (DN) as disambiguated by SiteMinder. For an unauthenticated user, this is the user ID as specified by the user in the logon attempt.

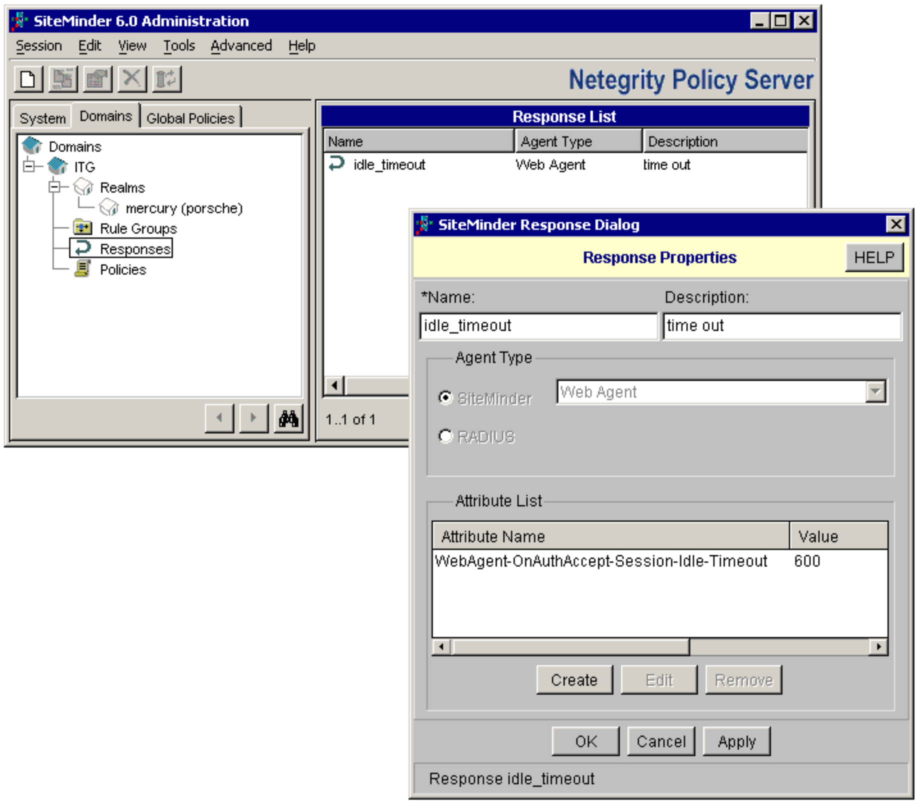
   - SM_SERVERSESSIONID

     This is the session ID of a user who has already authenticated, or the session ID that is going to be assigned to the user upon successful authentication.

   - SM_SERVERSESSIONSPEC

     This is the user's session ticket.

   The following example shows the configuration for a timeout response.



Response List

Name	Agent Type	Description
idle_timeout	Web Agent	time out

*Name: idle_timeout

Description: time out

Agent Type: ● SiteMinder ○ RADIUS — Web Agent

Attribute Name	Value
WebAgent-OnAuthAccept-Session-Idle-Timeout	600

Response idle_timeout

4. All other SiteMinder entities have no corresponding Mercury IT Governance Center settings.

   Consult the SiteMinder documentation for configuration details for those entities.

Step Four: Restart SiteMinder

After making changes to SiteMinder's Policy Server (using the SiteMinder Policy Server User Interface), the Policy Server must be restarted. See the *SiteMinder Policy Server Operations Guide* for more details.

Step Five: Restart Mercury IT Governance Center

After configuring Mercury IT Governance Center and SiteMinder as previously described, the Mercury IT Governance Server must be restarted for the parameter changes to take affect. Restart the Mercury IT Governance Server and log on. In SSO mode, SiteMinder should now be controlling access to Mercury IT Governance Center and users should be logging on from a SiteMinder authentication page. In mixed mode, users log onto Mercury IT Governance Center and SiteMinder authentication is then performed.

Additional Notes

Logoff

If a user logs off Mercury IT Governance Center by using the **Sign Out** button, the SiteMinder session is terminated. If the user attempts to access another SiteMinder-enabled application or Mercury IT Governance Center again, the user is be prompted for username and password information.

Disabled server.conf Parameters

The following `server.conf` parameters are ignored when SiteMinder is controlling access to Mercury IT Governance Center.

- LOGON_TRIES_INTERVAL
- MAX_LOGON_TRIES

Mercury
379 North Whisman Road
Mountain View, CA 94043
Tel: (650) 603-5200
Toll Free: (800) TEST-911
Customer Support: (877) TEST-HLP
Fax: (650) 603-5300

If you have any comments or suggestions regarding this document, please send email to documentation@mercury.com.

updated 03.31.05