CA™ SiteMinder® ERP Agents

Agent Guide for Siebel

r5.6 SP4

CA Product References

This document references the following CA products:

- CA™ SiteMinder®

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 4: Post-installation Options 43

Chapter 5: Troubleshooting 49

Appendix A: NPSEncrypt and NPSVersion Tools 61

Appendix B: Upgrading from a Previous Version 63

Appendix C: Security Adapter Settings 65

Chapter 1: Overview and Architecture

This section contains the following topics:

Background

The Web is becoming the standard interface for newly deployed applications. In an effort to meet the requirements of customers and to enable more widespread use of applications, many leading ERP vendors, including Siebel, have developed either web-based versions of applications or web-based front ends for applications. As a minimum, these web-based front ends provide:

- A standard look and feel for employees
- User authentication
- Basic security (user identity and password)
- Single signon (SSO) capability

SiteMinder enables you to create a centrally managed environment, providing a secure, personalized user experience across all web applications. Through published interfaces, SiteMinder can authenticate users to Siebel. This integration enables the Siebel .COM-based applications to coexist with other portals and web applications, while offering the maximum user experience and benefit.

Increased Security with Tier 2 Integration

Tier 1 Integration

Tier 1 integration typically describes the process in which an underlying application reads and interprets the authentication information passed by SiteMinder so the application (Siebel) can log the user in and create its own session if necessary. Tier 1 integration is the minimum security required to provide SSO. With Tier 1 integration, the underlying application fully trusts that the information was sent from SiteMinder and does no verification. Tier 1 integration can leave important integration issues untouched, such as session timeouts. In Tier 1, the point of trust is entirely within the first tier—the web server. This design is adequate in environments where the application server and web server are located entirely on a trusted network, where security requirements are low to moderate.

Tier 2 Integration

In Tier 2 implementation, the point of trust moves away from the web server and into a more trusted host, in this case the Siebel Object Manager.

In Tier 2 integrations, the application that implements the application logic and security is given the ability to call SiteMinder APIs to communicate with a Policy server, to validate the information that is presented, ostensibly, from the web agent. The API used in this integration is a Siebel-specific API called the Security Adapter API.

Session Linking

Many web-based applications use an independent session management scheme, frequently through the use of a cookie. Therefore, SiteMinder's replay prevention and session management logic may be bypassed. The possibility that the SiteMinder and application sessions could lose synchronization with each other is one of the main security problems when integrating applications that maintain their own sessions.

Due to the enormous value of the data stored in Siebel, CA believes that extra security measures are warranted. The integration documented here includes the SessionLinker component, whose purpose is to prevent such session synchronization issues. SessionLinker is a web server plug-in that monitors the SiteMinder Session ID header and Siebel session cookie. When the two sessions diverge, action is taken to prevent the application from operating until a new session within Siebel is established. By default the action is to destroy the Siebel session, which causes Siebel to create a new session for the correct user.

SessionLinker is used in a number of solutions from CA, and is installed as part of the Siebel agent installation. Further information on SessionLinker is available in *eTrust SiteMinder Agent - SessionLinker Guide*.

Architecture

Components

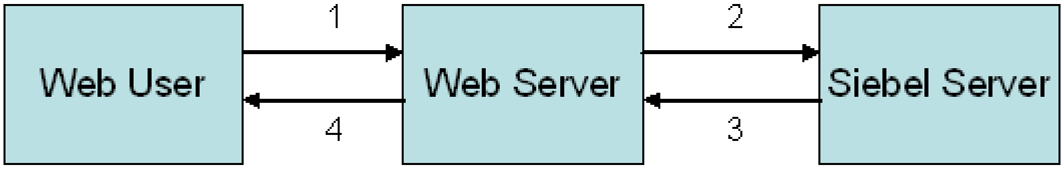
The main components of the eTrust SiteMinder Agent for Siebel are the following:

- A SiteMinder Active Response that generates an "Authentication Ticket" securely identifying the user.
- Siebel templates and a session initiator page.
- A SiteMinder-enabled Siebel Security Adapter conforming to Siebel's Security Adapter API.
- The web server code used for initiating a Siebel session through the Security Adapter.
- A SiteMinder Authentication Scheme that accepts the Authentication tickets generated by the Active Response.
- SessionLinker, which is a web server plug-in that maintains a mapping from the SiteMinder session to the Siebel session to prevent session hijacking attacks.

  For more information, see *eTrust SiteMinder Agent - SessionLinker Guide*, included in the distribution kit.

Conventional Environment

In a conventional Siebel .COM environment, users connect to a web server, which in turn connects to the Siebel Server. The web server collects the user's credentials and transports them to the Siebel Server, which validates them, generates a session cookie, and outputs HTML content to the user. See the following illustration:



Integrated Environment

The flow changes after SiteMinder and the eTrust SIteMinder Agent for Siebel have been added to the environment. Before reaching the Siebel Web Engine on the web server, the web agent either collects and verifies the user's credentials or verifies an existing SiteMinder session by communicating with the Policy server. A single signon ticket is generated and passed through the Siebel server in place of the user's password. The web agent allows the request to be passed on to the Siebel Web Engine.

The Siebel Web Engine passes the request along to the Siebel server – including the username and ticket (in place of a password). The Siebel server, via a customized Security Adapter, communicates with the Policy server to verify the username and ticket.

In an integrated environment, user authorization and data access within Siebel continue to operate exactly as they had without the SSO agent.

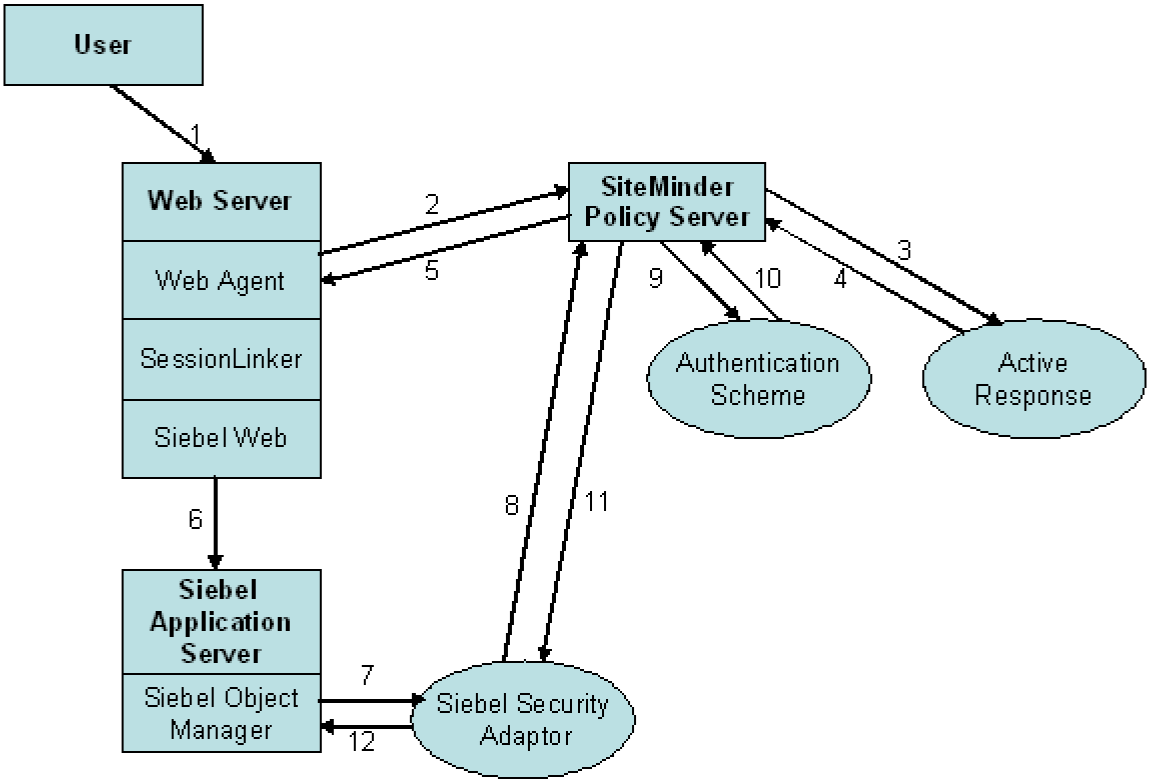
Thick Clients

In addition to single signon through the web, the eTrust SiteMinder agent for Siebel provides support for conventional Siebel thick clients authenticating with username and passwords through the Siebel server. Once eTrust SiteMinder agent for Siebel is installed, user passwords stored in the database are no longer accepted for authentication; instead users need to present their SiteMinder username and password.

Note: Through a number of means, Siebel is enabled to accept the SiteMinder username and password as well as the database username and password. To enable this support, you will need to configure the SiteMinder Policy server to authenticate users out of both the enterprise directory and the Siebel database. Please contact Technical Support for further information if required.

Data Flow

The following illustration shows the various components within an integrated SiteMinder/Siebel installation in more detail. Note that certain components are omitted – for example the user directory, the Siebel database, and additional SiteMinder responses are not shown, nor are the normal IsProtected, Login, and IsAuthorized calls shown.



The steps in the preceding illustration are the following:

1. User makes a request to the Siebel application, for example, http://*machine.domain:port*/service_enu.
2. Web Agent intercepts the request, and uses Policy server to perform SiteMinder Authentication/Authorization.

   Note: If the Siebel responses are configured for a Get-Post rule under the realm protecting the Siebel application in the Policy server, steps 3, 4 and 5 are implemented. Otherwise, control passes to step 6.

3. If SiteMinder authentication by Policy server is successful, the following takes place:
   - Active Response is fired, and generates the Siebel Authentication Ticket, SIEBELTICKET. This authentication ticket is specific to the user accessing the application.
   - Siebel user response is fired, sending a user attribute, whose value maps to a valid Siebel user.
4. Relevant results are provided to the SiteMinder Policy server.
5. Web Agent receives the Active response and Siebel user response from Policy server, and generates the HTTP headers for these responses: HTTP_SIEBELTICKET and HTTP_SIEBELUSER. These responses are sent to the session launching code.
6. The Siebel web component (SWSE) intercepts the request, performs some Siebel-controlled request transformation, and sends the request to Siebel Object Manager using Anonymous user credentials.
   a. On receiving the request from SWSE, Siebel Object Manager checks for the Anonymous user credentials before sending the Siebel Login Web template (SWELogin.swt) customized with the Siebel Agent session launching code back to the SWSE. For verifying the anonymous user credentials, Object manager calls Security Adapter (or Security Provider).

      Security Adapter verifies the passed Anonymous user credentials against the Anonymous username/password credentials specified in the SmSiebelSSO.conf file.

      Once the Anonymous user credentials are successfully verified, the customized SWELogin.swt is fetched and sent to SWSE.

   b. SWSE converts the modified SWELogin.swt into HTML format, and redirects the request to the /SiebelConnector/siebelstartup.asp hosted at the web server. A typical URL format for such a redirection is as follows:

      http://<machine.domainname:Port/SiebelConnector/siebelstartup.asp?URL=http%3A//corsairerp.ca.com/service_enu/start.swe%3FSWECmd%3DStart%26SWEHo%3Dcorsairerp.ca.com

   c. Since the /SiebelConnector/* resources are protected by Policy Server using Siebel SSO Authentication scheme, the web agent validates the user session from the Policy Server.

      Step 3 is carried out, and the Siebel Authentication Ticket (SIEBELTICKET) and SIEBELUSER responses are generated. Web Agent receives the above responses and generates HTTP headers HTTP_SIEBELUSER and HTTP_SIEBELTICKET from them.

      Important! The above two responses get fired irrespective of the fact that they have or have not got fired in the previous step 3. The values generated by these responses in the above two steps are used in the subsequent steps.

   d. siebelstartup.asp converts the URL into a form which SWSE uses to send the username and password to Siebel Object Manager.

      siebelstartup.asp extracts username (SIEBELUSER) and password (Siebel Ticket) from the HTTP request headers, HTTP_SIEBELUSER and HTTP_SIEBELTICKET, and places their values in ‘SWEUsername‘and ‘SWEPassword’ query parameters respectively.

      A sample URL follows:

      http://<machine.domainname:port>/service_enu/start.swe?SWECmd=ExecuteLogin&SWEUserName=test&SWEPassword=%5BNDSEnc%2DD%5DOgUW%2BrRBnuuopBC42MXk%2B6NZgEawPMd67%2FdqK6S4p4w%3D

      Note: The ticket in the above URL is in encoded form.

7. SWSE again sends the request to Siebel Object manager along with the above user credentials. Siebel Object Manager calls Security Adapter or Security Provider and passes the user credentials to it for verification.

8. Security Provider contacts Policy server and accesses the protected resource /SiebelConnector/ (configured in the SmSiebelSSO.conf file) using the user credentials previously received (SIEBELUSER and SIEBELTICKET).

9. Policy server uses the Siebel SSO authentication scheme to verify the user credentials.

   Authentication Scheme verifies the user credentials, SIEBELUSER, and the Siebel authentication Ticket (SIEBELTICKET).

10. The Siebel SSO Authentication scheme results are returned to Policy server.

11. Policy server returns the results of user credentials authentication back to Security Adapter. These results also contain relevant information, such as Siebel Roles and Siebel User Response.
12. Security provider checks the SIEBELUSER response returned previously against the response that was extracted from the HTTP headers. If the user credential authentication is successful and Siebel user responses match, Security Provider reports the results to Siebel Object Manager and creates a Siebel user context for the SIEBELUSER user, which creates a Siebel user session and sends the request to the main application startup page in the SWSE.

More information:

Monitoring the Processing of a Request (see page 55)

Chapter 2: Pre-installation Steps

This section contains the following topics:

System Requirements

The minimum requirements for using the ERP Agent for Siebel are the following:

- SiteMinder Policy server v5.5
- A web server with a SiteMinder web agent v5QMRx
- Siebel version 7.0x, 7.5x, 7.7 or 7.8.2
- Siebel .COM components
- ERP SessionLinker web server plug-in.

For updated information about platform and web server support, see the appropriate Platform Support Matrix available at the http://ca.com/support site.

SessionLinker

To ensure security, SessionLinker must be installed. Although eTrust SiteMinder Agent for Siebel provides single signon to Siebel without SessionLinker, unless SessionLinker is installed, the integration is not secure.

SessionLinker prevents session synchronization issues by monitoring the SiteMInder Session ID header and the Siebel session cookie sent by the user. When the two sessions diverge, action is taken to prevent the application from operating until a new session within Siebel is established. By default, the action is to destroy the existing session, which forces Siebel to create a new session for the correct user. Another possibility is not to destroy the existing session, but instead, to redirect the user to a configured redirect URL.

Note: The configuration parameter for SessionLinker is COOKIE=_sn.

Important! SessionLinker is installed as part of the installation of the Agent for Siebel.

Selecting and Configuring Database Credentials

Once an external authentication system such as SiteMinder is implemented, Siebel is no longer capable of employing the individual user's credentials to connect to the database for the following reasons:

- SiteMinder does not store or expose the user's credentials once the user has been authenticated. This is intentional for security reasons.
- Even if SiteMinder stored the user's credentials, there is no way to know or guarantee that the database would be able to use those credentials – users might authenticate to SiteMinder with certificates, SecurID or other one-time passwords, NTLM or some other authentication scheme which would not be acceptable to the database.

The Siebel Object Manager continues to communicate with the database for all data; however, because users no longer present credentials that the Object Manager can use to connect on their behalf, a special administrative account is necessary. This account's credentials need not be published, and are not used by any person or application other than the Siebel Object Manager.

The use of a generic database user does not in any way impair the ability to audit user activity because Siebel's internal access control, data protection, and audit capabilities continue to operate as with individual user database accounts. A database account should be created and the password set to a complex, non-guessable value.

A benefit of Siebel using a generic database account is that after the eTrust SiteMinder agent for Siebel is installed, individual database accounts are no longer necessary. This relieves the system of the administrative burden of account creation, password maintenance or synchronization, and removal upon termination of employment.

Chapter 3: Installation

This section contains the following topics:

Installing the ERP Agent for Siebel

Installation is performed using the InstallAnywhere software developed by the Macrovision Corporation.

InstallAnywhere can be run in the following modes:

- GUI mode for Windows or UNIX platforms
- Console mode for UNIX platforms

Run InstallAnywhere in GUI Mode

Perform the following procedure to install the ERP for Siebel agent in GUI mode.

To run InstallAnywhere in GUI mode

1. Access the executable file in the installation media, and click it. A window appears, with the caption InstallAnywhere is preparing to Install..., and a progress bar shows you the progress of the operation. When InstallAnywhere is loaded, the CA Siteminder ERP Agents v5.6 SP3 Introduction window appears.

   Note: It is recommended that you quit all programs before continuing with the installation.

2. Click Next. The License Agreement window appears. Read it.
3. Check the "I accept the terms of the License Agreement" check box, and click Next. The Important Information window appears.
4. Read the INSTALLATION NOTES and the DOCUMENTATION NOTES, and click Next. The Select an ERP Agent to Install window appears.

5. Select the radio button next to Siebel Agent, and click Next. The Finding Installed Software window appears.

   Elements of the Siebel agent must be installed on the following servers:

   - Siebel application server
   - Web server, where the Web Agent has been installed.
   - Policy server

   Note: Depending on your configuration, whether the above-mentioned servers are located on the same or on different machines, you will need to run Installer once, twice or three times.

6. Mark the check box(es) next to the relevant software, and click Next. The Choose Install Folder window appears.

7. You must specify the location where you want the Siebel agent to be installed. A default folder C:\Program Files\CA\erpconn is indicated. You may accept the default folder or click Choose, browse to the required folder and click OK. Click Next. The Pre-Installation Summary window appears.

8. Review your selections, and click Previous to change any of your choices or click Install. The installation takes place, and a progress bar appears, indicating the installation of the Merge Module. When the installation is achieved, the Install Complete window appears: a message indicates that the installation is finished. In case errors occurred, a relevant message is issued. You are directed to view the installation log for details.

   Note: The log indicates the following:

   - Whether the installation succeeded or failed
   - The number of successes
   - The number on non-fatal errors
   - The number of fatal errors

9. Click Done to exit InstallAnywhere.

Run InstallAnywhere in Console Mode

Perform the following procedure to install the ERP for Siebel agent in console mode.

To run InstallAnywhere in console mode

1. Run the executable installer file from the command line, using the following command:

   ```
   executable name -i console
   ```

   When InstallAnywhere is loaded, the CA Siteminder ERP Agents v5.6 SP3 Introduction window appears.

   Note: It is recommended that you quit all programs before continuing with the installation.

2. Press the Enter key to continue. The License Agreement window appears. Read it, pressing the Enter key as necessary to view the whole text. At the end of the text, the "I accept the terms of the License Agreement" text appears.

3. Enter **Y** if you accept, and want to continue Installing the ERP Agent, and press the Enter key to continue. The Important Information window appears.

4. Read the INSTALLATION NOTES and the DOCUMENTATION NOTES, pressing Enter as many times as needed to get to the end of the text. The Select an ERP Agent to Install window appears. The options vary according to your platform. For example, on Windows, the options are as follows:

   1- SAP Web Application Server Agent

   2- PeopleSoft Agent

   3- Siebel Agent

   4- SAP ITS Agent

   You are prompted to ENTER THE NUMBER FOR YOUR CHOICE OR PRESS <ENTER> TO ACCEPT THE DEFAULT, WHICH IS MARKED BY AN ARROW.

5. Enter the number that corresponds to Siebel Agent, and press the Enter key. The Finding Installed Software window appears.

   Elements of the Siebel agent must be installed on the following servers:

   1- Siebel application server

   2- Web server, where the Web Agent has been installed.

   3- Policy server

   Note: Depending on your configuration, whether the above-mentioned servers are located on the same or on different machines, you will need to run Installer once, twice or three times.

You are prompted to ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES OR PRESS <ENTER> TO ACCEPT THE DEFAULT, which is marked by an arrow.

6. Enter your selection, for example, 1,3. The Choose Install Folder appears.
7. You must specify the location where you want the Siebel agent to be installed. A default folder, *Path to your home directory*/CA/erpconn, is indicated. You may accept the default folder and press the Enter key or enter the full path to the required folder. The Pre-Installation Summary window appears.
8. Review your selections, and press the Enter key to Install. The installation takes place, and a progress bar appears. When the installation is complete, a confirmation message is issued. In case errors occurred, a relevant message is issued. You are directed to view the installation log for details.

   Note: The log indicates the following:

   - Whether the installation succeeded or failed
   - The number of successes
   - The number on non-fatal errors
   - The number of fatal errors
9. Press the Enter key to exit InstallAnywhere.

Installing on the Policy Server

Install the Authentication Scheme

Perform the following procedure to install the authentication scheme.

To install the Authentication Scheme

1. Open the SiteMinder Policy server user interface and log in as a SiteMinder administrator.
2. Copy the Authentication Scheme library, SiebelSSOAuth, from the *Siebel Agent Installation Directory*/siebel/bin to the bin or lib directory in the Policy server.

3. Right-click Authentication Schemes in the left tab and click Create Authentication Scheme. Supply the following values in the SiteMinder Authentication Scheme Dialog window (also see *eTrust Policy Design Guide*):

Keyword	**Value**
Description	Siebel SSO Agent Authentication Scheme (When you have completed the installation, you may optionally disable password acceptance by this Authentication Scheme. See Disabling Password Acceptance (see page 43).)
Authentication Scheme Type	Custom Template
Protection Level	5 In general, this value should be NO HIGHER than the value for any other HTML-based authentication scheme supporting username and password authentication.
Password Policies	Checkmark—if Password Services is in use
Library	SiebelSSOAuth The Solaris and HP-UX platforms are case sensitive.
Secret	Enter a secret known only by the SiteMinder administrator.
Confirm Secret	Re-enter the secret to confirm.

Keyword	**Value**
Parameter	A configuration string constructed from the following parameters separated by a semicolon: ■ FCC=*<URL for a login form>* The FCC is the HTML page that collects credentials. This might be the URL that is used in another HTML-based authentication scheme. If you are unsure of the location of an appropriate FCC file on your system, and set the value for the FCC to: /siteminderagent/forms/login.fcc This displays the default SiteMinder login form. ■ ATTR=*<User attribute>* *<User attribute>* is the username that Siebel uses. The default is the UID. ■ PERIOD=*<Ticket Acceptance Period>* The value, in seconds, for the maximum amount of time between the moment the SSO ticket is created and the moment a user might present a ticket. In general, this will be a very short period of approximately 10 to 20 seconds. The default is 60. The order of the individual components in the parameter string is not important.
Enable this scheme…:	Leave this box unchecked

Create SiteMinder Policies

The creation of SiteMinder Policies will protect Siebel applications and provide the framework for single signon (SSO). For additional information on any of these steps, see *eTrust Policy Design Guide*.

To create SiteMinder Policies

1. Create a Policy Domain to contain all of the Siebel Applications.
2. Within the Policy Domain, create one realm for each Siebel application to be integrated. For example, create a /sales/ realm and a /purchase/ realm. Make sure the Agent Object used to protect this realm is enabled to Support 4.x agents, which is done by clicking the 4.x check box in the Agent Object dialog box.
3. In each realm create two rules:
   - A rule with the actions Get and Post for the * resource
   - A rule with the Authentication event OnAuthAccept
4. For each of the realms, make sure to select the Authentication Scheme you created in Install the Authentication Scheme (see page 22).
5. Create a response for SessionLinker. Siebel v7 uses _sn as the name of the cookie. Thus, the correct configuration string for the SessionLinker is: "COOKIE=_sn"
6. Create a policy:
   a. Add appropriate users.
   b. Add both rules in each realm.
   c. Link the SessionLinker response to the OnAuthAccept rule.
7. Create a Realm within the same Policy Domain for the SiteMinder Agent startup URL (/SiebelConnector/). Make sure the Agent Object used to protect this realm is enabled to Support 4.x agents (by clicking the 4.x check box on the Agent Object dialog box).
8. Make sure to select the Authentication Scheme you created in Install the Authentication Scheme (see page 22).
9. In the SiteMinder Agent Startup realm, create two rules:
   - One rule with the actions Get and Post for the * resource
   - One rule with the Authentication event OnAuthAccept
10. Create a response (for example, Siebel connector response).

11. In the SiteMinder Response Attribute Editor, create two responses for the WebAgent-HTTP-Header-Variable attribute:

    - A response for the username. Specify the following values:

Attribute Kind	User Attribute
Variable Name	SIEBELUSER
Attribute Name	uid This value should be the attribute used by the directory to locate users (whatever user attribute contains the Siebel username, typically uid). To determine the correct value, examine the user directory configuration and the DN lookup start and end.

    - A response for the single signon (SSO) ticket. Specify the following values:

Attribute Kind	Active Response
Variable Name	Leave this blank
Library Name	SiebelSSOAuth
Function Name	GetSSO Ticket In some environments, the function name should be GETSSOTicketWithDN. See Upgrade and Enable the New Encryption Ticket (see page 64).

Parameters	Enter a string constructed from the following values: ▪ ATTR=*<User attribute>* *<User attribute>* is the username that Siebel uses. This is the value you entered in the Authentication Scheme's configuration string (Step 3 in Install the Authentication Scheme (see page 22)). ▪ SECRET=*<Secret String>* This value should be same as the value entered in the Secret field of the Authentication Scheme. This parameter is mandatory. If you want to encrypt the secret, use the NPSEncrypt tool. See NPSEncrypt Tool (see page 61). Parameters can be in any order, separated by semicolons.
Attribute Caching	Recalculate the value to a number that is less than the PERIOD setting in the Authentication Scheme, typically 60 seconds or less. See also: ▪ Step 3 in Install the Authentication Scheme (see page 22). ▪ Ticket Outside Acceptance Window (see page 51).

1. Click the Advanced tab and remove the equal sign (=), which, if it exists, is found before the less than (<) sign.
2. Create a Policy binding the OnAuthAccept rule with the response for all users that should have access to Siebel.

Installing on the Web Server

Install the Startup Page

Perform the following procedure to install the startup page:

To install the startup page

1. Locate the folder that is appropriate for the web server you are using, from the following list:
   - *Siebel Agent installation folder*\Siebel\Config\WWW\ASP (for Microsoft IIS)
   - *Siebel Agent installation folder*\Siebel\Config\WWW\CGI (for IBM HTTP Server (IHS))
   - *Siebel Agent installation folder*\Siebel\Config\WWW\JSP (for Sun ONE)
2. Copy the entire contents of the directory to a new folder named "SiebelConnector" within the web server's document root directory, for example:
   C:\Inetpub\WWWRoot (for Microsoft IIS)
3. For the IBM HTTP server, you might need to do the following:
   a. Give Execute permissions to the perl (.pl) files in the SiebelConnector folder.
   b. Define the ExecCGI option for the SiebelConnector folder. Specify the cgi handler for the .pl files. The following sample configuration might help in defining in the httpd.conf file:

```
Alias /SiebelConnector/ "home/ngtyerpc/apps/IHS/htdocs/en_US/SiebelConnector/"
<Directory "/home/ngtyerpc/apps/IHS/htdocs/en_US/SiebelConnector">
        AllowOverride None
        Options None EXecCGI
        Order allow,deny
        Allow from all
</Directory>
AddHandler cgi-script .pl
```

c. If you use the Siebel 7.5.3 web server extensions on IHS 2.0.41.1 with prefix PQ73029, make sure the following links have been created in the *IHS-Root*/lib folder:

```
ln –s libapr-0.so libapr.so
ln –s libaprutil-0.so libaprutil.so
```

d. If you use the startapa and stopapa scripts to start and stop the IHS web server, modify the scripts to append the path of the SWSE bin folder to the *LIBPATH* variable rather than preceding it.

Do not change the files in any way. After the installation is operating properly, you may customize the files while preserving the functionality. Some of the files contain comments to help you customize the files.

Verify SiteMinder Responses

To verify responses, open a web browser and access the relevant URL page, depending on your web server:

```
http://<machine.domain.com>/SiebelConnector/test.asp
http://<machine.domain.com>/SiebelConnector/test.jsp
http://<machine.domain.com>/SiebelConnector/test.pl
```

When loaded, this page verifies the contents of the SiteMinder responses for the Siebel Username and Ticket.

- The SiteMinder login page should appear. If the SiteMinder login page does not appear, stop the installation and verify the SiteMinder Policies. See Creating SiteMinder Policies (see page 25) to determine the cause of the problem before continuing with the installation.
- The Siebel Connector Test Page appears. Do one of the following:
  - If the page has green OK indicators and a message that no errors are found, verification is successful. Continue with the installation by going to Installing on the Object Manager (see page 30).
  - If the text has a red background and the description of a problem, verification is unsuccessful. Resolve the problem by following the suggestion on the test page. Rerun the test page after fixing the problem.

Installing on the Object Manager

Security Adapter File Names

eTrust SiteMinder Agent for Siebel supports several versions of Security Adapter. There are two sets of files (one for v7.0.x and another for both v7.5.x, v7.7 and 7.8.2), which are installed in the *Siebel Agent installation folder*\Siebel\bin folder.

Important! Do not change the file names to suit your version.

Files for v7.0.x

Files differ according to the platform:

AIX and **Solaris:**	libSmSecurityProvider.so ProviderTest libsmagentapi.so
HP-UX:	Version 7.0.x is not supported on HP-UX.
Windows:	SmSecurityProvider.dll ProviderTest.exe SmAgentAPI.dll

Files for v7.5.x, v7.7 and v7.8.2

Files differ according to the platform. File names containing the number 75 are used for versions v7.5.x, v7.7 and v7.8.2.

AIX and **Solaris:**	libSmSecurityProvider75.so ProviderTest75 libsmagentapi.so
HP-UX:	libSmSecurityProvider75.sl ProviderTest75 libsmagentapi.sl
Windows:	SmSecurityProvider75.dll ProviderTest75.exe SmAgentAPI.dll

Install Security Adapter

Perform the following procedure to install Security Adapter.

To install Security Adapter

1. Copy the files from the folder *Siebel Agent Installation folder*\Siebel\bin\ to the Siebel Server installation's bin directory. (See the list of files in Security Adapter File Names (see page 30).)
2. This step differs according to the Agent for Siebel version:
   - For v7.7 or v7.8.2, copy the following initialization and configuration files from the *Siebel Agent Installation folder*\Siebel\config\SecurityAdapter folder to the Siebel Server installation's bin directory:

     ```
     \SmSiebelSSO.ini
     \SmSiebelSSO.conf
     ```

   - For v7.0.x and v7.5.x, copy only the configuration file from the *Siebel Agent Installation folder*\Siebel\config\SecurityAdapter folder to the Siebel Server installation's bin directory:

     ```
     \SmSiebelSSO.conf
     ```

Configuring Security Adapter

Perform the following steps to configure Security Adapter:

1. Edit the sample SmSiebelSSO.conf file that you copied in Step 3 of Installing Security Adapter. Use parameters appropriate for your environment. See Sample SmSiebelSSO.conf File (see page 31).
2. If you make changes to this configuration file after Security Adapter is enabled in Siebel, you must restart Object Manager.

Sample SmSiebelSSO.conf File

Configuration parameters are listed in Commonly Used Configuration File Settings (see page 32). Additional details can be found inSecurity Adapter Settings (see page 65).

Security Adapter ignores comments (lines beginning with the # character) and unrecognized settings.

```
# Feel free to edit this file at will

# Where should the log data go?
LogFile=c:/logs/Test.log
```

```
# Log level is an integer between 0 and 3
# Level     Meaning
#  0       None
#  1       Errors
#  2       Information
#  3       Debug
LogLevel=3
# These settings dictate how you communicate with the Policy server

PolicyServer=127.0.0.1
AgentName=siebel1
SharedSecret=secret
Resource=/SiebelConnector/

# And finally how do you talk to the Database?
DatabaseUser=sadmin
DatabasePassword=sadmin
```

Commonly Used Configuration File Settings

Modify the parameters in the SmSiebelSSO.conf file according to your environment requirements. Common settings are listed in the table that follows. For additional information on configuration file settings, see Security Adapter Settings (see page 65).

Parameter	Description
LogFile	(Optional) Specifies the full path to the log file. Make sure the folder containing the log file exists. **Example** (on Windows)**:** C:\logs\connector.log
LogLevel	(Optional) Specifies the level of logging. Values are the following: ▪ 0 No logging ▪ 1 Errors ▪ 2 Information ▪ 3 Debug For production, CA recommends that you set LogLevel to 1. If a value is not specified, log level 0 is the default.

Parameter	Description
PolicyServer	Specifies one or more Policy server IP addresses with which the eTrust SiteMinder Agent for Siebel communicates when validating sessions. Specify an IP address. **Example:** 127.0.0.1 If you specify multiple Policy server IP addresses, separate them with a space. If the Policy server uses ports other than the default port, enter the ports *after* the Policy server IP, and separate them with a comma (,) in the order of Acct, Auth, and Az ports (Accounting, Authentication, and Authorization). If you do not specify the ports, the default port values of 44441, 44442 and 44443 are assumed for the Acct, Auth, and Az servers respectively. **Note:** Either specify all of the ports for a particular Policy server IP or specify none. **Example** (IP specification of multiple policy servers with specific ports)**:** 127.0.0.1,44441,44442,44443 192.168.122.1,44441,44442,44443
EnableFailover	By default Security Adapter uses all the Policy servers in a round robin mode. When this parameter is set to the value Yes, the Policy servers are used in a Failover mode instead.
AgentName	Specifies the agent name, as set in the WebAgent.conf file, used by the eTrust SiteMinder Agent for Siebel login module. **Example:** siebel1 The value of this parameter must match the agent name used in the policies described in Creating SiteMinder Policies (see page 25).
SharedSecret	Specifies the shared secret for AgentName. This is the shared secret as configured in the Web Agent. **Example:** secret You may encrypt this value with the NPSEncrypt tool (NPSEncrypt.exe), which is installed in the *Siebel Agent Installer folder*\Siebel\Tools folder, while you cannot copy and paste a value encrypted with the Web Agent's encryption tools.

Parameter	Description
Resource	Specifies a resource protected with the eTrust SiteMinder Agent for Siebel's Authentication Scheme. This must be the same as the realm protected in Step 7 of the To create SiteMinder Policies procedure in Creating SiteMinder Policies (see page 25). **Example:** /SiebelConnector/
Action	(Optional) Specifies the desired action on the Resource. Typically valid actions are GET and POST. The default is GET.
DatabaseUser DatabasePassword	Once the eTrust SiteMinder Agent for Siebel is installed, a generic user is used to connect to the database. This username and password are used in this capacity. As with SharedSecret the value of DatabasePassword may be encrypted with NPSEncrypt. **Example:** sadmin

Initialization File Settings for v7.7 and v7.8.2

For v7.7 or v7.8.2, you copied the initialization file (SmSiebelSSO.ini) from the *Siebel Agent Installation folder*\config\SecurityAdapter folder (see Installing Security Adapter). Modify the parameters in the SmSiebelSSO.ini file according to your environment requirements. Common settings are listed in the following table.

Parameter	Description
[SiteMinder]	This value should match the config section name specified in Step 3 of the To create a named subsystem procedure in Creating Named Subsystem for Custom Security Adapter (see page 37). **Example:** [SiteMinder]
ConfigFileName	The absolute path to the SmSiebelSSO.conf file. **Example** (on Windows)**:** d:\siebel\bin\enu\SmSiebelSSO.conf

Executing the Security Adapter Test

After you modify the configuration file (Configuring Security Adapter (see page 31)), test Security Adapter by verifying the installation and the settings in the configuration file (SmSiebelSSO.conf).

To execute the Security Adapter test

1. Run the ProviderTest program (which you installed in Step 2 in Security Adapter File Names (see page 30)). The output from the execution is shown in the following code:

```
C:\>providertest
Enter username: dsherman
Enter password: password
Testing provider with username 'dsherman' and password 'password'
Loading library... OK
Finding entry point... OK
enter Config File: test.conf
Calling SecurityLogin()...OK
Return code is OK
Test 1: GetUsername()
    Username: dsherman
Test 2: GetAccountStatus()
    Account state: ACTIVE
Test 3: GetCredentials()
    pCred->m_pType:
    pCred->m_pUsername:  DBUser
    pCred->m_pPassword:  10 characters long
Test 4: GetUserInfo:
    m_accountStatus: ACTIVE
    m_bPasswordSet: 0
    m_pCredentialsArray
        #:    Type |  Username |  Password
        ------------------------------
        0:         |   DBUser |  10 chars
    m_pNewUsername: (null)
    m_p_Password: (null)
Test 5: GetRoles()
    GetRoles returned SecurityErrOK
    Role 00: A
    Role 01: B
    Role 02: C
    Role 03: D
    Total: 4 roles
```

2. If ProviderTest finds a problem, it displays messages such as Provider test failed or pUser is NULL, or something similar. Check the log file specified in the configuration file. If no log file is generated, check if the path to the configuration file is correct and that the user running ProviderTest has permission to open that file.
3. When the test is successful, enable the Security Adapter:
   - Enabling v7.0.x and v7.5.x Security Adapter (see page 36).
   - Enabling v7.7 and v7.8.2 Security Adapter (see page 37)

Enable v7.0.x and v7.5.x Security Adapter

These steps are only for v7.0.x and v7.5.x of Security Adapter. If you have v7.7 or v7.8.2, see Enabling v7.7 and v7.8.2 Security Adapter (see page 37).

For each Siebel application that will use the eTrust SiteMinder Agent for Siebel, edit the appropriate configuration file on the Siebel Application Server, for example, the file esales.cfg for E-Sales. Refer to the Siebel documentation to determine the appropriate configuration file. A sample .cfg file is located in the *Siebel Agent Installation folder*\Siebel\config\siebsrvr\ExampleConfigFile folder.

To enable versions 7.0.x and 7.5.x of Security Adapter

1. Make sure you have completed the steps in Executing the Security Adapter Test (see page 35).
2. Refer to the Siebel documentation to determine the appropriate configuration file.

   A sample configuration file, which you can use for reference, is located in the following folder:

   Siebel Agent Installation folder\Siebel\Config\siebsrvr\ExampleConfigFile\sample_esales.cfg
3. Within your Siebel configuration file locate the line:
   ```
   ;SecurityAdapter = LDAP
   ```
4. Below that line, add the following line:
   ```
   SecurityAdapter = SiteMinder
   ```
5. Locate the lines:
   ```
   [SecurityAdapters]
   LDAP = LDAP
   ```
6. Below those lines, add the following line:
   ```
   SiteMinder = SiteMinder
   ```

7. Scroll to the end of the file and add a new section similar to the following section (for your platform), updating the file paths as appropriate for your environment:

   ```
   [SiteMinder]
   DllName = C:\Program Files\CA\Siebel Connector\SmSecurityProvider.dll
   ConfigFile = C:\Program Files\CA\Siebel Connector\SmSiebelSSO.conf
   ```

   The DllName setting should be the full path to the DLL or shared object. For UNIX, the full path should be to the corresponding library. If the installation is under Siebel Security Adapter v7.5.x, the file name should contain the number 75, for example SmSecurityProvider75.

8. Restart Siebel Object Manager after you modify the configuration files. After restarting Siebel Object Manager, all authentication attempts will pass through the eTrust SiteMinder agent for Siebel to the SiteMinder Policy server.

9. You are now ready to activate Security Adapter. See Activating v7.0.x and v7.5.x Security Adapter (see page 39).

Enabling v7.7 and v7.8.2 Security Adapter

The following steps apply to Security Adapters v7.7 and v7.8.2:

- Create named Subsystem for Custom Security Adapter (see page 37)
- Configure the Components to Use Custom Adapter (see page 39)

Create Named Subsystem for Custom Security Adapter

Perform the following procedure to create a named subsystem for Custom Security Adapter.

To create a named subsystem

1. Log in to the server manager using the following command:

   ```
   srvrmgr parameters
   ```

   The parameters include the following:

   - /e *ent_name*
   - /g *gtwy*
   - /s *srvr*
   - /u *username*
   - /p *password*

2. Create a named subsystem, SiteMinderSecAdpt, for the custom Security Adapter (sample output is shown in the following table), by using the following commands:

   ```
   srvrmgr:srvr>create named subsystem SiteMinderSecAdpt for subsystem InfraSecAdpt_CUSTOM
   srvrmgr:srvr>list param for named subsystem SiteMinderSecAdpt
   ```

PA ALIAS	PA VALUE
CustomSecAdpt_CRC	********
CustomSecAdpt_SecAdptD11Name	
ConfigFileName	
CustomSecAdpt_HashAlgorithm	RSASHA1
CustomSecAdpt_HashDBPwd	False
CustomSecAdpt_HashUserPwd	False
CustomSecAdpt_PropagateChange	False
ConfigSectionName	
CustomSecAdpt_SingleSignOn	False
CustomSecAdpt_TrustToken	********
CustomSecAdpt_UseAdapterUsername	False
11 rows returned.	

3. Modify the named subsystem created in Step 2 so that it uses the SiteMinder security provider library and configuration files, using the following commands:

   ```
   srvrmgr:srvr> change param CustomSecAdpt_SecAdptDllName=SmSecurityProvider75 for named subsystem SiteMinderSecAdpt
   srvrmgr:srvr> change param ConfigFileName=d:\siebel\bin\enu\SmSiebelSSO.ini for named subsystem SiteMinderSecAdpt
   ```

   Note: The absolute path of the SmSiebelSSO.ini file must be specified in this command to modify the ConfigFileName.

   ```
   srvrmgr:srvr> change param ConfigSectionName=SiteMinder for named subsystem SiteMinderSecAdpt
   ```

   Note: The section name, SiteMinder, in this command to modify the ConfigSectionName, must match the section name defined in the SmSiebelSSO.ini file.

   ```
   srvrmgr:srvr> list param for named subsystem SiteMinderSecAdpt
   ```

   A sample output is shown in the following table:

PA ALIAS	PA VALUE
CustomSecAdpt_CRC	********

```
CustomSecAdpt_SecAdptD11Name          SmSecurityProvider75
ConfigFileName                        d:\siebel\bin\enu\
CustomSecAdpt_HashAlgorithm           RSASHA1
CustomSecAdpt_HashDBPwd               False
CustomSecAdpt_HashUserPwd             False
CustomSecAdpt_PropagateChange         False
ConfigSectionName                     SiteMinder
CustomSecAdpt_SingleSignOn            False
CustomSecAdpt_TrustToken              ********
CustomSecAdpt_UseAdapterUsername      False
11 rows returned.
```

Configure the Components to Use Custom Adapter

Perform the following steps to configure the server components.

To configure the server components

1. Execute the following commands for the desired server component, such as esales_enu Object Manager:

   ```
   srvrmgr:srvr > change param secadptname=SiteMinderSecAdpt for comp eSalesObjMgr_enu
   srvrmgr:srvr > change param secadptmode=CUSTOM for comp eSalesObjMgr_enu
   ```

2. Restart the Siebel Server.

Activate v7.0.x or v7.5.x Security Adapter

The following steps are required for v7.0.x and v7.5.x only.

To activate v7.0x or v7.5x Security Adapter

1. Make sure you have Siebel Administrative rights.
2. From within the Siebel application select View, and Site Map.
3. In the Site Map, select the Server Administration section, and then Components.
4. On the Server Components tab, execute a search for the Component Name (application) to which you want to add Security Adapter, for example, eSales*.

5. Select the Component Parameters tab from the lower window, and query for a Parameter of SecurityAdapter.
6. Change the Current Value to SiteMinder. This changes the Value on Restart.

   Note: The Effective Immed check does not indicate that the setting takes effect immediately; the server must be restarted for this change to take effect.
7. Restart Siebel Object Manager.

Configure External Applications to Use SWELogin.swt

By default, customer-facing applications (such as eSales) use a different login view than the SWELogin.swt required by the SiteMinder Agent. (Internal Seibel applications, such as CallCenter, use SWELogin.swt by default.) Perform the following procedure to configure other applications to use SWELogin.swt.

To configure external applications to use SWELogin.swt as their login view

1. Open the eapps.cfg file present in *Siebel_SWSE_install*/bin folder.
2. Search the *application_language* file (such as esales_enu) for the string corresponding to the application for which the SWELogin.swt needs to be enabled and remove or comment the “startcommand” entry defined under it.
3. Restart the Web Server.
4. Open the *application*.cfg file (such as esales.cfg) from *Siebel_Server_Root*/bin/enu folder. Search for and comment the "LoginView = Login View" entry.
5. Restart the Siebel application server.

Test Security Adapter Within Siebel

Perform the following procedure to test Security Adapter within Siebel.

To test Security Adapter within Siebel

1. Select a user whose password within Siebel is different from the SiteMinder password.
2. After the server is restarted, open a web browser and access the selected application. For example, select the application esales by specifying:

   http://*machine.domain.com*/esales/

   Be sure to include the full domain name so that the browser accepts SiteMinder's cookies. If a SiteMinder session has not yet been established, the SiteMinder login screen appears, Enter a valid username and password and complete the SiteMinder login process.
3. Verify the status of the operation, and perform the following:
   - If SiteMinder authentication is successful, the Siebel login screen appears. Provide the same credentials used to log into SiteMinder and submit the form. Access to Siebel is granted. Close the web browser and open it again to destroy the existing SiteMinder and Siebel sessions.
   - If SiteMinder authentication is unsuccessful, the Siebel login page *does not appear* and a Server Busy message is displayed. This could indicate that Security Adapter has not been installed, configured or activated correctly. Repeat the steps described in the following sections:

     Security Adapter File Names (see page 30)

     Configuring Security Adapter (see page 31)

     Executing the Security Adapter Test (see page 35).

More information:

Agent API Not Loaded (see page 52)

Test Single Signon

When you verify that Security Adapter and Authentication Scheme are functioning correctly, SSO should also succeed.

To test single signon

1. Access the relevant URL, depending on your server:

   http://*machine.domain.com*/SiebelConnector/testsso.asp

   http://*machine.domain.com*/SiebelConnector/testsso.jsp

   http://*machine.domain.com*/SiebelConnector/testsso.pl

2. Enter the correct URL for the Siebel.COM application (for example, esales), which you configured in either Enabling v7.0.x and v7.5.x Security Adapter (see page 36) or Enabling v7.7 and v7.8.2 Security Adapter (see page 37).
3. Click Test Single Sign On. No additional login pages need to be presented and the application startup page automatically appears.
4. If single signon is successful, go to Directing Users Through the SSO Process (see page 42).
5. If single signon is unsuccessful, examine the Security Adapter log file and the relevant Policy server log (either Authentication or Authorization) for additional information. The most common causes for failure are the following:
   - SiteMinder responses (tested in Verify SiteMinder Responses (see page 29))
   - Failing to select the Siebel SSO Auth Scheme for the realm used by Security Adapter (tested in Step 11 in Create SiteMinder Policies (see page 25)). Re-check the Policy server configuration.

Direct Users Through the SSO Process

Once single signon is functioning correctly, you can have all users automatically directed through the single signon process rather than presenting the Siebel login page.

To direct users through the SSO process

1. Locate the Siebel Login web template file:
   Siebel Agent Installation folder/Config/siebsrvr/Webtempl/SWELogin.swt
2. Copy it to the web templates (Webtempl) directory of the Siebel Server.
3. Modify the file to work with your web server (it is currently set up to work with .asp files). If you use .jsp or .pl files, open the SWELogin.swt file and change the instances of asp to jsp or pl respectively.

Chapter 4: Post-installation Options

The post-installation steps are optional.

This section contains the following topics:

Disabling Password Acceptance

After completing the installation, you may select to disable the acceptance of passwords by the Authentication Scheme. Currently, the installation is configured in a way that allows a user, accessing the Siebel Object Manager, to provide a username and either a password or a single signon token generated through Active Response.

In many environments, Object Manager can be accessed through the Siebel Web Engine (SWE) components or via a thick client. Therefore, disabling password acceptance by the Authentication Scheme is valuable and necessary.

In other customer environments, once SiteMinder is enabled, it mediates all access to the system; passwords are unacceptable and are considered a security risk. In these cases, access by a password can easily be disabled.

Once you disable the acceptance of passwords by the Authentication Scheme, the following occurs:

- Any realm protected by this Authentication Scheme will no longer accept a password, resulting in portions of the web site no longer accepting users.
- ProviderTest (or ProviderTest75) itself can fail, rendering troubleshooting extremely difficult.

Preventing Security Adapter from accepting passwords includes the following:

1. Make sure your environment is working properly.
2. Consider the implications and possibly create additional realms, rules and policies within SiteMinder exclusively for use by Security Adapter. If you have any questions, contact CA for assistance.
3. Add the following text to the existing parameter for the SiebelSSOAuth Authentication Scheme:

   ```
   ;AcceptPassword=No
   ```

More information:

Install the Authentication Scheme (see page 22)

Providing Siebel Roles from SiteMinder Policies

In addition to supporting single signon and authentication, eTrust SiteMinder Agent for Siebel has the ability to provide Siebel with a set of roles and responsibilities for individual users. The roles and responsibilities to be presented are collected from SiteMinder responses by the connector at login time and are presented to the Siebel server whenever needed.

Note: The connector can add to a user's privileges but cannot remove roles and responsibilities configured within Siebel itself. This is an important consideration for privilege management because security can be compromised if roles and responsibilities are administered in both the enterprise directory and Siebel.

To provide roles to Siebel via the connector, create responses (and appropriate values) with the name SIEBELROLE. The connector does not attempt to validate the roles provided to Siebel; it simply passes to Siebel the values provided as responses for Siebel’s use.

Using Load Balanced Web Servers with Siebel

eTrust SiteMinder Agent for Siebel does not impart any additional restrictions on load balancing. For information on configuring a web load balancer in a Siebel environment, see the Siebel documentation.

Security Adapter is a SiteMinder Agent in its own right. Security Adapter is independent of the Web Agent and should not use the same agent name as any of the Web Agents in the environment.

When you configure policies, create an agent group, which should contain all of the Web Agents that will be protecting Siebel, and add the Security Adapter agents to that Agent Group.

To understand why each Security Adapter has its own agent name, consider the following environment as a similar case:

1. The SiteMinder Secure Proxy Server (SPS) can be used as a front-end proxy to a number of web servers. Each web server can have a SiteMinder Web Agent installed. Each Web Agent is configured to use its own name; the fact that the user passed through the SPS makes no difference in the Web Agent configuration.
2. When this environment includes more than one SPS in a load balanced configuration, the Web Agent configuration remains unchanged; it makes no difference to the Web Agents which SPS instance sent the request to the web server, or even that the SPS was involved.

Using a number of web servers in front of a single Siebel Object Manager with the eTrust SiteMinder Agent for Siebel is virtually identical to the SPS and Web Agent environment described above. Access permissions to the Siebel Object Manager, protected by SiteMinder Security Adapter, are predicated upon the policies and it makes no difference what web server was used to reach Object Manager.

Use a Different Authentication Scheme

You may use an authentication scheme other than Siebel SSO Authentication Scheme. For example, you might use SecurID or Certificates instead of the username and password-based authentication.

The following steps assume that the Web Agent and Siebel Security Adapter use different agent names and are in a common Agent Group. If both the Web Agent and Security Adapter are configured to use the same agent name, one of the agent names will need to be changed and the relevant system restarted.

To use a different authentication scheme

1. Open the SiteMinder Policy Management GUI and create another realm.
   a. For the agent, select the agent name used by Security Adapter.
   b. For the Authentication Scheme, select the Siebel SSO Auth scheme you already created.
   c. For the resource, enter /SecurityAdapter/
2. Create a rule for GET and POST to the resource *.
3. Create a Policy binding the GET/POST rule to the existing response for all users that should gain access to Siebel.

4. In the SmSiebelSSO.conf file, change the resource to:

   /SecurityAdapter/

5. Run ProviderTest (or ProviderTest75) to verify the new configuration.
6. Restart Siebel Object Manager.
7. Change the realm for the Web Agent to use the desired Authentication Scheme.
8. Remove the Security Adapter's realm from the Agent Group.
9. Retest the environment, paying particular attention to the log files.

Once the system is working properly, consider changing the Authentication Scheme's configuration to prevent it from accepting passwords.

More information:

Disabling Password Acceptance (see page 43)

Supporting Multiple Siebel User Attribute Responses for Siebel 7.8

In the current design of the application, only one of the user attributes, such as uid, can be passed via the Siebel User attribute response header, SIEBELUSER.

The new parameter, UsernameHeaders, in the SmSiebelSSO.conf file, enables the SiteMinder agent for Siebel to support multiple Siebel User attribute response headers, as follows:

- In the SmSiebelSSO.conf file, set the UsernameHeaders parameter to multiple Siebel user response names in a comma-separated list, for example SIEBELUSER1,SIEBELUSER2, ...
- In the Policy server, create Siebel user attribute responses that are identical to the names entered as values in the UsernameHeaders A different user attribute can be configured for each Siebel user attribute response.

  Note: For the multiple user attribute functionality to be used correctly with the SiteMinder agent for Siebel, for any user request only one of the Siebel user attribute responses configured in Policy server should carry a value. All other Siebel user attribute responses should be empty for the signing in user.

- Based on your environment, modify the following Siebel agent web server files to check for the Siebel user response, which is carrying a value, and pass a valid non-null and non-empty value to the SWEUsername parameter in URL before redirection:
  - functions.inc, for ASP-based files.
  - getheaders.jsp, for JSP-based files.
  - siebelstartup.pl, for Perl-based files.

Note: If parameter UsernameHeaders is not configured in the SmSiebelSSO.conf file, the Siebel agent will continue to look only for the SIEBELUSER response.

Chapter 5: Troubleshooting

This section contains the following topics:

Response Test or Session Startup Errors

Symptom:

An error occurred during the response test or on session startup.

Solution:

Verify the SiteMinder Policies by using SiteMinder Test Tool.

To verify SiteMinder Policies

1. Access SiteMinder Test Tool as follows:

   Start, Programs, Netegrity, SiteMinder, SiteMinder Test Tool

2. Specify the correct Agent Name, Shared Secret, and IP address. Click Connect.

3. Enter the correct validation realm resource (for example, /esales/), the action GET, and click IsProtected.

4. Enter a valid SiteMinder username and password. Click IsAuthenticated, and IsAuthorized.

5. If at any time a red indicator appears or if the NPS_SESSION_LINKER response does not appear in the Attributes box, examine the SiteMinder Policy server configuration and logs. The logs are mandatory for proper configuration.

6. Change the resource to /SiebelConnector/. Click IsProtected, IsAuthenticated, and IsAuthorized. Verify that no red indicators appear and that responses appear for both SIEBELUSER and SIEBELTICKET.

Unable to Reach Siebel Startup or Siebel Login Page

500 Server Error

Symptom:

The web browser shows a 500 Server Error page or the web browser continuously returns to the SiteMinder login page.

Solution:

Examine the Web Agent log.

Possible solutions to these problems may be found in the *eTrust SiteMinder Agent Operations Guide*. Further diagnosis is beyond the scope of this document, but an examination of the Web Agent log file in conjunction with the troubleshooting section of the Web Agent manual should help resolve the issue.

Note: Customers continuing to have this problem should open a support case with CA. This problem does not relate to the Siebel SSO agent– it is a problem in the site’s Web Agent configuration.

Server Busy Error

Symptom:

ProviderTest (or ProviderTest75) reported no problems but a message indicates that the server is busy or experiencing difficulties.

Solution:

Examine the Security Adapter logs.

Consider using the AnonUsername and AnonPassword settings.

More information:

Security Adapter Settings (see page 65)

Ticket Outside Acceptance Window Issue

Symptom:

The symptoms of this problem include an infinite loop in the browser window and the following message that appears in the Policy server Authentication Log:

```
Ticket outside acceptance window - replay attack?
```

The most common problem encountered is an error in response creation, specifically in configuring attribute caching.

Solution:

Perform the following procedure to correct a ticket outside acceptance window issue.

To correct a ticket outside acceptance window issue

1. Open the response and adjust the Attribute Caching setting (see the Attribute Caching parameter in Step 11 in the section Create SiteMinder Policies (see page 25)).
2. In SiteMinder versions prior to and including v5.5 Service Pack 2, a defect prevented you from setting the cache directly in the GUI. If you have one of these versions, verify that the setting is correct by doing one of the following:
   - Upgrade to SiteMinder 5.5 SP2 CR002 or later.

     These versions include the fix to the GUI problem, allowing you to set attribute cache through the GUI.
   - Run the responsecheck script.

     This script examines the Policy Store, verifies the response cache value, and rectifies any error in the Attribute Caching setting. The script is in the

     ```
     <Siebel Agent Installation folder/Siebel/Config/PolicyServer/responsecheck.zip zip file.
     ```

     To use the script, extract the contents of the .zip file, read the Readme.txt file contained in the .zip, and run the responsecheck file for your platform.

- Manually export, correct, and re-import the Policy Store, as described in the Policy server documentation.

  Run the command line tool smobjexport with appropriate command line options to create a text file copy of the site's Policy Store, for example:

  ```
  objectclass: ResponseAttr
  Oid: 08-ebf2fc68-1a78-4449-846d-b1de5e15cad0
  DomainOid: 03-0583c2f4-180b-4c24-a3c9-10ea686e7c4d
  Response: 07-c6d204e-d9f2-894a-701775c05092
  AgentTypeAttr: 11-8d78bb90-ae15-11d1-9cdd-006008aac24b
  Value:
  TTL: 0
  Flags: 20
  ActiveExpr: 1f-c7249c4f-6128-43cd-90b7-7c93f3c82144

  objectclass: ActiveExpression
  Oid: 1f-c7249c4f-6128-43cd-90b7-7c93f3c82144
  DomainOid: 03-0583c2f4-180b-4c24-a3c9-10ea686e7c4d
  Expr: <@lib="SiebelSSOAuth" func="GetSSOTicket" param="SECR
  Variables:
  UsesVariables: false
  ```

  Within this file there is an entry for the SiebelSSOAuth ticket. This line indicates that the change in the Time To Live (TTL) value needs to be made in the ResponseAttr which points to the active expression containing SiebelSSOTicket.

  The value of TTL is the maximum amount of time, in seconds, that the response can be cached by the Web Agent. A value of 0 indicates that the response can be cached indefinitely. The TTL value must be less than the value of the PERIOD setting of the Authentication Scheme.

  The TTL for this ResponseAttr should be set to 30 seconds or less. The resulting file can be imported with the command smobjimport and the command line option -f to forcibly overwrite any pre-existing value.

Agent API Not Loaded

Symptom:

Security Adapter attempts to dynamically load the SiteMinder Agent API when needed. If the Agent API library cannot be found, the following message appears in the Security Adapter log file:

```
Agent API Not loaded
```

This message indicates that the system is unable to locate the relevant SiteMinder Agent API file (SmAgentAPI.dll, libsmagentapi.so, libsmagentapi.sl).

Solution:

Check that the Agent API file is present (see Security Adapter File Names (see page 30)).

If the file is present, but this error persists, do the following, according to your platform:

- AIX or Solaris: Do one of the following:
  - Copy the *Siebel agent installation folder*/siebel/bin/libsmagentapi.so file to /usr/lib
  - Copy the *Siebel agent installation folder*/siebel/bin/libsmagentapi.so file to a directory in the LD_LIBRARY_PATH (or LIBPATH on AIX)
  - Update the LD_LIBRARY_PATH (or LIBPATH on AIX) to include the directory where the libsmagentapi.so is located
- HP-UX 11: Do one of the following:
  - Copy the *Siebel agent installation folder*/siebel/bin/libsmagentapi.sl file to /usr/lib
  - Copy the *Siebel agent installation folder*/siebel/bin/libsmagentapi.sl file to a directory in the SHLIB_PATH
  - Update the SHLIB_PATH to include the directory where the libsmagentapi.sl is located
- Windows: Copy the *Siebel agent installation folder*\siebel\bin\SmAgentAPI.dll file to the C:\WinNT\system32 directory.

Note: Within the Security Adapter file (SmSiebelSSO.conf), the settings for LogFile and LogLevel determine what information is logged. Make sure you have defined a log file and a level of logging.

More information:

Configuring Security Adapter (see page 31)

Resolving Various Issues

Symptom:

An error message is issued.

Solution:

CA support will typically be the best help in resolving issues within the login library, however there are a number of simple steps that can be taken before checking with CA. The following steps will enable CA to assist in the resolution of problems:

1. Set the log level to 2, and examine the logs. The most common problems reported to CA are the result of errors in the configuration of the Policy server, IP Agent Name and Shared Secret. At log level 2, many of these errors will appear and the solution will be obvious. For example, the following message implies that the agent name or shared secret is the likely cause of the problem:

   ```
   Failed to connect agent - check shared secret and agent name
   ```

2. Increase log level to 3, and examine logs again. This level reveals additional information including the cause of the problem.

Connecting to Server Error

Valid for Agent for Siebel 7.7 and 7.8.2 for HI client application

Symptom:

An error connecting to server message appears at the top of the Siebel application page when the SiteMinder session times out before the Siebel session times out.

Solution:

Set the SiteMinder session to a large value, and set the Siebel session timeout to a lower value so that Siebel governs the idle session timeouts.

Set the TurnLoopingOff variable as follows:

- 1 in the siebelstartup.asp file
- true in siebelstartup.jsp or siebelstartup.pl files.

Web Server Trace File Issue

Valid when Siebel WSE resides on IIS6.

Symptom:

The web agent trace file on the web server does not log additional information.

Solution:

When Siebel WSE resides on IIS6, it creates a virtual folder for the Siebel application within the default website that has a different application associated to it.

You must do the following:

Add the ISAPI6WebAgent.dll wildcard application mapping for the Siebel application/folder within the default website.This will cause the additional logging to appear in the webagent trace file.

Monitoring the Processing of a Request

The following stages in the processing of a request are documented in various log files:

- Generation of a Siebel authentication ticket (see page 56)
- Siebel User response (see page 56)
- Anonymous User Authentication (see page 56)
- Security Provider Contacts Policy Server (see page 57)
- Policy Server Contacts the Siebel SSO Authentication Scheme (see page 58)
- Security Provider Checks the SIEBELUSER Response (see page 59)

Generation of a Siebel Authentication Ticket

Generation of a Siebel authentication ticket is recorded in the Policy server trace, as shown in the following example:

```
.
****************************************************
…….Siebel SSO Ticket Generation Parameters
*****************************************************
.
.
Generating SSO ticket WITHOUT DN
.
[SIEBELTICKET=[NDSEnc-D]IhOoXn6KH6D9GMSQ2yQOywuZa4Hw+Qcr6zYdZ/oqzxM=]
```

Siebel User Response

Firing a Siebel user response, which sends a user attribute whose value maps to a valid Siebel user, is recorded in the Policy server trace, as shown in the following example:

```
[SIEBELUSER=test]
```

Anonymous User Authentication

Anonymous user authentication is recorded in the Siebel Agent Security Provider logs, as shown in the following example:

```
.
Checking for Anonymous user
Anonymous user password correct
.
```

Security Provider Contacts Policy Server

The process in which Security Provider contacts Policy server and accesses the protected resource /SiebelConnector/ can be seen in the Siebel Agent Security Adapter log, as shown in the following example:

```
.
.
SecurityLogin8() called
Username: 'test'
Password: *Not shown* (54 chars)
Config file already loaded
SmAgentConnection::Connect()
Checking for Anonymous user
Anonymous user, checking password
Invalid Anonymous password - user will be authenticated via SiteMinder
SecurityLogin8() calling AuthAzAndCollectResponse()
.
.
```

Policy Server Verifies the User Credentials

The process in which Policy server uses the Siebel SSO authentication scheme to verify the user credentials can be seen in the Policy server traces as shown in the following example:

```
.
.
[SiebelConnector: Authentication phase]
.
[SiebelConnector: Authenticating user with SSO ticket]
.
[SiebelConnector: Username to be validated is 'test']
.
[SiebelConnector: Validating token [NDSEnc-D]LYwrQqKp9mugsmf6mdHid3MRaQch4iilKUzi+PD0olw= for user
test]
.
[SiebelConnector: Ticket decrypted to 19 bytes]
.
[SiebelConnector: Decrypted ticket - checking contents]
.
[SiebelConnector: Ticket parser results:]
.
[SiebelConnector: Time: 1132825779]
.
[SiebelConnector: LoginName: test]
.
[SiebelConnector: Ticket in acceptance window]
.
[SiebelConnector: Auth succeeded]
.
```

Security Provider Checks the SIEBELUSER Response

Security provider checks the SIEBELUSER response against the response that was extracted from the HTTP headers. This can be seen in Siebel Agent Security Adapter log, as shown in the following example:

```
.
AuthAzAndCollectResponse - Authentication ACCEPTED
AuthAzAndCollectResponse - Authorization ACCEPTED
Found SIEBELUSER Response
Usernames match
There are 0 responses saved
Credentials for user 'sadmin' accepted
User authenticated - returning SecurityErrOK
SecurityGetCredentials8() called
Requested credential type is ServerDataSrc
Returning SecurityErrOK
```

Appendix A: NPSEncrypt and NPSVersion Tools

This section contains the following topics:

NPSEncrypt Tool

Sometimes, *secret* values must be stored in a configuration file. For security purposes, you may want to encrypt and store the encrypted form of these secret values. To do this, use the NPSEncrypt tool.

When a setting allows encrypted values to be used, this product will decrypt it before use. If the setting is not encrypted, the value entered will be used as is.

The NPSEncrypt utility takes plain text entered on the command line, encrypts it, and prints the result on the screen. The resulting encrypted text can be cut and pasted wherever it is needed.

A product that allows an encrypted value will automatically decrypt the value when needed.

To encrypt a value, use the command prompt and type the NPSEncrypt command followed by a space and followed by the text to be encrypted, as shown in the following example:

```
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-B]CKtyevyWkrF24Aj9Ly+xEQ==
```

In this case the encrypted form of secret is as follows:

```
[NDSEnc-B]CKtyevyWkrF24Aj9Ly+xEQ==
```

When you copy and paste, grab the entire line, including the portion beginning with [NDSEnc-].

NPSEncrypt will encrypt the same text to many different cipher-text values. Use any of the values, for example:

```
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-C]iQO2KVyRN2fB4tMwjtgRYQ==
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-C]FWhVC+MiA7aNnA87szw76g==
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-B]PD24A2Iz6H+KeDh7j4zUIg==
```

NPSVersion Tool

Use the NPSVersion tool to extract version information from many CA products. To use this tool, type the NPSVersion on a command line followed by a space and the name of the executable whose version information you want, for example:

```
C:\> NPSVersion sessionlinkd
     [NPSVersion Version 1.0 - NPSVersion Revision 1]
     sessionlinkd    -  Package: NPSSessionLinker V1.3
     sessionlinkd    - Component: SessionLinker daemon V1.3.2 (Jul 14 2003 20:26:16)
     sessionlinkd    -  Platform: AIX
C:\>
```

You may use the NPSVersion tool on one platform to extract information for a product built for any other platform. The actual information displayed might differ in format and content from that shown above, but the relevant lines when discussing any issues with Support are Package and Component. Each line has a version number.

Package refers to the version of the Product, in this case the SessionLinker version 1.3 product.

Component refers to the actual part of the product that is enclosed within this specific file. It is not uncommon for this version number to be larger than the *Package* version number. This is usually due to the Component having one of more bugs repaired or minor enhancements added, which did not require the entire Package to be rebuilt or renumbered.

Appendix B: Upgrading from a Previous Version

This section contains the following topics:

Changes from SiebelSSOAuth Version 1.0.4

This release of the eTrust SiteMinder agent for Siebel includes a new version of the Siebel SSO Authentication Scheme (v1.0.5).

SiebelSSOAuth versions 1.0.4, and earlier generated an encrypted ticket that contained only a user's username and timestamp. As of version 1.0.5, the Active Response can generate both this old form of ticket and a newer form that includes the user's DN.

This new feature allows Siebel to perform SSO Authentication within the Authentication Scheme rather than relying upon SiteMinder to do this work. This feature is useful in a number of environments including, but not limited to, environments where the following occur:

- The Siebel username differs from the SiteMinder username
- SiteMinder does not know how to search the user directory (for example, with custom directory providers and with certain database configurations)

This feature might cause problems in environments where the following occur:

- The user DN is large, resulting in a ticket larger than the largest length supported by Siebel
- You want the eTrust SiteMinder agent for Siebel to perform authentication or authorization against a different user directory than that used for the Web Agent

Upgrade and Enable the New Encryption Ticket

Before upgrading for the new feature in a production environment, perform the installation in a test environment to make sure the upgrade does not have any adverse consequences.

To upgrade and enable the new encryption ticket

1. Run smobjexport command to generate a backup of the existing Policy Store. Refer to the Policy server documentation.
2. Stop one Policy server.
3. Replace the existing file, SiebelSSOAuth.dll, libSiebelSSOAuth.so or libSiebelSSOAuth.sl with the file in the *Siebel agent installation folder*\Siebel\bin folder.
4. Start the Policy server.
5. Wait several minutes to allow all agents to begin again using this Policy server.
6. Repeat Step 2 through Step 5 for each Policy server in the environment.
7. Open the SiteMinder Admin GUI and find the response for the Siebel Ticket. Change the Function Name from CreateSSOTicket to CreateSSOTicketWithDN (you do not have to flush the cache manually, it happens automatically).
8. Wait several minutes for every Policy server to detect the changed response and for the cache on every Web Agent to be flushed.

   Note: Manually flushing the cache does not accelerate this process.
9. Test the environment to ensure that Siebel is working correctly.

Appendix C: Security Adapter Settings

This section contains the following topics:

Introduction

The initialization and configuration files for Security Adapter are located in the *Siebel Agent Installation folder*:

For v7.0.x and v7.5.x, only the configuration file is necessary:

Siebel Agent installation folder\Siebel\Config\SecurityAdapter\SmSiebelSSO.conf

For v7.7 or v7.8.2, you must have both the initialization and configuration files:

Siebel Agent installation folder\Siebel\Config\SecurityAdapter\SmSiebelSSO.ini
Siebel Agent installation folder\Siebel\Config\SecurityAdapter\SmSiebelSSO.conf

You install these files on the Siebel Application Server's Object Manager, and modify the settings in the configuration file.

If you make any changes to the configuration file(s) after Security Adapter is enabled in Siebel, restart Object Manager.

More information:

Configuring Security Adapter (see page 31)

Settings

LogFile

Specify the full path to the file that Security Adapter will use as a log file. On Windows systems, this path should include the drive, directory and file name. For example:

```
c:\logs\connector.log
```

On UNIX systems, the path should be absolute, for example:

```
/var/log/siebelconnector.log
```

LogLevel

Valid levels of logging are listed in the following table.

Level	Log Indicator	Meaning
0	*(not applicable)*	None; log file off.
1	ERR	Errors only; errors in initialization and communication are logged.
2	INF	Informational; indicates the general cause of the problem.
3	DBG	Debug; information not typically useful in production environments.
4	XXX	Extra; helps locate problems in the Login Library code itself, and thus is typically not intended for non-CA personnel.

Note: At higher log levels (2 through 4) the file can increase in size very quickly. At a production site, using log level 1 is recommended.

PolicyServer

Security Adapter must communicate with the same Policy server or servers as the Web Agent. You may specify a single Policy server, multiple Policy servers, or even one or more Policy servers running on non-default ports.

Specifying a Single Policy Server

Minimally, you can set the IP address of a single Policy server, for example:

```
127.0.0.1
```

In this case, Security Adapter assumes that the Policy server is operating on the default ports.

More information:

Specifying Ports (see page 67)

Specifying Multiple Policy Servers

For multiple Policy servers, you can specify all IP addresses or host names. You must enter them on a single line, separating them with a space. An example of two Policy servers is:

```
192.168.1.4 192.168.1.5
```

In this case, Security Adapter assumes that the Policy servers are operating on the default ports.

Specifying Ports

If you do not specify ports, Security Adapter assumes that the Policy server(s) is/are operating on the default ports, which are the following:

1. 44441—Accounting port
2. 44442—Authentication port
3. 44443—Authorization port

If a Policy server is not operating on the default ports, you must specify the ports. Use commas (not spaces) to separate the information items in the Policy server string:

```
IPAddress,AccountingPort,AuthenticationPort,AuthorizationPort
```

For example:

```
192.168.1.4,44441,44442,44443
```

If multiple Policy servers are using ports other than the default, you must separate each Policy server string (which includes Policy server and ports) by a space, for example:

```
192.168.1.4,44441,44442,44443 192.168.1.5,44441,44442,44443
```

Although the Accounting server might not be used and the eTrust SiteMinder Agent for Siebel does not connect to the SiteMinder Accounting server, 44441 is entered here for consistency with SiteMinder Web Agent configuration file syntax as well as to allow for future expandability. (You must specify the first port as the Accounting port, even though it is not being used internally.)

Setting the EnableFailover Attribute

As with Web Agents, Security Adapter supports more than one Policy server in either failover or round robin mode. This setting allows you to define the mode.

Setting EnableFailover to YES (failover mode) causes Security Adapter to use the first Policy server in the list until that server fails. If the first server in the Policy server list fails, Security Adapter will use the second Policy server in the list. This behavior continues until all Policy servers have become unreachable or unresponsive.

Setting EnableFailover to NO causes Security Adapter to use all Policy servers in a round robin fashion. When one Policy server fails, it is removed from the list and the Security Adapter will continue to use all other Policy servers automatically.

The SiteMinder Agent API automatically checks failed servers on a regular basis and reconnects them when they become available.

AgentName and SharedSecret

Security Adapter uses AgentName and SharedSecret settings to initiate connection to the Policy server. AgentName must match the name entered in the Policy Management GUI. The SharedSecret setting must match the shared secret entered in the Policy server GUI.

Encryption

The SharedSecret setting can be encrypted.

You cannot copy and paste a value encrypted with the Web Agent's encryption tools; you must use the NPSEncrypt tool. The tool is located in the following folder:

Siebel Agent installation folder/Siebel/Tools

More information:

NPSEncrypt Tool (see page 61)

SiteMinder 5.X

For authenticating themselves, SiteMinder v5 Web Agents use a new model called the *Trusted Host* model. However, eTrust SiteMinder Agent for Siebel continues to use the Agent Name and Shared Secret model used in Web Agents v4 and earlier.

When you use the SiteMinder Agent Dialog box to create an agent for Security Adapter, make sure to place a check in the check box labeled Support 4.x agents.

Action and Resource

The Action and Resource settings define the strings that the Security Adapter should send to the Policy server when validating the user's ticket and their authorization to access Siebel. These strings are typically GET and /SiebelConnector/ and should only be changed by customers that fully understand SiteMinder Policies and have a reason for not being able to use GET and /SiebelConnector/.

DatabaseUser and DatabasePassword

Once the Security Adapter is installed, Object Manager uses the username and password specified by the settings DatabaseUser and DatabasePassword whenever credentials are needed for communication to another system. The most common system for which Object Manager needs these credentials is the underlying database. Customers should refer to the section Select/Configure Database Credentials for additional information on the security implications of using the same credentials for all users when communicating with the database.

The setting DatabasePassword can be encrypted.

More information:

NPSEncrypt Tool (see page 61)

Credential Types

Using the same credentials to communicate with any other system is generally not a problem in test environments because administrative accounts tend to share a common set of credentials. In production environments, however, this can be a problem because security requirements typically dictate that common passwords may not be used for multiple systems.

To solve this problem, Security Adapter can be configured to return an alternative set of credentials for each credential type requested by the Object Manager.

For example, if a user has selected an administrative task and attempted to manage another Enterprise Server, the current Object Manager attempts to initiate communication with another Object Manager and fails. It displays a Login failed message.

In addition, the Server Manager's log file shows the following information:

```
(admauth.cpp 9(148) err=901042 sys=2) ADM-01042: Login failed for specified username, password, and data source
```

To configure Security Adapter properly, examine the Security Adapter's log file (with the log level set to 3) for the entry beginning with:

```
Requested credential type is ServerDataSrc.
```

To change the credentials returned, add two lines to the configuration file, one each for the username and password. Use the following format:

```
Credentials.Type.Username=<Username>
Credentials.Type.Password =<Password>
```

For example, the log file entries are:

```
Credentials.GatewayDataSrc.Username=sadmin
Credentials.GatewayDataSrc.Password=sadminpassword
```

The correct values vary, depending on your environment.

You may encrypt the credentials password by using the NPSEncrypt tool.

AnonUsername and AnonPassword

Once installed, Siebel Security Adapter is called by the Object Manager every time a username and password are presented. This feature allows SiteMinder to integrate fully with Siebel and support both username and password-based signon, and the ticket-based single signon.

Having Object Manager call Security Adapter for every username and password presented does have one unintended consequence, which is that the Siebel Web Server Extension (WSE) connects to the Object Manager to download the Login page (typically SWELogin.swt file).

To make this connection, WSE sends a special username and password configured in the eapps.cfg file. By default, this username is SADMIN. When this username and password are sent to Security Adapter, Security Adapter passes it on to SiteMinder for verification. As long as the user exists in the SiteMinder's user store, with the password defined in eapps.cfg, WSE is able to download the login page. If the anonymous user does not exist in SiteMinder, WSE returns an error saying that the server is either busy or experiencing difficulties. In these cases adding a special user to the SiteMinder user store is not a good solution.

The eTrust SiteMinder agent for Siebel has a feature that allows sites to define one special user that the eTrust SiteMinder agent for Siebel will not verify against SiteMinder. To ensure security, use this feature only for the WSE.

The configuration settings AnonUsername and AnonPassword can be set to the username and password specified in the eapps.cfg file. These are case sensitive; sadmin is not the same as SADMIN. This is intended to match the behavior of most user directories supported by SiteMinder.

To encrypt AnonPassword, use NPSEncrypt.

More information:

NPSEncrypt Tool (see page 61)