

Web SSO Configuration Guide

Sun™ ONE Identity Server Policy Agents

Version 2.0

816-6901-10
August 2003

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.

Copyright 2003 Sun Microsystems, Inc. All rights reserved.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, Sun ONE, iPlanet, and all Sun, Java, and Sun ONE based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

Netscape is a trademark or registered trademark of Netscape Communications Corporation in the United States and other countries.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of the product or this document may be reproduced in any form by any means without prior written authorization of Sun Microsystems, Inc. and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2003 Sun Microsystems, Inc. Tous droits réservés.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, Sun ONE, et iPlanet sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et d'autre pays.

UNIX est une marque enregistrée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company Ltd.

Netscape est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

Le produit décrit dans ce document est distribué selon des conditions de licence qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ni de ce document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de Sun Microsystems, Inc. et, le cas échéant, de ses bailleurs de licence.

CETTE DOCUMENTATION EST FOURNIE “EN L'ÉTAT”, ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.

Contents

About This Guide	5
What You Are Expected to Know	5
Identity Server Documentation Set	5
Documentation Conventions Used in This Manual	6
Typographic Conventions	7
Terminology	7
References	7
Related Information	7
Chapter 1 Setting Up Web Single Sign-on Solution	9
Need for Identity Management	9
Sun ONE Identity Server 6.0	10
Siebel 7.5 and Security Architecture	10
Integration Process	11
Supported Platforms	11
Overview	12
Pre-requisites to Integration	14
Integration Steps	14
Known Issues and Limitations	16
Appendix A Relevant Configuration Files	19
Appendix B Siebel Applications Configuration Files	21
Index	23

About This Guide

This guide offers procedures to integrate Sun™ ONE Identity Server 6.0 and Siebel 7.5 to provide a Web Single Sign-on solution.

This preface contains the following sections:

- [What You Are Expected to Know](#)
- [Identity Server Documentation Set](#)
- [Documentation Conventions Used in This Manual](#)
- [Related Information](#)

What You Are Expected to Know

This book is considered to be an auxiliary manual in the documentation series provided with Sun ONE Identity Server 6.0 SP1. It's essential that you have experience in:

- Directory technologies
- Lightweight Directory Access Protocol (LDAP)
- Sun ONE Directory Server
- Siebel applications

As you try to understand the concepts described in this guide, you should reference the *Sun ONE Identity Server* and the *Sun ONE Directory Server* documentation.

Identity Server Documentation Set

The Sun ONE Identity Server documentation set contains the following titles:

- *Product Brief* provides an overview of the Sun ONE Identity Server and its features and functions.
- *Installation Guide* provides details on how to install and deploy the Identity Server on Solaris™, Linux and Windows® 2000 systems.
- *Administration Guide* describes how to use the Identity Server console as well as manage user and service data via the command line.
- *Programmer's Guide* documents how to customize an Identity Server system specific to your organization. It also includes instructions on how to augment the application with new services using the public APIs.
- *Getting Started Guide* documents how to use various features of Identity Server to set up a simple organization with identities, policies and roles.
- *J2EE Policy Agents Guide* documents how to install and configure Identity Server policy agents for application servers on a remote server. It also includes troubleshooting and information specific to each agent.
- *Web Policy Agents Guide* documents how to install and configure Identity Server policy agents for web servers on a remote server. It also includes troubleshooting and information for these agents.
- *Web SSO Configuration Guide (this guide)* describes the steps for enabling Web SSO between Sun ONE Identity Server 6.0 and Siebel 7.5 applications.
- The *Release Notes* file gathers an assortment of last-minute information, including a description of what is new in this release, known problems and limitations, installation notes, and how to report problems.

NOTE	Be sure to check the Identity Server documentation web site for updates to the release notes and for revisions to the guides. They are available at http://docs.sun.com/db/prod/slidsrv#hic . Updated documents will be marked with a revision date.
-------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Documentation Conventions Used in This Manual

In this guide, there are certain typographic and terminology conventions used to simplify discussion and to help you better understand the material. These conventions are described below.

Typographic Conventions

This book uses the following typographic conventions:

- *Italic type* is used within text for book titles, new terminology, emphasis, and words used in the literal sense.
- `Monospace font` is used for sample code and code listings, API and language elements (such as function names and class names), filenames, pathnames, directory names, HTML tags, and any text that must be typed on the screen.
- *Italic serif font* is used within code and code fragments to indicate variable placeholders. For example, the following command uses *filename* as a variable placeholder for an argument to the `gunzip` command:

```
gunzip -d filename.tar.gz
```

Terminology

Below is a list of the general terms that are used in the Sun ONE Identity Server Policy Agent documentation:

- *Agent_Install_Dir* is a variable placeholder for the directory where you have installed the Sun ONE Identity Server Policy Agent.
- *S1IS_Install_Dir* is a variable placeholder for the home directory where you have installed Sun ONE Identity Server 6.0.

References

1. Security Guide for Siebel eBusiness v7.5
2. Technical note 0300: Quick Guide to Using Netscape LDAP Server with Siebel eBusiness Applications
3. Sun ONE Identity Management White Paper

Related Information

In addition to the documentation provided with Sun ONE Identity Server, there are several other sets of documentation that might be helpful. This section lists these and additional sources of information.

iPlanet Directory Server Documentation

iPlanet Directory Server 5.1 documentation can be found at

http://docs.sun.com/db/coll/S1_ipDirectoryServer_51

iPlanet/Sun ONE Web Server Documentation

iPlanet/Sun ONE Web Server documentation can be found at

http://docs.sun.com/db/coll/S1_ipwebsrvree60_en

Sun ONE Certificate Server Documentation

Sun ONE Certificate Server documentation can be found at

http://docs.sun.com/db/coll/S1_slCertificateServer_47

iPlanet Proxy Server Documentation

iPlanet Proxy Server documentation can be found at

http://docs.sun.com/db/coll/S1_ipwebproxysrvr36

Other iPlanet Product Documentation

Documentation for all other Sun ONE servers and technologies can be found at

<http://docs.sun.com/prod/ds/sunone>

Download Center

Links to download any of Sun's Sun ONE/iPlanet software are at

<http://www.sun.com/software/download/>

Sun ONE Technical Support

Technical Support can be contacted through

<http://www.sun.com/service/support/software/iplanet/index.html>

Professional Services Information

Professional Service can be contacted through

<http://www.sun.com/service/sunps/iplanet/>

Sun Enterprise Services for Solaris Patches And Support

Solaris patches and support can be obtained through

<http://www.sun.com/service/>

Developer Information

Information on Sun ONE Identity Server, LDAP, the Sun ONE Directory Server, and associated technologies can also be found at

<http://developer.iplanet.com/tech/directory/>

Setting Up Web Single Sign-on Solution

This guide describes the steps required to enable Web Single Sign-On (SSO) between Siebel 7.5 and the Sun ONE Identity Server 6.0. Web SSO services allow a user to access multiple, distributed web-based applications, services, or sites during a single session without having to reauthenticate while switching between applications or services.

The topics covered in this document include:

- [Need for Identity Management](#)
- [Integration Process](#)
- [Known Issues and Limitations](#)

Need for Identity Management

Today, a typical business environment has numerous applications and services deployed throughout its enterprise. The identity information for each of these applications and services is most likely maintained separately. If each component manages its own identities, identity information tends to be widely distributed. It runs on different operating systems, uses different rules and standards for security, and is owned and controlled by a widespread group of individuals. As the number of components in an enterprise grows, distributed identity management becomes problematic for IT organizations as the size, cost, and maintenance of the infrastructure sky rockets, redundancy increases, and security risks become a concern.

The solution to this problem lies in implementing a centralized identity management infrastructure. If every application and service in an enterprise used the same identity management infrastructure for managing the identities of their users, including authentication, authorization, roles and policies, then a lot of the problems that IT organizations face today, including increased cost, redundancy, and security risks, could be alleviated. Such a centralized identity management infrastructure, which includes directory services, access management, identity provisioning, and identity administration, is what the Sun ONE Identity Management framework provides through its suite of products.

Sun ONE Identity Server 6.0

One of the core products in the Sun ONE Identity Management framework is the Sun ONE Identity Server. It helps organizations manage secure access to web-based resources via access management services that enable web single sign-on, identity administration, and directory services. Web single sign-on services allow a user to access multiple, distributed web-based applications, services, or sites during a single session without the need for reauthentication as the user switches between components. Since web single sign-on through Sun ONE Identity Server greatly enhances the overall user experience and solves one of the most complex IT problems, it is the focus of this integration with Siebel.

Siebel 7.5 and Security Architecture

Siebel 7.5 applications, the latest release of Siebel eBusiness Applications, provide market leading depth and breadth of functionality in sales, marketing, service, and partner relationship management.

To understand the web single sign-on solution between Sun ONE Identity Server 6.0 and Siebel 7.5, it is important to understand the security architecture of this product. Siebel 7.5 adheres to commonly accepted security standards to facilitate the integration of the application into the customer's business environment and security infrastructure. These industry-wide security standards are used to support three authentication methods in Siebel 7.5. Each of these authentication methods is briefly explained below.

- **Native Database Authentication** - In this method, the underlying security system of the database verifies user credentials for Siebel 7.5. Each user must have a valid database account in order to access the Siebel application.

- **Security Adapters for External Authentication** - Siebel 7.5 includes a preconfigured security adapter interface to allow organizations to externalize credential verification. The interface connects to a security adapter, which contains the logic to validate credentials to a specific authentication service. Customers of Siebel Systems, Inc. can therefore verify user credentials with security standards such as the Lightweight Directory Access Protocol (LDAP). Siebel 7.5 includes security adapters for the leading authentication services. In addition, Siebel also provides a developer's toolkit so that customers can build customized security adapters.
- **Web Single Sign-On** - Siebel 7.5 offers customers the ability to enable a single login across multiple web applications. This is also known as Web SSO. With Web SSO, users are authenticated independently of Siebel applications, either through a third-party authentication service or through the web server. Web SSO with Siebel can be achieved in two different modes: server mode and header mode.

Integration Process

This section provides an overview of the integration between Sun ONE Identity Server 6.0 and Siebel 7.5 to achieve Web SSO.

This integration has been done using the Siebel 7.5 application Call Center. The integration can, however, be applied to other Siebel applications as well. The header mode is the Web SSO mode used for this solution. Header mode works by setting a HTTP header variable and passing it to the Siebel Web Engine.

Supported Platforms

The following table displays the agents available for the web servers supported by Siebel.

Table 1-1

Web Server	Platform	Agent Available?
Microsoft IIS 5.0	Windows 2000 Server/Advanced Server with SP2 or above running on x86 only	Yes
Sun ONE Web Server 6.0 SP2	Solaris 8 with recommended Patch Cluster (kernel level 13 or above)	Yes

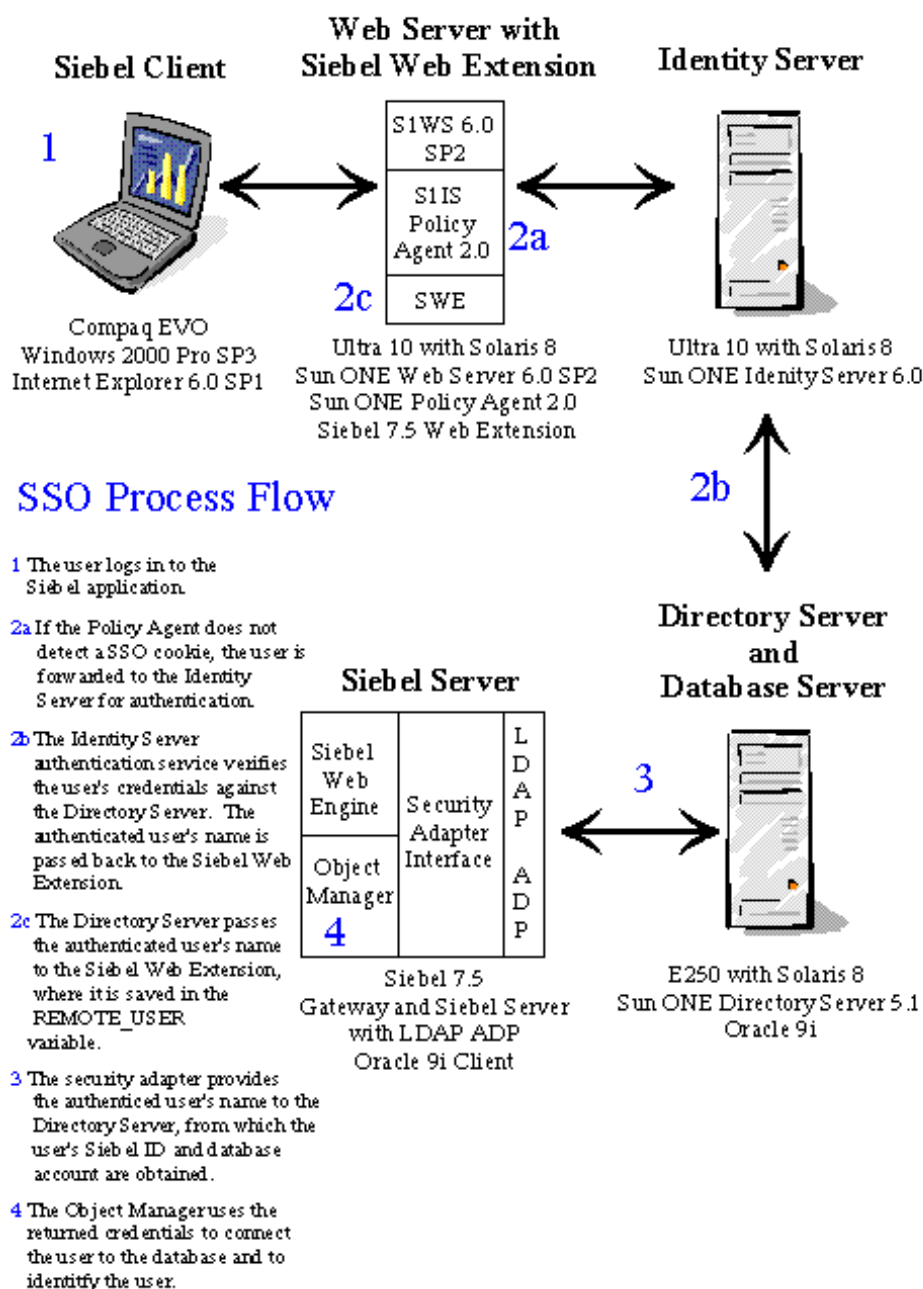
Table 1-1

Web Server	Platform	Agent Available?
IBM HTTP Server Limited Release 2.0.30	Servers running AIX 5L with Maintenance Level 1 or above	No

Overview

This integration uses Siebel's LDAP Security Adapter in conjunction with the LDAP authentication module of Sun ONE Identity Server. All user data and application information for Siebel are stored in a relational database. This integration uses Sun ONE Identity Server and Siebel Security Adapter for authentication only. To understand how the users get logged onto their Siebel application, even though they authenticate to Sun ONE Identity Server, it is important to know how the Siebel Security Adapter works in conjunction with Sun ONE Identity Server.

This Web SSO solution uses the traditional policy agent implementation model, where a URL Policy Agent is installed on the web server hosting the Siebel application. All HTTP requests are intercepted by the agent, and in the absence of an SSO Token, the user is redirected to the Sun ONE Identity Server 6.0 login page for authentication. Upon successful authentication, the agent populates a pre-determined header variable with the Siebel `uid`. The Siebel Web Server Extension (SWSE) extracts this header value and passes the authenticated user's name to the authentication manager, a component of the Siebel Object Manager. The security adapter then provides this user name to Sun ONE Directory Server from which the user's Siebel `uid` and database account are returned to the authentication manager. Siebel Object Manager then uses the returned database credentials to connect the user to the database to identify the user. Figure 1 depicts the deployment architecture and SSO process flow.

Figure 1-1 Deployment Architecture and SSO Process Flow

Pre-requisites to Integration

Before you begin the integration, make sure that:

- Siebel and all of its required components, including the web server and the database server, are installed and running in the environment. For detailed information on how to do this, please refer to the Siebel Bookshelf.
- Sun ONE Identity Server, including Sun ONE Directory Server, is installed and running. For information on how to install these products, please refer to the Sun ONE Identity Server product documentation.

Integration Steps

Once you have the products mentioned above installed and running, follow the steps listed below to enable Web SSO between Siebel 7.5 and Sun ONE Identity Server.

NOTE	Although this document describes only the steps to integrate Sun ONE Identity Server with Siebel Call Center 7.5 for Web SSO, it has been validated against Call Center, eSales, ERM and eChannel. Validation against four distinct Siebel applications makes this a generic solution, which can be used across all Siebel 7.5 eApps1.
-------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1. Set up Sun ONE Directory Server 5.1 so that the database accounts and the user's Siebel `uid` can be retrieved.

Users in the Siebel database must correspond to users in Sun ONE Directory Server.

Users in Sun ONE Directory Server must have attributes containing values for Siebel `uid`, password and database account. Attribute names must correspond to what is configured in the web server plug-in configuration file, `eapps.cfg`, and the Call Center configuration file, `uagent.cfg`. The web server plug-in configuration file is located in `$WEB_PLUGIN_HOME/bin` directory on the web server machine. The Call Center configuration file is located in `$$SIEBEL_HOME/siebsrvr/bin` directory on the Siebel server machine. If you are using a Siebel application other than Call Center, make sure you look at that particular application's configuration file rather than the Call Center configuration file.

2. Edit the parameters in the web server plug-in configuration file, `eapps.cfg`, residing on the web server machine to have the following values:

Code Example 1-1

```
[defaults]
AnonUserName = sadmin
AnonPassword = sadmin
AnonUserPool = 120
StatsPage = _stats.swe
HTTPPort = 8080
HTTPSPort = 443
EnableFQDN = FALSE
FQDN = CHANGE_ME
AnonSessionTimeout = 900
GuestSessionTimeout = 300
SessionTimeout = 900
DoCompression = TRUE
SingleSignOn = TRUE
TrustToken = siebel2sun
UserSpec = REMOTE_USER
UserSpecSource = Header
```

3. Edit the parameters in the Call Center configuration file, `uagent.cfg`, as described below. If you are using another Siebel application, make sure to edit the appropriate configuration file in a similar manner (see Appendix C).

Code Example 1-2

```
[LDAP]
DllName = libsscfldap.so
ServerName = e450b.sunmde.com
Port = 389
BaseDN = "ou=People,o=siebel.com"
SharedCredentialsDN = "uid=sadmin,ou=People,o=siebel.com"
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = dbaccount
;RolesAttributeType = siebelrole
;SslDatabase =
ApplicationUser = "uid=amAdmin,ou=People,o=siebel.com"
ApplicationPassword = netscape1
;EncryptApplicationPassword = FALSE
;EncryptCredentialsPassword = FALSE
SingleSignOn = TRUE
TrustToken = siebel2sun
;UseAdapterUsername = FALSE
```

Code Example 1-2

```
;SiebelUsernameAttributeType =
;UseRemoteConfig =
```

4. Install Sun One Identity Server Policy Agent, version 2.0 on the web server hosting the Siebel application. For information on how to install this agent, please refer to the policy agents documentation at http://docs.sun.com/db/coll/S1_IdServ_60.
5. Modify the file `amAgent.properties` to allow the policy agent to set values in the HTTP header. The `amAgent.properties` file is the configuration file for the policy agent. It is typically located in `/etc/opt/SUNWam/agents/es6/config/_opt_SUNWam_servers_<webserver_instance>/AMAgent.properties`. In the file, modify the following properties as listed below:

```
com.sun.am.policy.am.fetchHeaders=true
com.sun.am.policy.am.headerAttributes=uid|uid
```

6. Create policies in Sun ONE Identity Server 6.0 to allow/deny access to your Siebel application. The steps for creating policies are documented in the Sun ONE Identity Server Administration Guide, which is located at <http://docs.sun.com/source/816-6686-10/index.html>.

Policies can be set on users, roles, or organizations. For this integration, policies have been set on the organization.

7. Stop the Web Server, Web Server Admin, Siebel Server, and then the Gateway Server. Restart them in the reverse order.

To verify if the integration is successful, access the Call Center application URL. You will be redirected to Sun ONE Identity Server login page for authentication and upon successful authentication, you will be able to access the Call Center application.

Known Issues and Limitations

- In Header mode, Siebel applet pop-up window hangs after logging in. You can work around this by refreshing the browser.

- The integration has been validated in a Solaris environment with the browser Internet Explorer as the client program. The validation on an all Windows 2000 environment is soon to follow.

Relevant Configuration Files

A total of four Siebel applications were validated against this SSO solution: Call Center, eSales, ERM, PRM (formerly known as eChannel). All Siebel applications tested are assumed to be version 7.5 build 15051.

The files involved are the application's individual configuration file and a file named `eapps.cfg`, which contains parameters used by the Siebel Web Engine to control all Siebel applications' interactions with the Web Engine.

The relevant portions of the long application configuration files are the portions that fall under the headings "[Siebel]", "[SecurityAdapters]", and "[LDAP]". So for Call Center, eSales, ERM and PRM you would need to make sure the sections under the aforementioned headings contain the following:

Code Example A-1

```
[Siebel]
Security Adapter= LDAP

[SecurityAdapters]
LDAP= LDAP

[LDAP]
DllName                        = libsscfldap.so
ServerName                    = e420-101-4.sundevsjc.com
Port                          = 389
BaseDN                        = "ou=People,o=siebel.com"
SharedCredentialsDN           = "uid=sadmin,ou=People,o=siebel.com"
UsernameAttributeType         = uid
PasswordAttributeType         = userPassword
CredentialsAttributeType      = dbaccount
;RolesAttributeType           = siebelrole
;SslDatabase                   =
ApplicationUser               =
"uid=amAdmin,ou=People,o=siebel.com"
ApplicationPassword           = password1
EncryptApplicationPassword    = FALSE
EncryptCredentialsPassword    = FALSE
```

Code Example A-1

```
SingleSignOn           = TRUE
TrustToken              = siebel2sun
UseAdapterUsername      = FALSE
;SiebelUsernameAttributeType =
; UseRemoteConfig       =
```

The file `eapps.cfg` has a heading for each Siebel application, for example [callcenter], and [sales] as well as one named [defaults]. Anything specified under the specified application will override what is specified in defaults. For the purposes of this integration, the SSO specific configuration was specified in defaults as given here:

Code Example A-2

```
[defaults]
AnonUserName  = sadmin
AnonPassword  = sadmin
AnonUserPool  = 10
StatsPage     = _stats.swe
HTTPPort      = 8080
HTTPSPort     = 443
EnableFQDN    = FALSE
FQDN          = CHANGE_ME
AnonSessionTimeout = 900
GuestSessionTimeout = 300
SessionTimeout    = 900
DoCompression     = TRUE

SingleSignOn  = TRUE
TrustToken    = siebel2sun
UserSpec      = REMOTE_USER
UserSpecSource = Server
```

Siebel Applications Configuration Files

To configure Web SSO for a Siebel 7.5 application, it is necessary to modify its respective configuration file. The following table lists the configuration files of all the Siebel's applications for your easy reference.

Table 1-2 Configuration files for various Siebel applications

Siebel Application	Configuration File
Siebel Call Center	uagent.cfg
Siebel eBriefings	ebriefings.cfg
Siebel eAuction	esales.cfg
Siebel PRM Partner Portal	scw.cfg
Siebel PRM Webphone	wpechan.cfg
Siebel eCustomer	ecustomer.cfg
Siebel eEvents	eevents.cfg
Siebel eMarketing	emarketing.cfg
Siebel Employee Relationship Management	erm.cfg
Siebel eSales	esales.cfg
Siebel eService	eservice.cfg
Siebel eService Webphone	wpeserv.cfg
Siebel eTraining	etraining.cfg

Table 1-2 Configuration files for various Siebel applications

Siebel Application	Configuration File
Siebel Field Service	sfs.cfg
Siebel Marketing	market.cfg
Siebel Partner Manager	pmanager.cfg
Siebel Sales	siebel.cfg
Siebel Sales for CE	cssales.cfg
Siebel Sales for Palm	cssalespalm.cfg
Siebel Sales WebPhone	wpsales.cfg
Siebel Service	service.cfg
Siebel Service Webphone	wpserve.cfg

The integration was tested only with Siebel Call Center, Siebel eSales, Siebel Employee Relationship Management and Siebel Partner Relationship Management.

Index

A

Authentication
 native database [10](#)
 security adapters [11](#)
 Web Single Sign-On [11](#)

C

Certificate Server
 Documentation [8](#)

D

Developer Information [8](#)
Documentation
 Certificate Server [8](#)
 Proxy Server [8](#)
 Web Server [8](#)
Downloads
 Sun ONE Software [8](#)

I

Identity Management [9](#)
Identity Server
 Related Product Information [7](#)

Identity Server 6.0 [10](#)

Integration

 Issues and Limitations [16](#)
 overview [12](#)
 pre-requisites [14](#)
 process [11](#)
 steps [14](#)

Issues

 integration [16](#)

L

Limitations
 integration [16](#)

P

Platforms
 Supported [11](#)
Professional Services [8](#)
Proxy Server
 Documentation [8](#)

R

References [7](#)

S

Security Architecture

Siebel 7.5 [10](#)

Solaris

Patches [8](#)

Support [8](#)

Sun ONE

Support [8](#)

Support

Professional Services [8](#)

Solaris [8](#)

Sun ONE [8](#)

W

Web Server

Documentation [8](#)