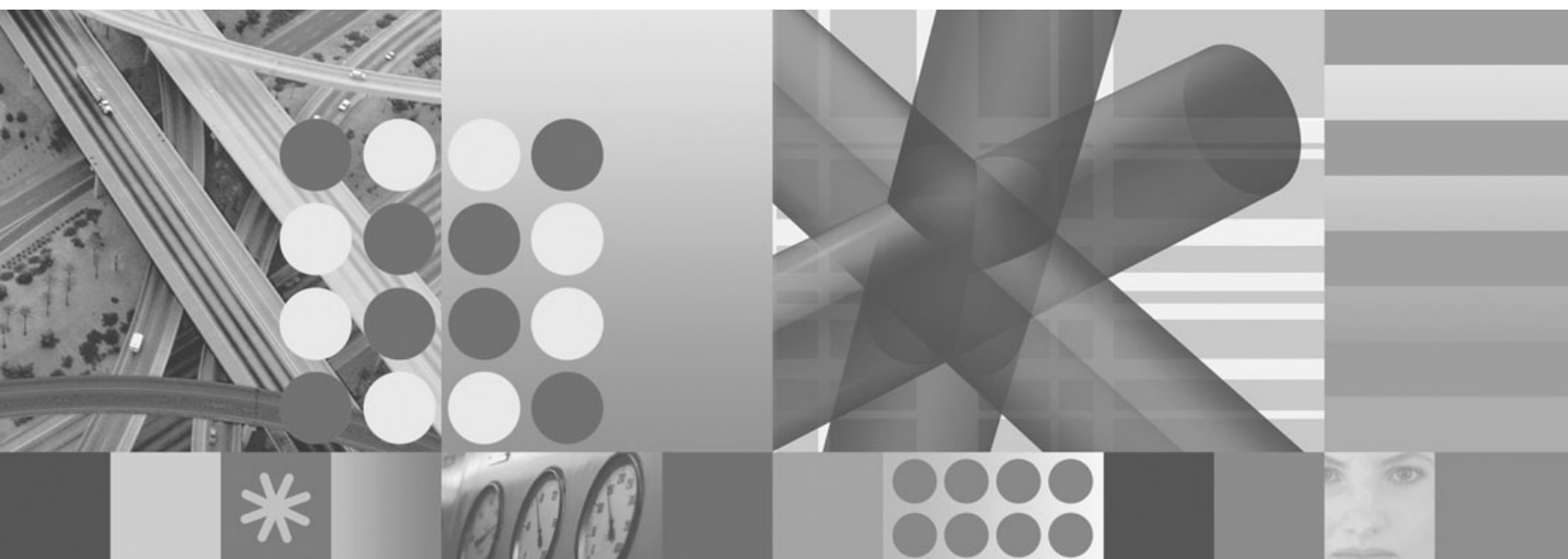




**Siebel eBusiness Applications 7.5, 7.7, 7.8 or 8.0  
Integration Guide**





**Siebel eBusiness Applications 7.5, 7.7, 7.8 or 8.0  
Integration Guide**

**Note**

Before using this information and the product it supports, read the information in Appendix B, “Notices,” on page 49.

This edition applies to version 3.0.06 of the Tivoli Access Manager Integration with Siebel eBusiness Applications, and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2004, 2008.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

|                                                                                           |               |
|-------------------------------------------------------------------------------------------|---------------|
| <b>Preface</b>                                                                            | <b>v</b>      |
| Who should read this book                                                                 | v             |
| Publications                                                                              | v             |
| Base Information                                                                          | v             |
| WebSEAL Information                                                                       | v             |
| Accessing Publications Online                                                             | vi            |
| Contacting Software Support.                                                              | vi            |
| Tivoli technical training                                                                 | vi            |
| Conventions Used in this Book.                                                            | vii           |
| <br><b>Chapter 1. Introduction</b>                                                        | <br><b>1</b>  |
| Integration Scenario One: Siebel LDAP Security Adapter.                                   | 1             |
| Integration Scenario Two: Tivoli Access Manager Security Adapter for Siebel               | 3             |
| Overview of the Siebel Security Model                                                     | 4             |
| Integration Scenario Three: Tivoli Access Manager Lightweight Security Adapter for Siebel | 5             |
| Limitations                                                                               | 7             |
| Integration Product Versions and Supported Platforms                                      | 7             |
| Integration Package Contents                                                              | 7             |
| Integration Process Flow                                                                  | 8             |
| Integration Checklist                                                                     | 10            |
| <br><b>Chapter 2. Integration Process</b>                                                 | <br><b>11</b> |
| Before You Start                                                                          | 11            |
| WebSEAL Configuration                                                                     | 12            |
| Creating a WebSEAL Junction                                                               | 12            |
| WebSEAL Configuration options                                                             | 12            |
| WebSEAL Login Page Modification                                                           | 13            |
| Tivoli Access Manager Configuration                                                       | 13            |
| Siebel Configuration                                                                      | 16            |
| Configuring the Siebel Web Extension                                                      | 16            |
| Modifying Default.htm in Siebel 7.7, 7.8 and 8.0                                          | 17            |
| Security Adapter Configuration in Siebel 7.5                                              | 17            |
| Configuring Siebel Applications in Siebel 7.5                                             | 22            |
| Security Adapter Configuration in Siebel 7.7, 7.8 and 8.0                                 | 23            |
| Configuring Siebel Applications in Siebel 7.7, 7.8 and 8.0                                | 27            |
| Configuring Siebel Logout Behavior                                                        | 28            |
| Checking the Integration                                                                  | 30            |
| Test Programs                                                                             | 31            |
| pdadmin_pool_test                                                                         | 31            |
| PDSiebelTest                                                                              | 31            |
| pd_siebel_test_setup.pdadmin                                                              | 32            |
| pd_siebel_test_cleanup.pdadmin                                                            | 32            |
| Uninstallation                                                                            | 33            |
| <br><b>Chapter 3. Additional Notes</b>                                                    | <br><b>37</b> |
| Actuate Reports for Siebel                                                                | 37            |
| WebSEAL Junction Creation to the Actuate Server                                           | 37            |
| Configuring Actuate Reports for Siebel 7.5                                                | 37            |
| Configuring Actuate Reports for Siebel 8.0                                                | 38            |
| Siebel Computer Telephony Integration (CTI)                                               | 38            |
| WebSEAL Filtering for CTI                                                                 | 38            |
| Siebel Analytics 7.8.2                                                                    | 39            |
| Troubleshooting                                                                           | 40            |
| Known Issues                                                                              | 42            |

|                                                               |           |
|---------------------------------------------------------------|-----------|
| <b>Appendix A. IBM Software Support</b>                       | <b>45</b> |
| Determine the business impact of your problem                 | 45        |
| Describe your problem and gather background information       | 46        |
| Submit your problem to IBM Software Support                   | 46        |
| Searching knowledge bases                                     | 46        |
| Search the information center on your local system or network | 47        |
| Search the Internet                                           | 47        |
| Obtaining fixes                                               | 47        |
| <b>Appendix B. Notices</b>                                    | <b>49</b> |
| Trademarks                                                    | 51        |

---

## Preface

This guide tells you how to configure and manage your IBM® Tivoli® Access Manager version 5.1 installation to work with Siebel eBusiness Applications version 7.5, 7.7, 7.8 or 8.0.

This document assumes that both Tivoli Access Manager and Siebel are installed, configured and running on your network. This guide does not provide details on the installation and administration of these products, except where necessary to achieve integration.

---

## Who should read this book

This guide is for those responsible for the installation, deployment and administration of IBM Tivoli Access Manager and Siebel. The reader should be familiar with the administration of Tivoli Access Manager, Tivoli Access Manager WebSEAL and Siebel products, including eBusiness Applications and Siebel Tools.

Readers should also be familiar with the following:

- PC and UNIX® operating systems,
- Security management,
- Internet protocols, including HTTP, HTTPS and TCP/IP,
- Lightweight Directory Access Protocol (LDAP) and directory services,
- A supported user registry,
- Authentication and authorization.

---

## Publications

The following publications complement the information contained in this guide:

### Base Information

- *IBM Tivoli Access Manager Base Installation Guide*  
Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Tivoli Access Manager Base Administrator's Guide*  
Describes the concepts and procedures for using Access Manager services. Provides instructions for performing tasks from the Web portal manager interface and by using the **pdadmin** command.

### WebSEAL Information

- *IBM Tivoli Access Manager WebSEAL Installation Guide*  
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Tivoli Access Manager WebSEAL Administrator's Guide*  
Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.
- *IBM Tivoli Access Manager WebSEAL Developer's Reference*

Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

## Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli software library:

<http://www.ibm.com/software/tivoli/library>

To locate product publications in the library, click the **Product manuals** link on the left side of the page. Then, locate and click the name of the product on the Tivoli Software Information Center page.

Product publications include release notes, installation guides, user's guides, administrator's guides, and developer's references.

**Note:** To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe® Acrobat Print window (which is available when you click **File →Print**).

---

## Contacting Software Support

Contact IBM Software Support by using the methods described in the *IBM Software Support Guide* at the following Web site:

<http://techsupport.services.ibm.com/guides/handbook.html>

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers, depending on the country in which you are located
- A list of information you should gather before contacting customer support

For more information, see Appendix A, "IBM Software Support," on page 45.

---

## Tivoli technical training

For Tivoli technical training information, refer to the IBM Tivoli Education Web site: <http://www.ibm.com/software/tivoli/education>.

---

## Conventions Used in this Book

The following typeface conventions are used in this book:

**Bold** Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java™ classes, and objects are in **bold**.

*Italic* Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

Monospace

Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in monospace.



---

## Chapter 1. Introduction

This guide describes the procedures for integrating IBM Tivoli Access Manager for e-business with Siebel eBusiness Applications to achieve Single Sign-On (SSO) capability.

This chapter introduces the available integration scenarios and their limitations, describes the supported product versions and platforms, details the contents of the integration package and provides a process flow diagram and checklist to assist you as you work through the integration process.

Three different integration scenarios are possible:

**Integration Scenario One: Siebel LDAP Security Adapter**

See “Integration Scenario One: Siebel LDAP Security Adapter.”

**Integration Scenario Two: Tivoli Access Manager Security Adapter for Siebel**

See “Integration Scenario Two: Tivoli Access Manager Security Adapter for Siebel” on page 3.

**Integration Scenario Three: Tivoli Access Manager Lightweight Security Adapter for Siebel**

See “Integration Scenario Three: Tivoli Access Manager Lightweight Security Adapter for Siebel” on page 5.

The integration solution that best suits your company will depend on your Siebel environment and security requirements.

---

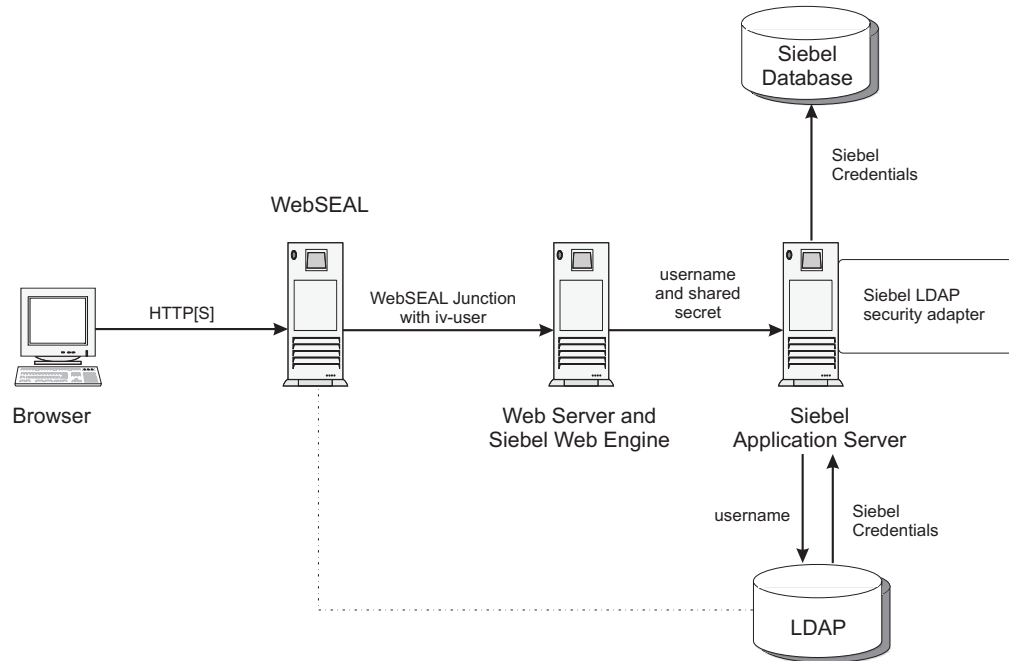
### Integration Scenario One: Siebel LDAP Security Adapter

This scenario describes the procedures necessary to configure your Tivoli Access Manager environment to achieve single sign-on to the Siebel eBusiness Applications components using the Siebel LDAP security adapter. This solution requires Tivoli Access Manager and Siebel user ID's to be matched.

User credentials in the form of an HTTP header are passed from Tivoli Access Manager WebSEAL to the Siebel Application, which then performs a lookup on the LDAP registry to retrieve the credentials required to log onto the Siebel database.

The diagram below shows an integration scenario architecture which supports the following processes:

1. A client requests a Siebel resource through the WebSEAL junction.
2. WebSEAL intercepts the request, authenticates and authorizes the user, then passes the username in the HTTP header (iv-user) to the Siebel Web Extension.
3. The username and preconfigured shared secret are then passed to the Siebel Application Server.
4. The Siebel application server passes the username to the LDAP directory through the Siebel LDAP security adapter. Based on the received username, the Siebel application server retrieves the corresponding credentials from the LDAP registry.
5. The retrieved credential is then used by the Siebel application to log the user on to the Siebel database.



*Figure 1. Scenario One: Tivoli Access Manager integration with Siebel using the Siebel LDAP security adapter*

Using this scenario, the Siebel server can only be administered through the dedicated client. Administration is not possible when signing on through WebSEAL.

External role management with the LDAP security adapter involves listing the roles of the user (as a comma separated list) in a selected LDAP attribute. Refer to the *Security Guide for Siebel eBusiness Applications* section of the *Siebel Bookshelf* for details.

---

## Integration Scenario Two: Tivoli Access Manager Security Adapter for Siebel

Siebel's eBusiness Applications provide a security adapter interface that permits the integration of an external user registry, through the implementation of a third party security adapter. This security adapter interface allows for external management of Siebel roles and credentials for enterprise systems.

This integration scenario provides the steps required to configure both Tivoli Access Manager and Siebel to utilize the Tivoli Access Manager security adapter. User and Role management are externalized to Tivoli Access Manager. The Administrator can use Tivoli Access Manager user groups to delegate Siebel Role memberships to Tivoli Access Manager users. The administration interface is less complex than that provided by the LDAP adapter. This solution is independent of the solution detailed in Scenario One.

This scenario allows a Siebel Administrator to administer the server remotely.

**Note:** The security adapter does not check the user's password. In browser-based applications, where single sign-on with WebSEAL is configured, the SSO mechanism relieves the adapter of this need. The security adapter does not cater for use without single sign-on through Tivoli Access Manager.

The diagram below shows an integration scenario architecture which supports the following processes:

1. A client requests a Siebel resource.
2. WebSEAL authenticates the client, and passes the username (as iv-user) in the HTTP header to the Siebel Web Extension (SWE).
3. The Siebel Web Extension passes the username along with the shared secret to the Siebel Application Server.
4. The Siebel Application Server invokes the security adapter in order to retrieve the credentials needed for the client to log onto the Siebel database.
5. The security adapter contacts Tivoli Access Manager. By making use of the Tivoli Access Manager GSO resource credential feature it retrieves the Siebel credentials for the user from the corresponding Tivoli Access Manager GSO resource credential.
6. The Siebel credentials are passed back to the Siebel Application server.
7. The credentials are then used to log on to the Siebel resource.

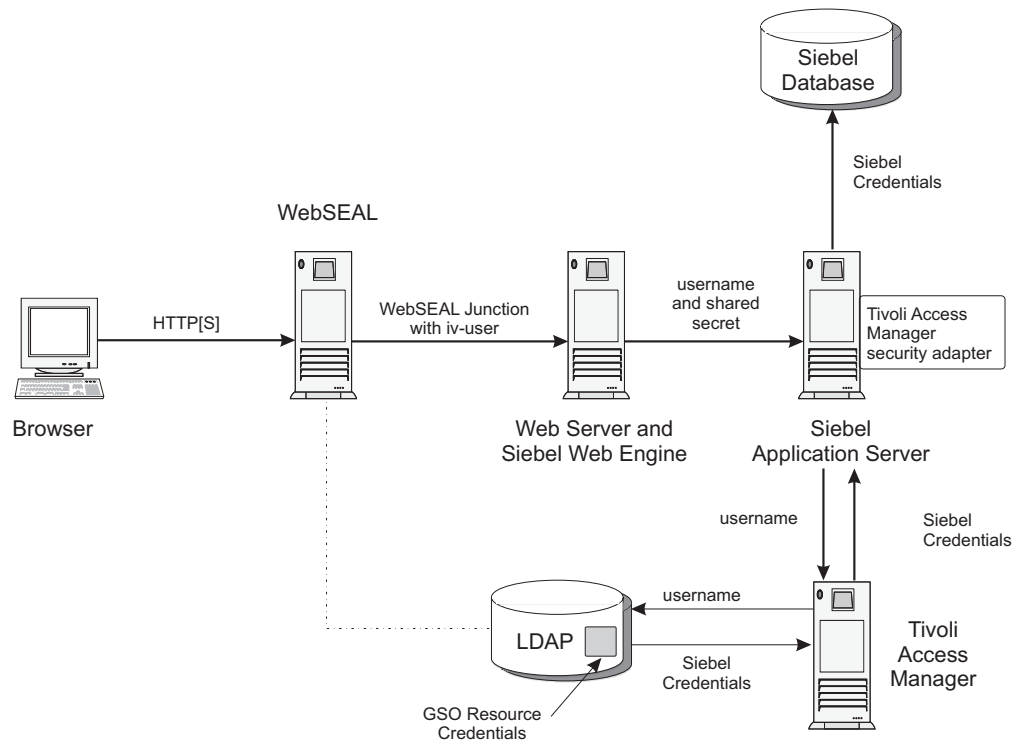


Figure 2. Scenario Two: Tivoli Access Manager integration with Siebel using the Tivoli Access Manager security adapter.

An overview of the Siebel Security Model and a description of how it maps to the Tivoli Access Manager Security Model is given below.

## Overview of the Siebel Security Model

The Siebel security model uses the following entities:

### User

The user entity is the fundamental representation of a user in the Siebel security model. Attributes of a user are:

- Username
- Password
- Account Status
- Set of roles
- Set of credentials

**Roles** A role in the Siebel system is a user attribute from which access control or entitlements information is derived. A user can have one or more roles in the system. A role is also defined as a *Responsibility* in many of the Siebel user interfaces. Responsibilities control which Views a user may see in the system.

### Credentials

Credentials are data that Siebel uses to authenticate a user to a data repository. A user may have one or more credentials. A Siebel implementation may also have a default credential that can be shared by multiple users that may not have a credential specific to them. A credential is defined by the following attributes:

- Credential type

- Username
- Password

### Mapping the Tivoli Access Manager Security Model

The security adapter developed for this Tivoli Access Manager integration maps the Siebel entities as follows:

| Siebel Entity  | Tivoli Access Manager Representation |
|----------------|--------------------------------------|
| Responsibility | Group                                |
| Credential     | GSO Resource Credential              |
| User           | User                                 |

Tivoli Access Manager groups and resource credentials are used for purposes other than just authorization and single sign-on solutions. Therefore the security adapter for this integration has configurable prefixes for the group names and resource credentials that map to Siebel roles and credentials. By default these prefixes are:

| Siebel Entity  | Tivoli Access Manager Representation | Default Prefix |
|----------------|--------------------------------------|----------------|
| Responsibility | Group                                | SiebelRole-    |
| Credential     | GSO Resource Credential              | SiebelCred-    |

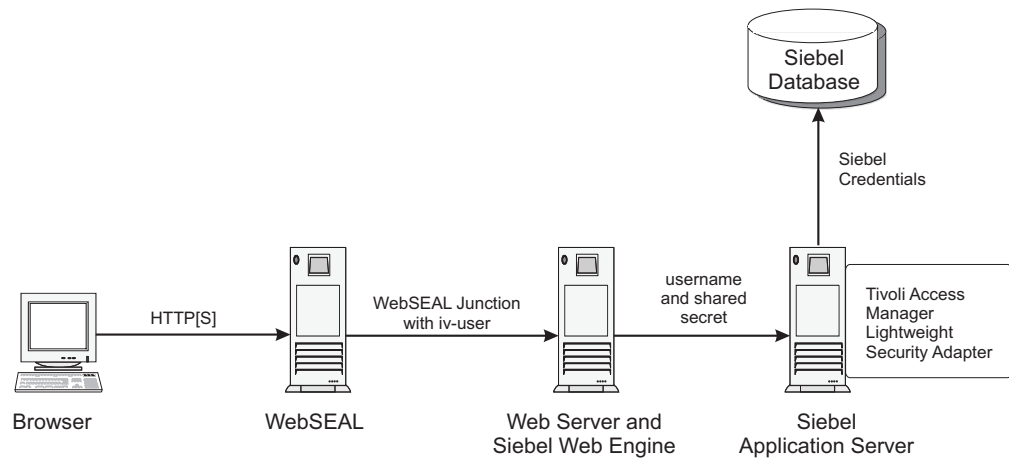
---

## Integration Scenario Three: Tivoli Access Manager Lightweight Security Adapter for Siebel

The Lightweight Security Adapter for Siebel provides the functionality to store logon details for the Siebel Database in a local configuration file. This is useful in heavily firewalled architectures where communication from the Siebel server is undesirable, other than standard web traffic. As stated in the introduction to this guide, User and Role management is administered through Siebel. The adapter does not provide this functionality.

The integration solution that best suits your company will depend on your Siebel environment and security requirements.

**Note:** The security adapter does not check the user's password. In browser-based applications, where single sign-on with WebSEAL is configured, the SSO mechanism relieves the adapter of this requirement. The security adapter does not cater for use without single sign-on through Tivoli Access Manager.



*Figure 3. Scenario Three: Tivoli Access Manager integration with Siebel using the Tivoli Access Manager Lightweight Security Adapter.*

The diagram above shows an integration scenario architecture which supports the following processes:

1. A client requests a Siebel resource.
2. WebSEAL authenticates the client, and passes the username (as iv-user) in the HTTP header to the Siebel Web Extension (SWE).
3. The Siebel Web Extension passes the username along with the shared secret to the Siebel Application Server.
4. The Siebel Application Server calls the security adapter, which returns to the Siebel server the credentials needed to log the user into the Siebel database. The credentials are stored in a local configuration file for the Siebel Application.
5. The credentials are then used to log onto the Siebel database.

---

## Limitations

All of the scenarios described in this document make use of Siebel's Web SSO feature. The following capabilities are not available as Siebel eBusiness Applications features in a Web SSO environment:

- User self-registration,
- Delegated administration of users,
- Login forms,
- Change password.

For further information regarding Web SSO, Security Adapter functionality and limitations refer to the *Security Guide for Siebel eBusiness Applications* section of the *Siebel Bookshelf*.

---

## Integration Product Versions and Supported Platforms

The integration detailed in this guide has been tested against, and is supported for, the following product versions:

- Siebel 7.5.3.7 (or above), 7.7.1, 7.8.1, or 8.0
- IBM Tivoli Access Manager Base version 5.1 and
- IBM Tivoli Access Manager WebSEAL version 5.1

The Tivoli Access Manager Security Adapters provided are currently supported on Windows® 2003 and AIX® 5.2 and 5.3.

---

## Integration Package Contents

The integration package contains the following files:

- This integration guide (am\_siebel\_int\_guide.pdf).
- A TAMLogout.swt file, for use with each of the integration scenarios.
- Security adapter libraries for the following platforms:

### Windows:

TAM Security Adapter

- PDSiebel\am51\x86\_nt\_5\PDSiebel.dll

Lightweight TAM Security Adapter

- PDSiebelLite\PDSiebelLite.dll

### AIX:

TAM Security Adapter

- PDSiebel\am51\rios\_aix\_5\libPDSiebel.a

Lightweight TAM Security Adapter

- PDSiebelLite\libPDSiebelLite.a

**Test Programs:****For Windows**

TAM Security Adapter

- PDSiebel\am51\x86\_nt\_5\PDSiebelTest.exe
- PDSiebel\am51\x86\_nt\_5\pdadmin\_pool\_test.exe

**For AIX**

TAM Security Adapter

- PDSiebel\am51\rios\_aix\_5\PDSiebelTest
- PDSiebel\am51\rios\_aix\_5\pdadmin\_pool\_test

**Pdadmin setup and cleanup scripts:**

- pd\_siebel\_test\_setup.pdadmin
- pd\_siebel\_test\_cleanup.pdadmin

---

## Integration Process Flow

The diagram below illustrates the optional paths that can be followed through the various integration procedures described in this document in order to achieve integration. Each task is detailed fully in Chapter 2, “Integration Process,” on page 11.

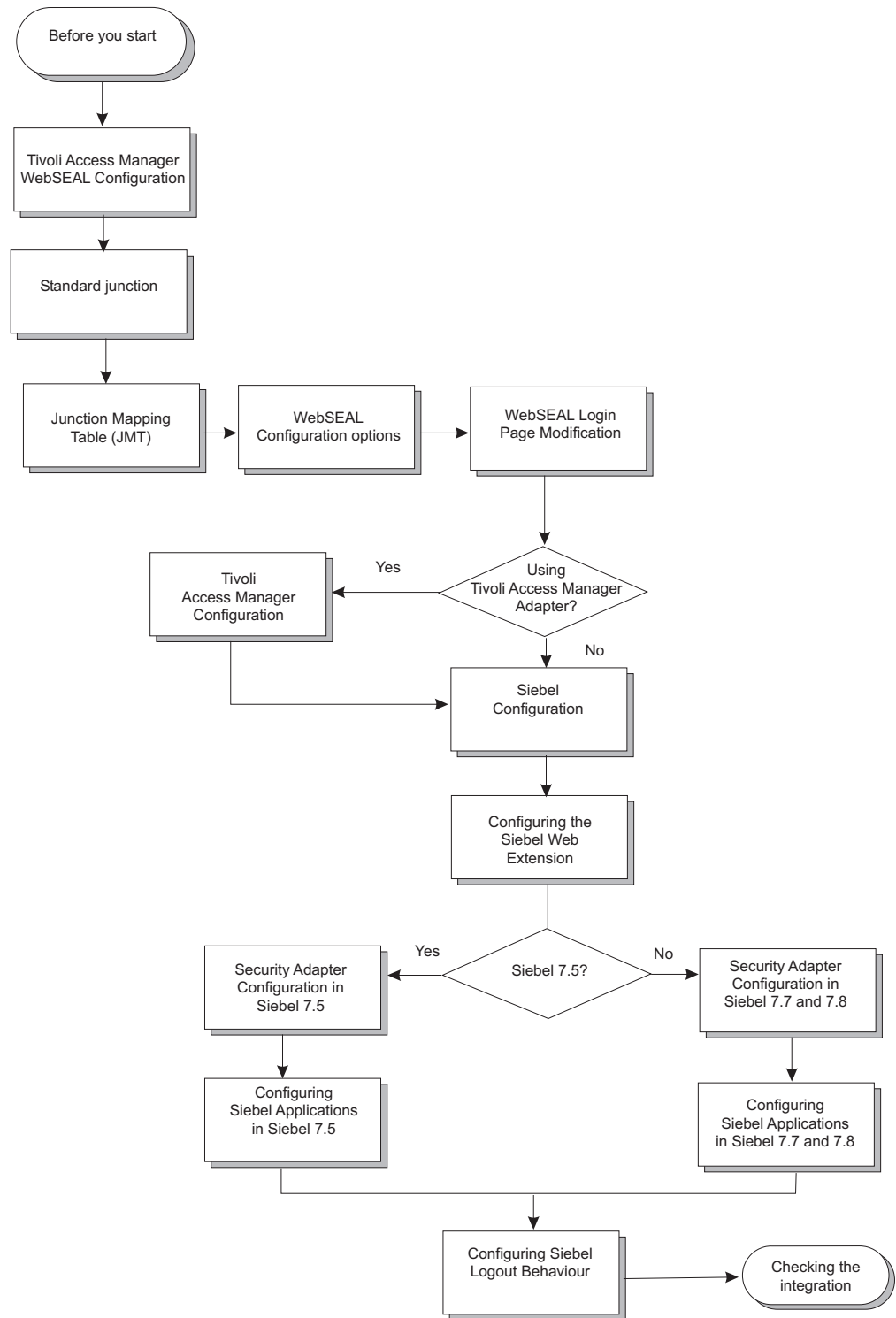


Figure 4. Integration Process Flow

---

## Integration Checklist

The following tables can be printed and used as a checklist to assist you as you work through the integration process. A list of each major task heading is provided, with a check box next to it. Each task is detailed fully in Integration Process.

Fill out the **Planning** column prior to starting the integration. Once all steps for the heading are complete, return to this page and check the appropriate box in the **Completed** column.

*Table 1. Tivoli Access Manager Configuration*

| Planning                                                       | Completed                     | Task Heading                        |
|----------------------------------------------------------------|-------------------------------|-------------------------------------|
| ✓ To Do                                                        | <input type="checkbox"/> Done | Creating a junction                 |
| <input type="checkbox"/> To Do<br><input type="checkbox"/> N/A | <input type="checkbox"/> Done | Junction Mapping Table (JMT)        |
| <input type="checkbox"/> To Do<br><input type="checkbox"/> N/A | <input type="checkbox"/> Done | WebSEAL Configuration Options       |
| ✓ To Do                                                        | <input type="checkbox"/> Done | WebSEAL Login Page Modification     |
| <input type="checkbox"/> To Do<br><input type="checkbox"/> N/A | <input type="checkbox"/> Done | Tivoli Access Manager Configuration |

*Table 2. Siebel Configuration*

| Planning                                                       | Completed                     | Task Heading                                                                                                                               |
|----------------------------------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ To Do                                                        | <input type="checkbox"/> Done | Configuring the Siebel Web Extension                                                                                                       |
| <input type="checkbox"/> To Do<br><input type="checkbox"/> N/A | <input type="checkbox"/> Done | Security Adapter Configuration: <ul style="list-style-type: none"><li>• in Siebel 7.5, or</li><li>• in Siebel 7.7, 7.8 and 8.0.</li></ul>  |
| <input type="checkbox"/> To Do<br><input type="checkbox"/> N/A | <input type="checkbox"/> Done | Configuring Siebel Applications: <ul style="list-style-type: none"><li>• in Siebel 7.5, or</li><li>• in Siebel 7.7, 7.8 and 8.0.</li></ul> |
| ✓ To Do                                                        | <input type="checkbox"/> Done | Configuring the Siebel Logout behavior                                                                                                     |
| ✓ To Do                                                        | <input type="checkbox"/> Done | Testing the Integration                                                                                                                    |

---

## Chapter 2. Integration Process

This chapter contains the following sections:

- “Before You Start”
- “WebSEAL Configuration” on page 12
- “Siebel Configuration” on page 16
- “Checking the Integration” on page 30
- “Uninstallation” on page 33

---

### Before You Start

For security reasons, you should ensure that the only network path to the Siebel Web Servers endpoint is through WebSEAL. When this integration is applied, the SWE is configured to extract user data from the HTTP request. Any HTTP request through a browser to the Siebel Application server, from any machine other than the Application Server itself, will result in an error (because the HTTP request does not contain an iv-user component). By ensuring that WebSEAL provides the only network path to the Siebel Web Servers endpoint, users are prevented from accessing the Siebel Web Extension (SWE) directly and masquerading as a different users.

For integration scenarios 1 and 2, it is assumed that Tivoli Access Manager and Siebel are sharing the same LDAP user registry. If this is not the case, you can still implement this integration scenario, provided user names are the same across the different registries. A directory synchronization tool such as IBM Directory Integrator (IDI) can be used for this purpose.

For all integration scenarios, to achieve single sign on capability, Tivoli Access Manager user names must match the user names in the Siebel user table. Before you begin this integration, ensure that users have a valid account in both the Tivoli Access Manager LDAP directory and the Siebel user table.

During the integration process, remember to always make backup copies of any files you modify, particularly configuration files.

---

## WebSEAL Configuration

This section details the integration steps required on Tivoli Access Manager WebSEAL.

### Creating a WebSEAL Junction

A standard WebSEAL junction must be created to connect WebSEAL with the Siebel Web Extension. The WebSEAL junction can be configured to use either TCP or SSL (recommended).

The junction creation command must specify the `-c iv_user` option, which configures WebSEAL to send the authenticated username in the `iv-user` HTTP header.

Example command for a standard junction (entered as one line):

```
pdadmin> server task instance-webseald-server_name create -t tcp  
-h siebel_fqdn -p port_no -c iv_user /junction_name
```

For more detailed instructions on WebSEAL junction creation, refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide*.

After creating a Standard junction as described above, proceed to “Junction Mapping Table (JMT).”

### Junction Mapping Table (JMT)

Server-relative URLs generated on the client-side by applets and scripts initially lack knowledge of the junction point. WebSEAL cannot filter such URLs because they are generated dynamically on the client side. During a client request for a resource using such a URL, WebSEAL can attempt to reprocess the server-relative URL using a pre-defined mapping table.

Perform the following tasks to create and configure a junction mapping table:

1. Open the Tivoli Access Manager WebSEAL configuration file:  
`webseal_install_dir/etc/webseald-instance.conf`
2. Within the [junction] stanza, ensure the value of the `jmt-map` option is set to `jmt.conf`.
3. If there is no previously created `jmt.conf` file, create the file in the directory `webseal_install_dir/www-instance/lib`.
4. Modify the `webseal_install_dir/www-instance/lib/jmt.conf` file to create a mapping table for each Siebel resource that is being protected. The format for entry into this file consists of the junction name followed by a space, and then the resource location pattern. For example, the entries for the **esales\_enu** and **echannel\_enu** components would be:

```
/siebel /esales_enu/*  
/siebel /echannel_enu/*
```

where `/siebel` is the junction to the Siebel server.

After creating a Junction Mapping Table as described above (if required), proceed to “WebSEAL Configuration options.”

### WebSEAL Configuration options

Locate the WebSEAL configuration file, `webseald.conf`, located in the directory `WebSEAL_install_dir/etc\`.

Within the **[script-filtering]** stanza, enable the **script-filter** and **rewrite-absolute-with-absolute** parameters. For example:

```
[script-filtering]
script-filter=yes
...
rewrite-absolute-with-absolute=yes
```

Restart WebSEAL for the above changes to take effect.

After modifying the WebSEAL configuration options as described above, proceed to “WebSEAL Login Page Modification.”

## WebSEAL Login Page Modification

Modify the WebSEAL login page as follows:

1. Add the following JavaScript™ code into the top of the body (<BODY></BODY>) section, above any other JavaScript code:

```
<!-- Siebel Add-in -->
<script>
{
    if (top.SWEReloadApp !=null)
    {
        top.SWEReloadApp();
    }
}
</script>
```

2. Save the login page change.
3. Restart WebSEAL.

**Note:** The WebSEAL login page is located in the following directory (on Windows, for example):

*WebSEAL\_install\_dir/www-instance/lib/htm/locale/login.html*

After modifying the WebSEAL Login Page as described above:

- If you are using the LDAP security adapter or the Tivoli Access Manager Lite security adapter, proceed to “Siebel Configuration” on page 16.
- If you are using the Tivoli Access Manager security adapter proceed to “Tivoli Access Manager Configuration,”

## Tivoli Access Manager Configuration

This section describes the additional configuration steps required for Tivoli Access Manager.

**Note:** This section is not relevant if you are using the LDAP Security Adapter or the Tivoli Access Manager Lightweight Security Adapter. If so, proceed to “Siebel Configuration” on page 16.

### Installing Tivoli Access Manager Components

On the machine running Siebel with the Tivoli Access Manager security adapter, the following components must be installed:

#### IBM GSKit

Appropriate for the Tivoli Access Manager Policy Server version.

#### IBM Tivoli LDAP Client

Appropriate for the Tivoli Access Manager Policy Server version.

## Tivoli Access Manager Runtime Environment

Configured into an appropriate Tivoli Access Manager domain

### CAUTION:

**When installing the LDAP client on the Siebel machine, ensure that the Siebel Gateway, Siebel Server and IIS are stopped before beginning the installation.**

For details on installing and configuring these components, refer to the *Tivoli Access Manager Base Installation Guide*.

## Configuring Tivoli Access Manager

The following steps require the use of the Tivoli Access Manager command line utility **pdadmin**. For detailed information about **pdadmin** commands, refer to the *IBM Tivoli Access Manager Base Administrator's Guide* and *IBM Tivoli Access Manager Command Reference*.

Configure Tivoli Access Manager as follows:

1. The Tivoli Access Manager user names must exactly match the user names in the Siebel user registry. Ensure that users have a valid account in both the Tivoli Access Manager LDAP directory and the Siebel user table. To create the users in Tivoli Access Manager, use the **pdadmin** command line utility. For example (enter each command as one line):

```
pdadmin>user create -gsouser testuser cn=testuser,o=tivoli,c=us  
testuser testuser password
```

```
pdadmin>user modify testuser account-valid yes
```

**Note:** In the first command, the **-gsouser** option creates the user as a GSO user. This is required so that the user is associated with Tivoli Access Manager GSO resource credentials that are returned, allowing the user to log onto the Siebel database. You must:

- create a user called **sadmin** in Tivoli Access Manager, to correspond with the Siebel administrator account, and
  - assign resource credentials to this user, using the steps in this section.
2. Create Siebel roles as Tivoli Access Manager groups and add any users to the group. For example (enter each command as one line):

```
pdadmin>group create SiebelRole-Employee  
cn=SiebelRole-Employee,o=acme,c=au SiebelRole-Employee
```

```
pdadmin>group modify SiebelRole-Employee add testuser
```

where *Employee* is the name of the Siebel responsibility that the user is to have, and where *SiebelRole* is the **RoleGroupPrefix** (as described in the table under the section “Tivoli Access Manager Adapter Parameters” on page 19).

3. Create GSO resources, **ServerDataSrc** and **GatewayDataSrc**. For example (enter each command as one line):

```
pdadmin> rsrc create SiebelCred-ServerDataSrc
```

```
pdadmin> rsrc create SiebelCred-GatewayDataSrc
```

where *SiebelCred* is the **CredentialTypePrefix** (as described in the table under the section “Tivoli Access Manager Adapter Parameters” on page 19).

4. Create the Siebel credentials for the **ServerDataSrc** resource as Tivoli Access Manager resource credentials. For example (entered as one line):

```
pdadmin> rsrccred create SiebelCred-ServerDataSrc rsrcuser siebel_db_user  
rsrcpwd siebel_db_password rsrctype web user testuser
```

where:

- *siebel\_db\_user* and *siebel\_db\_password* are the username and password combination required to log onto the Siebel database.
  - GSO Resource credentials can be either:
    - created for each individual user, or
    - created for one default user so that other users will then use these credentials (the default user is specified in a Siebel configuration file, as described in Siebel Configuration).
5. Create GatewayDataSrc credentials for users requiring administrative access, specifying a username and password for a Siebel user with administrative access. For example (entered as one line):

```
pdadmin> rsrccred create SiebelCred-GatewayDataSrc rsrcuser siebel_admin_user  
rsrcpwd siebel_admin_password rsrctype web user testuser
```

where:

- *siebel\_admin\_user* is a user with administrative privileges, and
- *siebel\_admin\_password* is their password.

**Note:** **GatewayDataSrc** credentials should not be created for a default user. Only assign **GatewayDataSrc** credentials for individual administrative users.

**SIEBEL 8.0 ONLY:** Create an additional GSO resource SiebelDB. For example (enter each command as one line):

```
pdadmin> rsrc create SiebelCred-SiebelDB
```

Create the Siebel credentials for the SiebelDB resource as Tivoli Access Manager resource credentials. For example (entered as one line):

```
pdadmin> rsrccred create SiebelCred-SiebelDB rsrcuser siebel_db_user  
rsrcpwd siebel_db_password rsrctype web user testuser
```

After performing the Tivoli Access Manager Configuration as described above proceed to “Siebel Configuration” on page 16.

---

## Siebel Configuration

This sections details the steps required to configure the Siebel Web Extension, the Security Adapter, the Siebel Applications and the Siebel logout behavior.

### Configuring the Siebel Web Extension

When setting up the junction in the previous section, the `-c iv-user` option was specified, causing WebSEAL to pass the username of the authenticated user in the HTTP header. The Siebel Web Extension must now be configured to extract the username from the HTTP header of the incoming request. It can then forward the username to the Siebel server.

Configure the Siebel Web Extension as follows:

1. Edit the Siebel Web Extension configuration file `eapps.cfg` (located in the `Siebel_install_dir/SWEApp/bin` directory) to read the HTTP header and pass the username to the Siebel Applications. For example, to enable SSO for the `callcenter_enu` and `esales_enu` applications, the sections for each of those applications in the configuration file `eapps.cfg` would be as follows:

```
[/callcenter_enu]
...
SingleSignOn = TRUE
UserSpec = IV-USER
UserSpecSource = Header
ProtectedVirtualDirectory = /callcenter_enu

[/esales_enu]
...
SingleSignOn = TRUE
UserSpec = IV-USER
UserSpecSource = Header
ProtectedVirtualDirectory = /esales_enu
```

**Note:** The Siebel Web Extension explicitly trusts the information it receives in the HTTP request. For security reasons you should ensure that the only network path to the Siebel Web server's endpoint is through WebSEAL. This prevents users accessing the Siebel Web Extension directly and masquerading as a different user. If this is not possible, the use of SSL junctions is recommended.

Make the above changes for each Siebel application requiring Tivoli Access Manager protection and single sign on capability.

2. Configure a shared secret that can be distributed between the Siebel Web Extension and the applications, so that information can be trusted. The secret is specified in the Siebel configuration file, `eapps.cfg`, as follows:

```
[defaults]
...
TrustToken = sso_shared_secret
```

3. Next, set the username for the anonymous user in the Siebel `eapps.cfg` configuration file for each Siebel application requiring protection. This username represents the privileges of an anonymous user. It should match a username found in the Siebel user table. For example:

```
[defaults]
...
AnonUserName=anon_user
AnonPassword=anon_password
```

**Note:** If applicable, you may be required to set `EncryptedPassword = False` if using a plaintext **TrustToken** and **AnonPassword**. You could however,

use the **encryptstring** utility to encrypt the **TrustToken** and **AnonPassword**. For more details, refer to the Siebel documentation.

4. Configure the Siebel Web Extension Server to disable compression:  
[defaults]  
...  
DoCompression = FALSE
5. Set the Siebel session timeout to be at least 5 minutes greater than the WebSEAL inactive timeout. For example:  
[defaults]  
...  
SessionTimeout=1800
6. After performing the above changes, save and close the file.

For Siebel 7.7, 7.8 and 8.0, proceed to “Modifying Default.htm in Siebel 7.7, 7.8 and 8.0.”

For Siebel 7.5, proceed to “Security Adapter Configuration in Siebel 7.5.”

## Modifying Default.htm in Siebel 7.7, 7.8 and 8.0

1. Open *Siebel\_install\_dir/SWEApp/PUBLIC/lang/default.htm*.
2. Locate the following GotoUrl JavaScript function:

```
function GotoUrl(url)
{
    // Append the current hostname to the server request
    // so that the server has
    // the top level host name. This is needed to support
    // reverse proxy servers.
    url += "&SWEHo=" + this.location.hostname;
    this.location = unescape(this.location.pathname) + url;
}
```

3. Change this to:

```
function GotoUrl(url)
{
    // Append the current hostname to the server request
    // so that the server has
    // the top level host name. This is needed to support
    // reverse proxy servers.
    url += "&SWEHo=Siebel_webserver_hostname/FQDN";
    this.location = unescape(this.location.pathname) + url;
}
```

where *Siebel\_webserver\_hostname/FQDN* is the value used in the -h (or -v, if used) parameter of the **junction create** command in WebSEAL.

4. Save and close the file.
5. Restart the Web Server.

After configuring the Siebel Web Extension, proceed to “Security Adapter Configuration in Siebel 7.7, 7.8 and 8.0” on page 23.

## Security Adapter Configuration in Siebel 7.5

Edit the configuration file for each Siebel application object to enable WebSEAL support and single sign-on, and to specify a shared secret that matches the one entered in the Siebel Web Extension configuration file.

Each Siebel application object has a corresponding configuration file, usually located in the *Siebel\_install\_dir/siebsvr/bin/lang* directory (for example, *esales.cfg* for *esales*, or *uagent.cfg* for *callcenter*).

Add the following lines to the [SWE] section:

```
EnableWebSealSupport=TRUE
DoCompression=FALSE
```

The security adapter parameters are specified in the stanza of the configured security adapter.

Proceed to the correct section for parameter configuration:

**If you are implementing the LDAP Security Adapter**

Proceed to “LDAP security adapter parameters.”

**If you are implementing the Tivoli Access Manager Security Adapter**

Proceed to “Tivoli Access Manager Adapter Parameters” on page 19.

**If you are implementing the Tivoli Access Manager Lite Security Adapter**

Proceed to “Tivoli Access Manager Lite Adapter Parameters” on page 21.

## LDAP security adapter parameters

The mandatory parameters for the LDAP security adapter are shown below with sample values:

```
[SecurityAdapters]
LDAP = LDAP

[LDAP]
...
SingleSignOn = TRUE
TrustToken = sso_shared_secret
...
DllName           = sscfldap.dll
ServerName        = ldap_server_fqdn
Port              = 389
BaseDN            = "o=Acme,c=au"
SharedCredentialsDN = "uid=sadmin,o=Acme,c=au"
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = mail
ApplicationUser    = "cn=root"
ApplicationPassword = password
```

**Note:** Plain spaces should be used in the configuration files. The use of tabs to separate parameters may cause errors.

The following table describes the required parameters:

*Table 3. SSO configuration parameters*

| Parameter                  | Use                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DllName</b>             | The Siebel LDAP security adapter name.                                                                                                                                                                        |
| <b>ServerName</b>          | The Fully Qualified Domain Name of the LDAP server.                                                                                                                                                           |
| <b>Port</b>                | The LDAP port number, typically 389.                                                                                                                                                                          |
| <b>BaseDN</b>              | The LDAP suffix beneath which the users are located.                                                                                                                                                          |
| <b>SharedCredentialsDN</b> | Represents an LDAP user that holds the default credentials for users when they do not possess specific credentials in their own user record (i.e. the one specified in the <b>CredentialsAttributeType</b> ). |

Table 3. SSO configuration parameters (continued)

| Parameter                                      | Use                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>UsernameAttributeType</b>                   | The LDAP attribute that stores the user's username.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>PasswordAttributeType</b>                   | The LDAP attribute that stores the user's password.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>CredentialsAttributeType</b>                | <p>Must contain at least one entry in the specified LDAP attribute. This LDAP attribute should contain a string of the form:</p> <p><code>username=user password=pwd</code></p> <p>where <i>user</i> and <i>pwd</i> correspond to the user name and password that users employ to authenticate to the Siebel database. Any LDAP string attribute can be chosen in this field or a new one can be created to avoid parameter overloading.</p> |
| <b>ApplicationUser and ApplicationPassword</b> | An LDAP DN and corresponding password that represent the identity that the Siebel applications use to bind to LDAP enabling the retrieval of the other data. The user should have read privileges to the user records beneath the specified <b>BaseDN</b> . No changes should be required for a default Tivoli Access Manager installation.                                                                                                  |

Restart your Siebel server for the configuration changes to take affect.

### Tivoli Access Manager Adapter Parameters

Depending on the platform where this integration is being deployed, copy the relevant Tivoli Access Manager security adapter library from the integration package to the *Siebel\_install\_dir/siebsrvr/bin/* directory (or *Siebel\_install\_dir\siebsrvr\lib\* on UNIX).

The parameters for the Tivoli Access Manager adapter are shown below with sample values:

```
[SecurityAdapters]
PD = PD

...

[PD]
DllName = PDSiebel.dll
AdminName = sec_master
AdminPassword = admin_pw
Domain = Default
DefaultCredentialUserID = username
ContextPoolSize = 3
RoleGroupPrefix = SiebelRole-
CredentialTypePrefix = SiebelCred-
StripRolePrefix = 0
SingleSignOn = TRUE
TrustToken = sso_shared_secret
Tracefile = path_to_tracefile
```

#### Notes:

1. The name of the adapter is platform specific, so replace *PDSiebel.dll* with the appropriate adapter name for the platform being used.
2. The *sso\_shared\_secret* is the same word as specified in the section "Configuring the Siebel Web Extension" on page 16.

Entries permitted in the service configuration file are shown in the following table:

| Configuration Item             | Description                                                                                                                                                                                                                                        | Mandatory | Default Value (if not mandatory) |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------|
| <b>DIName</b>                  | Tivoli Access Manager security adapter file name                                                                                                                                                                                                   | Y         | –                                |
| <b>AdminName</b>               | Tivoli Access Manager user name with administrative privileges.                                                                                                                                                                                    | Y         | –                                |
| <b>AdminPassword</b>           | Password for the Tivoli Access Manager user.                                                                                                                                                                                                       | Y         | –                                |
| <b>ContextPoolSize</b>         | Number of Tivoli Access Manager admin contexts created in the context pool. The context pool allows concurrent requests from the adapter without creating contexts (and SSL sessions) for short use.                                               | N         | 5                                |
| <b>RoleGroupPrefix</b>         | Prefix on Tivoli Access Manager group names that represent Siebel roles.                                                                                                                                                                           | N         | SiebelRole-                      |
| <b>StripRolePrefix</b>         | Flag to enable stripping of <b>RoleGroupPrefix</b> from the group name.                                                                                                                                                                            | N         | 0                                |
| <b>CredentialTypePrefix</b>    | Prefix on Tivoli Access Manager resource credentials that represent Siebel credentials.                                                                                                                                                            | N         | SiebelCred-                      |
| <b>DisableChangePassword</b>   | Flag to disable the change password propagation to Tivoli Access Manager.                                                                                                                                                                          | N         | 0                                |
| <b>DisableSetUserInfo</b>      | Flag to disable the propagation of account status or password changes to Tivoli Access Manager.                                                                                                                                                    | N         | 0                                |
| <b>DefaultCredentialUserid</b> | This parameter specifies a user name in the Tivoli Access Manager system to which default credentials are attached. If credentials cannot be found for a given user, this user name will be checked next in an attempt to find a valid credential. | N         | –                                |
| <b>TraceFile</b>               | The security adapter trace capability, for troubleshooting.                                                                                                                                                                                        | N         | –                                |
| <b>PDMgrRetryTimeout</b>       | Number of seconds to pause before retrying a connection to PDMgrd in the event that it is unavailable.                                                                                                                                             | N         | 5                                |
| <b>Domain</b>                  | The Tivoli Access Manager domain that contains the WebSEAL instance to be used.                                                                                                                                                                    | Y         | –                                |
| <b>Trust Token</b>             | A plaintext secret shared between the Siebel Web Extension and the Siebel server.                                                                                                                                                                  | Y         |                                  |

Restart your Siebel server for the configuration changes to take affect.

## Tivoli Access Manager Lite Adapter Parameters

Depending on the platform where this integration is being deployed, copy the relevant Tivoli Access Manager Lite security adapter library from the integration package to the *Siebel\_install\_dir/siebsrvr/bin/* directory (or *Siebel\_install\_dir\siebsrvr\lib\* on UNIX).

The mandatory parameters for the Tivoli Access Manager Lite Adapter are shown below with sample values:

```
[SecurityAdapters]
PDLite = PDLite
```

```
...
```

```
[PDLite]
DllName = PDSiebelLite.dll
ServerDataSrcUsername = Siebel_db_login_username
ServerDataSrcPassword = Siebel_db_login_password
GatewayDataSrcUsername = Siebel_admin_login_username
GatewayDataSrcPassword = Siebel_admin_login_password
Administrators = list_of_Siebel_administrators
SingleSignOn = TRUE
TrustToken = sso_shared_secret
TraceFile = path_to_tracefile
```

where *sso\_shared\_secret* is the same word as specified in the section Siebel Web Extension Configuration.

**Note:** The name of the adapter is platform specific, so replace *PDSiebelLite.dll* with the appropriate adapter name for the platform being used.

Entries permitted in the service configuration file are shown in the following table:

| Configuration Item            | Description                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DIIName</b>                | Tivoli Access Manager Lightweight security adapter file name.                                                                                  |
| <b>ServerDataSrcUsername</b>  | Username used to log onto the Siebel Database.                                                                                                 |
| <b>ServerDataSrcPassword</b>  | Password for the Siebel Database logon.                                                                                                        |
| <b>GatewayDataSrcUsername</b> | A Siebel Administrator username.                                                                                                               |
| <b>GatewayDataSrcPassword</b> | Password for the Siebel Administrator username.                                                                                                |
| <b>Administrators</b>         | A comma-separated list of Siebel Administrators. Do not place spaces between the entries. For example:<br>Administrators = admin,admin1,admin2 |
| <b>SingleSignOn</b>           | Set to <i>true</i> to enable Single Sign-on.                                                                                                   |
| <b>TraceFile</b>              | The security adapter trace capability, for troubleshooting.                                                                                    |
| <b>Trust Token</b>            | A plaintext secret shared between the Siebel Web Extension and the Siebel server.                                                              |

Restart your Siebel server for the configuration changes to take affect.

After performing the steps outlined above, proceed to “Configuring Siebel Applications in Siebel 7.5.”

## Configuring Siebel Applications in Siebel 7.5

The Siebel applications must now be configured to make use of the above changes to the configuration files.

Perform the following steps to configure the Siebel applications to use the above settings:

1. Start the Siebel client and login as **SADMIN**, the Siebel Administrator.
2. In the *Connect To* field, select **Server**.
3. From the *View* menu, choose **Site Map**.
4. Click **Server Administration**.
5. Click **Servers**.
6. Click **Server Components**.
7. Click the **Object Manager** for the application you wish to enable for single sign-on.
8. In the bottom frame, click **Component Parameters**.
9. In the bottom frame, click **Query**, and search for **Security\***.
10. Change the **Current<sup>®</sup> Value** field for **Security Adapter Name** to the appropriate value for your adapter:
  - *LDAP*,
  - *PD*, or
  - *PDLite*.

When the above changes are made, the Component Group must be restarted from the same interface. To do this:

1. From the combo box select **Show Servers**.

2. Select **Server Component Groups**.
3. Highlight the Component Group to be restarted, for example, **Siebel ISS**.
4. Click **Shutdown**.
5. Wait until the component group has been stopped. You may need to refresh the bottom frame by selecting **Query** and then **Go** with an empty query.
6. Click **Startup**.

After performing the steps outlined above, proceed to “Configuring Siebel Logout Behavior” on page 28.

## Security Adapter Configuration in Siebel 7.7, 7.8 and 8.0

Edit the configuration for each Siebel application object to enable single sign-on and to specify a shared secret that matches the one entered in the Siebel Web Extension configuration file.

The following sections describe the steps required for each of the given scenarios. Refer to the appropriate section.

### If you are implementing the LDAP Security Adapter

Proceed to “LDAP Security Adapter Steps:”

### If you are implementing the Tivoli Access Manager Security Adapter

Proceed to “Tivoli Access Manager Adapter Steps:” on page 24.

### If you are implementing the Tivoli Access Manager Lite Security Adapter

Proceed to “Tivoli Access Manager Lite Adapter Steps” on page 26.

### LDAP Security Adapter Steps:

Perform the following steps to configure the LDAP Security Adapter:

1. Start the Siebel client and login as **SADMIN**, the Siebel Administrator.
2. From the **Navigate** menu, select **Site Map**.
3. Click **Administration - Server Configuration**.
4. Click **Enterprises - Profile Configuration**.
5. In the middle frame, click **Query** and search for **LDAP Security Adapter**.
6. In the bottom frame, enter the correct parameters as described in the following table:

Table 4. SSO configuration parameters

| Parameter                                      | Use                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ServerName</b>                              | The Fully Qualified Domain Name of the LDAP server.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Port</b>                                    | The LDAP port number, typically 389.                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>BaseDN</b>                                  | The LDAP suffix beneath which the users are located.                                                                                                                                                                                                                                                                                                                                                                     |
| <b>SharedCredentialsDN</b>                     | Represents an LDAP user that holds the default credentials for users when they do not possess specific credentials in their own user record (i.e. the one specified in the <b>CredentialsAttributeType</b> ).                                                                                                                                                                                                            |
| <b>UsernameAttributeType</b>                   | The LDAP attribute that stores the user's username.                                                                                                                                                                                                                                                                                                                                                                      |
| <b>PasswordAttributeType</b>                   | The LDAP attribute that stores the user's password. Must be <b>userPassword</b> .                                                                                                                                                                                                                                                                                                                                        |
| <b>CredentialsAttributeType</b>                | Must contain at least one entry in the specified LDAP attribute. This LDAP attribute should contain a string of the form:<br><br>username=user password=pwd<br><br>where <i>user</i> and <i>pwd</i> correspond to the user name and password that users employ to authenticate to the Siebel database. Any LDAP string attribute can be chosen in this field or a new one can be created to avoid parameter overloading. |
| <b>ApplicationUser and ApplicationPassword</b> | An LDAP DN and corresponding password that represent the identity that the Siebel applications use to bind to LDAP enabling the retrieval of the other data. The user should have read privileges to the user records beneath the specified <b>BaseDN</b> . No changes should be required for a default Tivoli Access Manager installation.                                                                              |
| <b>SingleSignOn</b>                            | True.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>TrustToken</b>                              | The value specified for TrustToken in eapps.cfg ( <i>sso_shared_secret</i> ).                                                                                                                                                                                                                                                                                                                                            |

7. Restart your Siebel server for the changes to take effect.

After configuring the LDAP security adapter, proceed to "Configuring Siebel Applications in Siebel 7.7, 7.8 and 8.0" on page 27.

### Tivoli Access Manager Adapter Steps:

Perform the following steps to configure the Tivoli Access Manager Adapter:

1. Depending on the platform where this integration is being deployed, copy the relevant Tivoli Access Manager security adapter library from the integration package to the *Siebel\_install\_dir/siebsrvr/bin/* directory (or *Siebel\_install\_dir\siebsrvr\lib\* on UNIX).
2. Start the Siebel client and login as **SADMIN**, the Siebel Administrator.
3. From the **Navigate** menu, select **Site Map**.
4. Click **Administration - Server Configuration**.
5. Click **Enterprises - Profile Configuration**.
6. Click **New**.
7. Enter the following values:

Profile: TAM Security Adapter  
Alias: TAMSecAdpt  
Subsystem Type: InfraSecAdpt\_Custom  
Description: Tivoli Access Manager Security Adapter

8. Select **Menu** then **Save Record**.

9. In the bottom frame, enter the parameters as follows, default the remaining:

Security Adapter Dll Name: PDSiebel.dll  
Config File Name: *SIEBEL\_HOME*\siebsrvr\BIN\lang\PD.cfg  
Config Section Name: PD  
Single Sign On: True  
Trust Token: *sso\_shared\_secret*

10. Create a new configuration file at:

*SIEBEL\_HOME*\siebsrvr\BIN\lang\PD.cfg

11. Create a stanza in the PD.cfg file called **[PD]**.

12. In the new [PD] stanza, add startup parameters as shown in the following example. The parameters are explained in the table below:

```
[PD]
AdminName = sec_master
AdminPassword = admin_pw
Domain = Default
DefaultCredentialUserID = username
ContextPoolSize = 3
RoleGroupPrefix = SiebelRole-
CredentialTypePrefix = SiebelCred-
StripRolePrefix = 0
Tracefile = path_to_tracefile
```

Table 5. Security Adapter Configuration Parameters

| Configuration Item           | Description                                                                                                                                                                                          | Mandatory | Default Value (if not mandatory) |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------|
| <b>AdminName</b>             | Tivoli Access Manager user name with administrative privileges.                                                                                                                                      | Y         | –                                |
| <b>AdminPassword</b>         | Password for the Tivoli Access Manager user.                                                                                                                                                         | Y         | –                                |
| <b>ContextPoolSize</b>       | Number of Tivoli Access Manager admin contexts created in the context pool. The context pool allows concurrent requests from the adapter without creating contexts (and SSL sessions) for short use. | N         | 5                                |
| <b>RoleGroupPrefix</b>       | Prefix on Tivoli Access Manager group names that represent Siebel roles.                                                                                                                             | N         | SiebelRole-                      |
| <b>CredentialTypePrefix</b>  | Prefix on Tivoli Access Manager resource credentials that represent Siebel credentials.                                                                                                              | N         | SiebelCred-                      |
| <b>StripRolePrefix</b>       | Flag to enable stripping of <b>RoleGroupPrefix</b> from the group name.                                                                                                                              | N         | 0                                |
| <b>DisableChangePassword</b> | Flag to disable the change password propagation to Tivoli Access Manager.                                                                                                                            | N         | 0                                |

Table 5. Security Adapter Configuration Parameters (continued)

| Configuration Item             | Description                                                                                                                                                                                                                                        | Mandatory | Default Value (if not mandatory) |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------|
| <b>DisableSetUserInfo</b>      | Flag to disable the propagation of account status or password changes to Tivoli Access Manager.                                                                                                                                                    | N         | 0                                |
| <b>DefaultCredentialUserid</b> | This parameter specifies a user name in the Tivoli Access Manager system to which default credentials are attached. If credentials cannot be found for a given user, this user name will be checked next in an attempt to find a valid credential. | N         | –                                |
| <b>TraceFile</b>               | The security adapter trace capability, for troubleshooting.                                                                                                                                                                                        | N         | –                                |
| <b>PDMgrRetryTimeout</b>       | Number of seconds to pause before retrying a connection to PDMgrd in the event that it is unavailable.                                                                                                                                             | N         | 5                                |
| <b>Domain</b>                  | The Tivoli Access Manager domain that contains the WebSEAL instance to be used.                                                                                                                                                                    | Y         | –                                |

13. Restart your Siebel server for the changes to take effect.

After configuring the Tivoli Access Manager security adapter, proceed to “Configuring Siebel Applications in Siebel 7.7, 7.8 and 8.0” on page 27.

## Tivoli Access Manager Lite Adapter Steps

Perform the following steps to configure the Tivoli Access Manager Lite Adapter:

1. Copy the relevant Tivoli Access Manager Lite security adapter library from the integration package to the appropriate directory:

### Windows

*Siebel\_install\_dir/siebsrvr/bin/*

**UNIX** *Siebel\_install\_dir/siebsrvr/lib/*

2. Start the Siebel client and login as **SADMIN**, the Siebel Administrator.
3. From the **Navigate** menu, select **Site Map**.
4. Click **Administration - Server Configuration**.
5. Click **Enterprises - Profile Configuration**.
6. Click **New**.
7. Enter the following values:  
 Profile: TAM Lite Security Adapter  
 Alias: TAMLiteSecAdpt  
 Subsystem Type: InfraSecAdpt\_Custom  
 Description: Tivoli Access Manager Lite Security Adapter
8. Select **Menu** then **Save Record**.
9. In the bottom frame, enter the parameters as follows, default the remaining:  
 Security Adapter Dll Name: PDSiebelLite.dll  
 Config File Name: *SIEBEL\_HOME*\siebsrvr\BIN\lang\PD.cfg  
 Config Section Name: PDLite  
 Single Sign On: True  
 Trust Token: *sso\_shared\_secret*

10. Create a new configuration file at:  
`SIEBEL_HOME\siebsrvr\BIN\lang\PD.cfg`
11. Create a stanza in the PD.cfg file called **[PDLite]**.
12. In the new [PDLite] stanza, add startup parameters as shown in the following example. The parameters are explained in the table below:

```
[PDLite]
GatewayDataSrcUsername = Siebel_admin_login_username
GatewayDataSrcPassword = Siebel_admin_login_password
ServerDataSrcUsername = Siebel_db_login_username
ServerDataSrcPassword = Siebel_db_login_password
SiebelDBUsername = Siebel_db_login_username
SiebelDBPassword = Siebel_db_login_password
Administrators = list_of_Siebel_administrators
Tracefile = path_to_tracefile
```

Table 6. Security Adapter Configuration Parameters

| Configuration Item     | Description                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ServerDataSrcUsername  | Username used to log onto the Siebel Database.                                                                                                                                                                       |
| ServerDataSrcPassword  | Password for the Siebel Database logon.                                                                                                                                                                              |
| SiebelDBUsername       | Username used to log onto the Siebel Database                                                                                                                                                                        |
| SiebelDBPassword       | Password for the Siebel Database logon.                                                                                                                                                                              |
| GatewayDataSrcUsername | A Siebel Administrator username.                                                                                                                                                                                     |
| GatewayDataSrcPassword | Password for the Siebel Administrator username.                                                                                                                                                                      |
| Administrators         | A comma-separated list of Siebel Administrators. Do not place spaces between the entries. These users will have access to the Siebel administrative functions. For example:<br>Administrators = sadmin,admin1,admin2 |
| TraceFile              | Path to trace file. If written, the trace file will contain administrator usernames and passwords in clear text. This parameter can be omitted and no trace file will be written.                                    |

13. Restart your Siebel server for the changes to take effect.

After configuring the Tivoli Access Manager security adapter, proceed to “Configuring Siebel Applications in Siebel 7.7, 7.8 and 8.0.”

## Configuring Siebel Applications in Siebel 7.7, 7.8 and 8.0

The Siebel application must now be configured to make use of whichever Security Adapter is being used for the given scenario.

Perform the following steps to configure the Siebel applications:

1. Start the Siebel client and login as **SADMIN**, the Siebel Administrator.
2. From the **Navigate** menu, select **Site Map**.
3. Click **Administration - Server Configuration**.
4. Click **Servers - Components - Parameters**.
5. In the middle frame, select the application you wish to enable single sign-on (for example, **Call Center Object Manager**).

6. In the bottom frame, select **Parameters**.
7. In the bottom frame, click **Query** and search for **Security\***.
8. Change the value of **Security Adapter Mode** to:
  - *LDAP* for Scenario One,
  - *Custom* for Scenario Two or Three.
9. Change the value of **Security Adapter Name** to:
  - *LDAPSecAdpt* for Scenario One,
  - *TAMSecAdpt* for Scenario Two, or
  - *TAMLiteSecAdpt* for Scenario Three.

When the above changes are made, the Component Group must be restarted. Either restart the entire Siebel Server, or follow the steps below to restart only the modified application's component group:

1. From the **Navigate** menu, select **Site Map**.
2. Click **Administration - Server Management**.
3. Click **Servers - Component Groups**.
4. In the middle frame, select the appropriate **Component Group** (for example, **Siebel Call Center**).
5. In the bottom frame, select the appropriate **Component** (for example, **Call Center Object Manager**).
6. Click **Shutdown**.
7. Wait until the component has been stopped. You may need to refresh the bottom frame by selecting **Query** and then **Go** with an empty query.
8. Click **Startup**.

After completing the above steps, proceed to "Configuring Siebel Logout Behavior."

## Configuring Siebel Logout Behavior

**Note:** The steps described in this section require Siebel Tools. Refer to the Siebel documentation for details of Siebel Tools installation.

Each Siebel application configured for SSO through Tivoli Access Manager needs to have its default logout behavior modified so that users are logged out of Tivoli Access Manager when they select **Log off** from a Siebel application.

Do this as follows:

1. Copy the `TAMLogout.swt` file to the `Siebel_install_dir\siebsrvr\WEBTEMPL` directory.

**Note:** The `TAMLogout.swt` file redirects to `/pkmslogout`, which only logs out Tivoli Access Managers when using Forms Authentication. Where Basic Authentication is being used, users should be redirected to a suitable alternate location.

2. Stop the Siebel server process.
3. Start Siebel Tools.
4. Create a new project as follows:
  - a. In the Object Explorer window, click on **Project**.
  - b. Create a new record by selecting **Edit** then **New Record**.

- c. Enter TAM Logout as the new record's name, and select **Locked**.
5. Create a Web template as follows:
  - a. In the **Object Explorer** window, click on **Web Template**.
  - b. Add a new record named TAM Logout.
  - c. Enter TAM Logout for the **Project** parameter.
  - d. Specify **Web Page Template** for the **Type** parameter.
6. Create a Web Template File as follows:
  - a. Expand the **Web Template** tree and click on **Web Template File**.
  - b. Add a new record named TAM Logout.
  - c. Enter TAMLogout.swt for the **Filename** parameter.
7. Create a Web Page as follows:
  - a. In the **Object Explorer** window, click on **Web Page**.
  - b. Add a new record named TAM Logout.
  - c. Enter TAM Logout for the **Project** parameter.
  - d. Select TAM Logout for the **Web Template** parameter.
8. Lock the application project for each project requiring the logout page to be changed, as follows:
  - a. In the Object Explorer window, click on **Project**.
  - b. Locate the appropriate project and select **Locked** (for example, **Siebel Universal Agent** for Call Center, **eSales** for eSales).
9. In the **Application** window, select the Siebel module to be configured (each module must be configured separately).
10. Scroll to the right and locate the **Logoff Acknowledgement Web Page** parameter. Make a note of this value before changing it. Select **TAM Logout** (the Web page created in step 6).
11. Repeat steps 9 and 10 above for all Siebel modules that need to be configured.
12. Compile the changes as follows:
  - a. Select **Tools** then **Compile Projects**.
  - b. Select **Locked Projects**.
  - c. Enter the name of the Siebel repository file (for example, *Siebel\_install\_dir\siebsrvr\OBJECTS\lang\siebel.srf*).
  - d. Click **Compile**.
13. Unlock all locked projects.
14. Exit Siebel Tools.
15. Restart the Siebel Server and the Web server.

**Note:** If the Siebel server is installed on a UNIX platform, and the Siebel Tools client is installed on a Windows machine, the newly compiled .srf file will need to be copied to the UNIX machine.

After configuring the Siebel Logout behaviour, proceed to "Checking the Integration" on page 30.

---

## Checking the Integration

This section describes the steps required to test the integration. The integration package also includes two test programs which can be used to test the integration when using the Tivoli Access Manager Adapter. For details of these programs, see “Test Programs” on page 31.

To test the integration:

1. Open a browser and access a Siebel application through WebSEAL and the junction that was created:

**Standard junction:**

`http[s]://webseal_fqdn/junction_point/siebel_app`

**Transparent path junction:**

`http[s]://webseal_fqdn/siebel_app`

**Virtual host junction:**

`http[s]://siebel_fqdn:port/siebel_app`

where:

- where *webseal\_fqdn* is the fully qualified domain name of the WebSEAL server,
  - *junction\_point* is the junction created in the WebSEAL configuration step above,
  - *siebel\_app* is the Siebel application that was junctioned to (for example) *callcenter\_enu*.
2. WebSEAL displays an authentication challenge. Log in using the Tivoli Access Manager username and password. Remember that this username must also have a corresponding account in the Siebel user table.
  3. Upon successful authentication, the Siebel application will be displayed. Some Siebel applications will display a logout option in the top right hand corner, verifying that SSO has been achieved.

---

## Test Programs

This section describes the two test programs that are supplied with the integration package. They can be used to test the correct setup and connectivity between the Siebel Application Server and the Tivoli Access Manager policy server.

### pdadmin\_pool\_test

The **pdadmin\_pool\_test** program tests the Tivoli Access Manager administration context pool. It creates multiple threads to retrieve and use contexts. Use the trace output to verify that a context is not used on any two threads at the same time. The program also verifies connectivity to the Tivoli Access Manager management server.

Usage:

```
C:\> pdadmin_pool_test size admin pw domain thread_count loop_count
```

where:

|                     |                                                                              |
|---------------------|------------------------------------------------------------------------------|
| <i>size</i>         | The number of Tivoli Access Manager admin contexts to be created and pooled. |
| <i>admin</i>        | The Tivoli Access Manager administrator name.                                |
| <i>pw</i>           | Password for the Tivoli Access Manager administrator.                        |
| <i>domain</i>       | Enter <i>Default</i> for the default domain, or specify a domain.            |
| <i>thread_count</i> | Number of worker threads to create in the test program.                      |
| <i>loop_count</i>   | Number of task iterations per worker thread.                                 |

For example:

```
C:\> pdadmin_pool_test 5 sec_master password Default 5 10
```

### PDSiebelTest

The **PDSiebelTest** program tests all the interfaces in the security adapter. Configuration parameters normally found in the service configuration file are embedded in the program.

The program operates (destructively) on a GSO user called **pdsiebel\_testuser** and looks for Tivoli Access Manager groups prefixed with **PDSiebelTestRole-**. GSO resource names prefixed with **PDSiebelTestCred-** are also used.

Prior to executing the test program, the related GSO user, group and GSO credentials need to be created. To simplify the configuration, two scripts are provided, **pd\_siebel\_test\_setup.pdadmin** and **pd\_siebel\_test\_cleanup.pdadmin**. These can be used to set up and clean the test environment.

Usage:

```
# pdadmin -a sec_master -p password < pd_siebel_test_setup.pdadmin
```

and:

```
# pdadmin -a sec_master -p password < pd_siebel_test_cleanup.pdadmin
```

You must modify the LDAP suffix used in the file to match the one in your LDAP registry (the sample files below show the LDAP suffix highlighted in bold font).

To execute the test program, a Tivoli Access Manager administrator user name and password are specified on the command line when running the program.

Usage:

```
C:\> PDSiebelTest admin pw domain
```

To specify the default domain enter:

```
C:\> PDSiebelTest sec_master password Default
```

Otherwise enter the appropriate domain name.

## **pd\_siebel\_test\_setup.pdadmin**

```
user create -gsouser pdsiebel_testuser cn=pdsiebel_testuser,o=ibm,c=au
pdsiebel_testuser pdsiebel_testuser passw0rd

user modify pdsiebel_testuser account-valid yes

group create SiebelTestRole-Employee cn=SiebelTestRole-Employee,o=ibm,c=au
SiebelTestRole-Employee

group modify SiebelTestRole-Employee add pdsiebel_testuser

group create SiebelTestRole-Manager cn=SiebelTestRole-Manager,
o=ibm,c=au SiebelTestRole-Manager

group modify SiebelTestRole-Manager add pdsiebel_testuser

rsrsrc create SiebelTestCred-Server

rsrsrc create SiebelTestCred-Database

rsrccred create SiebelTestCred-Server rsrscuser testuser rsrcpwd password1
rsrctype web user pdsiebel_testuser

rsrccred create SiebelTestCred-Database rsrscuser TESTUSER rsrcpwd SECRET
rsrctype web user pdsiebel_testuser
```

## **pd\_siebel\_test\_cleanup.pdadmin**

```
user delete -registry pdsiebel_testuser
group delete -registry SiebelTestRole-Employee
group delete -registry SiebelTestRole-Manager
rsrsrc delete SiebelTestCred-Server
rsrsrc delete SiebelTestCred-Database
```

---

## Uninstallation

The uninstallation process is basically a reverse of the steps taken to configure Siebel and Tivoli Access Manager for SSO. To remove this integration, perform the steps described in the following sections.

### Restore Siebel Applications Settings in Siebel 7.5

1. Start the Siebel client and login as SADMIN. This is the Siebel database username and password.
2. In the **Connect To** field select **Server**.
3. From the **View** menu, choose **Site Map**.
4. Click **Server Administration**.
5. Click **Servers**.
6. Click **Server Components**.
7. Click the **Object Manager** for the application you wish to enable for single sign-on.
8. In the bottom frame, click **Component Parameters**.
9. In the bottom frame, click **Query**, and search for **Security\***.
10. Clear the entry in the **Current Value** field to make it blank.

### Restart the Component Group in Siebel 7.5

From the same interface:

1. From the combo box select **Show Servers**.
2. Select **Server Component Groups**.
3. Highlight the Component Group to be restarted, for example, **Siebel ISS**.
4. Click **Shutdown**.
5. Wait until the component group has been stopped. You may need to refresh the bottom frame by selecting **Query** and then **Go** with an empty query.
6. Click **Startup**.

### Restore Siebel Applications Settings in Siebel 7.7, 7.8 and 8.0

1. Start the Siebel client and login as SADMIN, the Siebel administrator.
2. From the **Navigate** menu, select **Site Map**.
3. Click **Administration** then **Server Configuration**.
4. Click **Servers** then **Components** then **Parameters**.
5. In the middle frame, select the application for which you wish to enable single sign-on (for example, **Call Center Object Manager**).
6. In the bottom frame, select **Parameters**.
7. In the bottom frame, click **Query** and search for **Security\***.
8. Change the value of **Security Adapter Mode** to *DB*.
9. Change the value of **Security Adapter Name** to *DBSecAdpt*.

### Restart the Component Group in Siebel 7.7, 7.8 and 8.0

From the same interface:

1. From the **Navigate** menu, select **Site Map**.
2. Click **Administration** then **Server Management**.
3. Click **Servers** then **Component Groups**.
4. In the middle frame, select the appropriate **Component Group** (for example, **Siebel Call Center**).

5. In the bottom frame, select the appropriate **Component** (for example, **Call Center Object Manager**).
6. Click **Shutdown**.
7. Wait until the component group has been stopped. You may need to refresh the bottom frame by selecting **Query** and then **Go** with an empty query.
8. Click **Startup**.

#### **Remove Security Adapter Configuration (Tivoli Access Manager and Tivoli Access Manager Lite Adapters only)**

When configuring the Siebel Applications to make use of the security adapter, two sections were added into the configuration file for each application. These stanzas can safely remain, as references to them were removed in the previous step. Leaving them in place makes restoring the integration easier. However if you prefer to remove them, then open each application's configuration file and comment out with a semicolon (;) or delete the following lines (in this example the entries have been commented out):

```
[SecurityAdapters]
;PD = PD

;[PD]
;DllName = PDSiebel.dll
;AdminName = sec_master
;AdminPassword = admin_pw
;Domain = Default
;ContextPoolSize = 3
;RoleGroupPrefix = SiebelRole-
;CredentialTypePrefix = SiebelCred-
;SingleSignOn = TRUE
;TrustToken = sso_shared_secret
```

#### **Restore Siebel Web Extension configuration**

Return the Siebel environment to its default state:

1. Open the `eapps.cfg` file in a text editor, and remove or comment out with a semicolon (;) the configuration data that was added previously in the step "Configuring the Siebel Web Extension" on page 16. For example, remove or comment out the following parameters:

```
[defaults]
...
;AnonUserName = GUESTCST
;AnonPassword = secret
;TrustToken = sso_shared_secret

[/callcenter_enu]
...
;SingleSignOn = TRUE
;UserSpec = IV-USER
;UserSpecSource = Header
;ProtectedVirtualDirectory = /callcenter_enu

[/esales_enu]
...
;SingleSignOn = TRUE
;UserSpec = IV-USER
;UserSpecSource = Header
;ProtectedVirtualDirectory = /esales_enu
```

2. Restart the Siebel Gateway and Siebel Server for the changes to take effect.

The Siebel environment can now be accessed directly without going through WebSEAL.

### Restore Siebel Default Logout Behavior

1. Stop the Siebel Server.
2. Start Siebel Tools.
3. In the **Object Explorer** window, select the application to restore (each application must be restored individually).
4. Scroll to the right and find the **Logoff Acknowledgement Web Page** parameter. Restore the default value that you noted earlier when changing the default behavior.
5. Exit Siebel Tools.
6. Restart the Siebel server and the Web server.

### Restore WebSEAL settings

1. Open the *WebSEAL\_install\_dir/etc/webseald-instance.conf* file and locate the **[script-filtering]** stanza.
2. Set the value for `script-filter` and `rewrite-absolute-with-absolute` to *no*:  

```
script-filter = no
rewrite-absolute-with-absolute = no
```
3. Modify the *WebSEAL\_install\_dir/www-instance/lib/jmt.conf* file and remove the mapping table entries for any applications created during the integration.
4. Delete the WebSEAL junction. Refer to the *Tivoli Access Manager WebSEAL Administration Guide* for details. An example command would be:  

```
pdadmin> server task webseald-server_name delete /junction_name
```

where:

  - *server\_name* is the WebSEAL server name, which must be displayed in the exact format as displayed in the output of the `pdadmin server list` command, and
  - *junction\_name* is the name chosen for the junction point.
5. Remove changes to the WebSEAL login page.
6. Restart WebSEAL for the changes to take effect.

### Restore Tivoli Access Manager Settings (For Tivoli Access Manager Adapter

**only)** To restore the Tivoli Access Manager environment to its default state, any users, groups and resources that were created must be removed. To remove the items that were created in this integration guide, for example, issue the following **pdadmin** commands:

1. To remove the user:  

```
pdadmin> user delete -registry testuser
```
2. To remove the group:  

```
pdadmin> group delete -registry SiebelRole-Employee
```
3. To remove the resource created:  

```
pdadmin> rsrc delete SiebelCred-ServerDataSrc
```



---

## Chapter 3. Additional Notes

This chapter contains the following sections:

- “Actuate Reports for Siebel”
- “Siebel Computer Telephony Integration (CTI)” on page 38
- “Siebel Analytics 7.8.2” on page 39
- “Troubleshooting” on page 40
- “Known Issues” on page 42

---

### Actuate Reports for Siebel

Actuate Reports is Siebel’s default reporting mechanism. If Actuate Reports is to be used with this integration, the following configuration steps must be completed for it to function correctly through WebSEAL.

#### WebSEAL Junction Creation to the Actuate Server

A WebSEAL junction must be created to the Actuate Reports server. The following examples use the default Actuate port of 8700 to create the junction.

##### Virtual Host Junction:

```
pdadmin> server task instance-webseald-server_name virtualhost create  
-t tcp -h actuate_server_name -p 8700 actuate_vh_name
```

##### Transparent Path Junction:

**Note:** The junction name must be /acweb if using a transparent path junction.

```
pdadmin> server task instance-webseald-server_name create -t tcp  
-h actuate_server_name -p 8700 -x /acweb
```

##### Standard Junction:

```
pdadmin> server task instance-webseald-server_name create -t tcp  
-h actuate_server_name -p 8700 /actuate_junction_name
```

Refer to the *IBM Tivoli Access Manager WebSEAL Administration Guide* for detailed information on creating WebSEAL junctions.

For Siebel 7.5, proceed to “Configuring Actuate Reports for Siebel 7.5.”

For Siebel 8.0, proceed to “Configuring Actuate Reports for Siebel 8.0” on page 38.

### Configuring Actuate Reports for Siebel 7.5

In order for Actuate Reports to work for Siebel 7.5, follow these steps:

1. Log into the Siebel Client as Administrator.
2. Click the **Site Map** icon.
3. Select **Server Administration**.
4. Select **Components**.
5. Select the required **Object Manager**.
6. Select **Component Parameters**.
7. Locate the entry for **Actuate Server Report Cast Host**.

8. Change the entry for **Current value** to the following:

**Virtual Host Junction**

Siebel fully qualified domain name and port:

*siebel\_fqdn:8700*

**Transparent Path Junction**

WebSEAL fully qualified domain name:

*webseal\_fqdn*

**Standard Junction**

WebSEAL fully qualified domain name and junction name:

*webseal\_fqdn/actuate\_junction\_name*

9. Press **Control-S** to save the record.
10. Restart the component for changes to take effect.

## Configuring Actuate Reports for Siebel 8.0

In order for Actuate Reports to work for Siebel 8.0, follow these steps:

1. Start the Siebel client and login as SADMIN, the Siebel administrator.
2. From the **Navigate** menu, select **Site Map**.
3. Click **Administration** then **Server Configuration**.
4. Click **Servers** then **Components** then **Parameters**.
5. In the middle frame, select the application for which you wish to enable single sign-on (for example, **Call Center Object Manager**).
6. In the bottom frame, select **Parameters**.
7. In the bottom frame, locate the entry for **Actuate Server Report Cast Host**
8. Change the entry for **Current value** to the following:

**Virtual Host Junction**

Siebel fully qualified domain name and port:

*siebel\_fqdn:8700*

**Transparent Path Junction**

WebSEAL fully qualified domain name:

*webseal\_fqdn*

**Standard Junction**

WebSEAL fully qualified domain name and junction name:

*webseal\_fqdn/actuate\_junction\_name*

9. Press **Control-S** to save the record.
10. Restart the component for changes to take effect.

---

## Siebel Computer Telephony Integration (CTI)

Siebel CTI applications include a communication toolbar, a Java Applet, that is placed at the top of the page.

### WebSEAL Filtering for CTI

In order for Siebel CTI to work through WebSEAL:

1. Locate the WebSEAL configuration file, *webseald.conf* in the directory *WebSEAL\_install\_dir\etc\*.
2. Within the `[filter-url]` stanza, add the following two filters alphabetically to the existing list:

```
COMMAND = URL
...
PARAM = VALUE
```

3. Restart WebSEAL for the above changes to take effect.

---

## Siebel Analytics 7.8.2

Siebel Analytics is a standalone analytical and reporting application that analyses and reports on data within the Siebel transactional database. Siebel provides a mechanism by which Analytics can be integrated into the Siebel application interface.

This integration configures SSO to Analytics via the Siebel application interface (for example, /callcenter\_enu). It does not cover access to the standalone Siebel Analytics Web application.

If using Transparent path junctions, create a junction to Analytics as follows (entered as one line):

```
pdadmin> server task instance-webseald-server_name create -t tcp -h
siebel_fqdn -c iv_user -x /Analytics
```

**Note:** The junction name must be **/Analytics**

When using Virtual host junctions or standard junctions, no specific Analytics junction is required.

In order to configure SSO between the Siebel applications and Analytics, perform the following steps:

1. Open the instanceconfig.xml file, which is located at:  
c:\siebelanalyticsdata\web\config\instanceconfig.xml
2. Add the following to the file between the <ServerInstance> and </ServerInstance> stanza tags:

```
<Auth>
<Impersonator>Admin</Impersonator>
<ImpersonatorPassword> Admin encrypted password</ImpersonatorPassword>
<SSOEnabled>y</SSOEnabled>
<SSOClientHeader>iv-user</SSOClientHeader>
</Auth>
```

Note the following:

- The <Impersonator> parameter is the user ID, which must be an administrator user and must be defined in PRD.
- <ImpersonatorPassword> is the encrypted password of the Impersonator user. To obtain this password, log in to Analytics Web as an administrator and fetch the following URL:  
`http://server/analytics/saw.dll?encryptString&string=secret`  
where *secret* is the password for Impersonator.
- <SSOEnabled> enables SSO, set the value to *y*.
- <SSOClientHeader> controls what is the header name needs to be retrieved. Set this value to *iv-user*.

3. Restart the Siebel Analytics Web Service.
4. Configure Symbolic URLs from inside Siebel CRM to not include user/password in request. To do this:

- a. Launch the Siebel operational application (for example, `callcenter_enu`) and navigate to **Site Map** then **Integration Administration** then **Symbolic URL Administration**.
- b. In the **Symbolic URL** section at the top, press **Query** then enter `*NQHOST*` in the URL column.
- c. Select all the Symbolic URLs for the Analytics application to be accessed through SSO. For example, to access the Service Analytics tab through SSO, highlight each Service Dashboard:  
`ServiceDashboard1,`  
`ServiceDashboard2,`  
`etc...`

For more information on what Symbolic URLs to change for your environment, refer to Siebel documentation.

- d. In the **Symbolic URL Arguments** section at the bottom of the page, de-select both the **Required Argument** and **Append as Argument** columns for both the **nqUser** and **nqPassword** rows
5. Restart the Component for the changes to be applied. For example, to apply changes to the Callcenter component:
  - a. Start the Siebel client and login as SADMIN.
  - b. From the **View** menu, choose **Site Map**.
  - c. Click **Server Administration**.
  - d. Click **Servers**.
  - e. Click **Server Components**.
  - f. Highlight the Component Group to be restarted. For example, **Call Center Object Manager (ENU)**.
  - g. Click **Shutdown**.
  - h. Wait until the component group has been stopped. You may need to refresh the bottom frame by selecting **Query** and then **Go** with an empty query.
  - i. Click **Startup**.

---

## Troubleshooting

The following cases provide solutions to common problems that may be encountered with this integration.

### Unable to create the WebSEAL junction:

Use the ping utility to determine that the WebSEAL server can contact the Siebel Web Extension Server.

### Creating the WebSEAL junction using the -j junction option:

Do not specify the -j junction option when creating the WebSEAL junction for this integration. In Siebel 7.0.4 and 7.5.2, an error message is displayed indicating *"Invalid encoding of property set..."*, and containing the `IV_JCT` Javascript in the first section of the error message. No message is displayed in Siebel 7.5.3 but various symptoms occur, including an *"Error connecting to server"* message that is briefly displayed by the menu frame.

### Creating Junction using Siebel FQDN

If `enableFQDN` is set to `TRUE` in the Siebel server configuration, ensure that the Siebel FQDN is used with the -h parameter when creating the WebSEAL junction.

### Page not found is returned:

- Ensure the fully qualified domain name is being used to access the WebSEAL server.
- Ensure that the WebSEAL junction is contained in the URL to the Siebel Application.
- When restarting the Web servers, ensure that the CPU load is minimal before proceeding to request a page.

**WebSEAL authenticates successfully, but unable to access Siebel Applications:**

- Ensure the application you are attempting to access has had its configuration file altered to contain the security adapter stanza detailed in this integration, and that it is configured to use the security adapter. The relevant security stanzas are:
  - [LDAP] for Scenario One,
  - [PD] for Scenario Two,
  - [PDLite] for Scenario Three.
- For Scenarios Two and Three, ensure that the security adapter has been copied to the *Siebel\_install\_dir/siebsrvr/bin/* directory.
- Check that the user exists in both the Tivoli Access Manager domain and in Siebel.

**Access to Siebel Reports (Actuate) requires a second login to WebSEAL:**

This is caused by users accessing the WebSEAL server using a hostname only, rather than using a fully qualified domain name (FQDN). The Actuate Reports configuration requires the FQDN of the WebSEAL server to be specified. When using the WebSEAL hostname only, the WebSEAL session cookie is not sent from the browser to WebSEAL, resulting in a login request.

The workaround to this problem is to only access WebSEAL using the FQDN.

**A second login is required when using BA authentication to WebSEAL over HTTPS with a TCP junction to Siebel:**

Ensure the `default.htm` file is modified to have the **SWEHo** parameter set to the `-h` (or `-v`) parameter of the Siebel Web Extension server. The second login is caused when a HTTP link to WebSEAL is being generated by the Siebel server and the user is not authenticated for HTTP access to WebSEAL.

**A blank page is returned after authenticating to WebSEAL when using forms authentication, or BA using HTTPS only:**

Ensure the `default.htm` file is modified to have the **SWEHo** parameter set to the `-h` (or `-v`) parameter of the Siebel Web Extension server. The blank page is caused when a HTTP link to WebSEAL is being generated by the Siebel server and the user is not authenticated for HTTP access to WebSEAL.

The following information may further assist in troubleshooting problems:

- The Siebel Web Extension log file is located in: *Siebel\_install\_directory/SWEApp/log*
- Turning on the LDAP server's trace capabilities may help to diagnose any problems. For the IBM Tivoli Directory Server, this is achieved using the web-based management tool.
- Turning on the trace capability of WebSEAL can also help determine problems. Refer to the *Tivoli Access Manager Problem Determination Guide* for details of how to set the trace capability for WebSEAL.

Since the Siebel processes on Windows 2000 run as services, they may not be able to access the Tivoli Access Manager runtime's certificate store and stash file when configured to use SSL. By default, these files are kept in the directory:

C:\Program Files\Tivoli\Policy Director\keytab\

Within this directory, files named pd.kdb and pd.sth should both be readable by the Windows user that runs the Siebel services. By default this is the SADMIN user. If necessary, make these file access modifications in Windows Explorer.

---

## Known Issues

The following issues exist for all three integration scenarios:

1. When a user logs into a Siebel Application through WebSEAL, and the timeout for the WebSEAL session is reached, WebSEAL re-authenticates the user by sending a login page to the browser. For those Siebel applications running in High-Interactivity mode, the Siebel client running on the user's browser is expecting Siebel RPC (Remote Procedure Call) requests from the Siebel Web Extension. Errors are displayed to the browser when it receives the WebSEAL login page. A number of workarounds exist for this problem:
  - Disable WebSEAL Inactivity Timeout in the webseald.conf file and set the WebSEAL session timeout to a large value.
  - If disabling inactivity timeout is an issue for other backend servers being protected by the same WebSEAL instance, create another WebSEAL instance and move the Siebel junctions to the new instance. This will allow the inactivity timeout to be disabled for the Siebel application only.
  - Disable the session timeout by setting WebSEAL to authenticate users using Basic Authentication (BA) rather than forms-based authentication.
  - If an inactivity timeout is required, then the Siebel applications can be set to use Standard Interactivity mode. Setting the Siebel applications to use this mode displays the applications in HTML only (no ActiveX controls are used). To set this for each application, open the associated configuration file (for example uagent.cfg) and set the following option:

HighInteractivity = FALSE

After making the changes, restart the relevant Siebel components.

Refer to the Siebel Support Web site for more information regarding this known issue.

2. When using SSL junctions to the Siebel Web Extension, some browsers will display the following warnings:

*This page contains both Secure and Non Secure items.  
Do you want to download non secure items?*

This known issue is documented in the *Security Guide for Siebel eBusiness Applications* from the *Siebel Bookshelf*. Despite this warning, Siebel Application requests will be processed over HTTPS and not HTTP.

3. If you are using IBM GSKit 7, use of the latest version (7.0.3.15 or above) is strongly recommended. If you are using an earlier version of IBM GSKit 7, rename the following directory from:

/opt/ibm/gsk7/icc/openssl/libcrypto.sl.0.9.7

to:

/opt/ibm/gsk7/icc/openssl/libcrypto.sl.0.9.7\_org

4. For Siebel 7.7, 7.8 and 8.0, after modifying the **GotoUrl** JavaScript function (as specified in “Configuring the Siebel Web Extension” on page 16) the Siebel Calendar functionality no longer works. To resolve this issue, do not modify the **GotoUrl** JavaScript function. Note that you will not be able to provide protocol switching; if the browser accesses WebSEAL using HTTPS, then an SSL junction to Siebel is required.



---

## Appendix A. IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus<sup>®</sup>, and Rational<sup>®</sup> products, as well as DB2<sup>®</sup> and WebSphere<sup>®</sup> products that run on Windows or UNIX operating systems), enroll in Passport Advantage<sup>®</sup> in one of the following ways:
  - **Online:** Go to the following Passport Advantage Web page and click **How to Enroll**:  
[http://www.lotus.com/services/passport.nsf/WebDocs/Passport\\_Advantage\\_Home](http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home)
  - **By phone:** For the phone number to call in your country, go to the IBM Software Support Web site (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region.
- For IBM eServer<sup>™</sup> software products (including, but not limited to, DB2 and WebSphere products that run in zSeries<sup>®</sup>, pSeries<sup>®</sup>, and iSeries<sup>®</sup> environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (<http://www.ibm.com/servers/eserver/techsupport.html>).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. "Determine the business impact of your problem"
2. "Describe your problem and gather background information" on page 46
3. "Submit your problem to IBM Software Support" on page 46

---

### Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

|                   |                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Severity 1</b> | <b>Critical</b> business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution. |
| <b>Severity 2</b> | <b>Significant</b> business impact: The program is usable but is severely limited.                                                                               |

|                   |                                                                                                                                                    |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Severity 3</b> | <b>Some</b> business impact: The program is usable with less significant features (not critical to operations) unavailable.                        |
| <b>Severity 4</b> | <b>Minimal</b> business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented. |

---

## Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be recreated? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

---

## Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online:** Go to the "Submit and track problems" page on the IBM Software Support site (<http://www.ibm.com/software/support/probsub.html>). Enter your information into the appropriate problem submission tool.
- **By phone:** For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see "Searching knowledge bases" and "Obtaining fixes" on page 47.

---

## Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

## Search the information center on your local system or network

IBM provides extensive documentation that can be installed on your local machine or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

## Search the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Support on the Web**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks®
- IBM DeveloperWorks
- Forums and newsgroups
- Google

---

## Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

1. Go to the IBM Software Support Web site (<http://www.ibm.com/software/support>).
2. Under **Products A - Z**, select your product name. This opens a product-specific support site.
3. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
4. Click the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the *Software Support Handbook* (<http://techsupport.services.ibm.com/guides/handbook.html>).



---

## Appendix B. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation  
2Z4A/101  
11400 Burnet Road  
Austin, TX 78758  
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

**COPYRIGHT LICENSE:** This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any

form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

---

## Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX  
DB2  
IBM  
IBM(logo)  
SecureWay  
Tivoli  
Tivoli (logo)  
Universal Database  
WebSphere

Microsoft<sup>®</sup>, Windows, Windows NT<sup>®</sup>, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.







Printed in USA