



**SECURITY GUIDE FOR SIEBEL
eBUSINESS APPLICATIONS**

MIDMARKET EDITION

VERSION 7.5

12-BD4FLF

SEPTEMBER 2002

Siebel Systems, Inc., 2207 Bridgepointe Parkway, San Mateo, CA 94404
Copyright © 2002 Siebel Systems, Inc.
All rights reserved.
Printed in the United States of America

No part of this publication may be stored in a retrieval system, transmitted, or reproduced in any way, including but not limited to photocopy, photographic, magnetic, or other record, without the prior agreement and written permission of Siebel Systems, Inc.

The full text search capabilities of Siebel eBusiness Applications include technology used under license from Hummingbird Ltd. and are the copyright of Hummingbird Ltd. and/or its licensors.

Siebel, the Siebel logo, TrickleSync, TSQ, Universal Agent, and other Siebel product names referenced herein are trademarks of Siebel Systems, Inc., and may be registered in certain jurisdictions.

Other product names, designations, logos, and symbols may be trademarks or registered trademarks of their respective owners.

U.S. GOVERNMENT RESTRICTED RIGHTS. Programs, Ancillary Programs and Documentation, delivered subject to the Department of Defense Federal Acquisition Regulation Supplement, are “commercial computer software” as set forth in DFARS 227.7202, Commercial Computer Software and Commercial Computer Software Documentation, and as such, any use, duplication and disclosure of the Programs, Ancillary Programs and Documentation shall be subject to the restrictions contained in the applicable Siebel license agreement. All other use, duplication and disclosure of the Programs, Ancillary Programs and Documentation by the U.S. Government shall be subject to the applicable Siebel license agreement and the restrictions contained in subsection (c) of FAR 52.227-19, Commercial Computer Software - Restricted Rights (June 1987), or FAR 52.227-14, Rights in Data—General, including Alternate III (June 1987), as applicable. Contractor/licensor is Siebel Systems, Inc., 2207 Bridgepointe Parkway, San Mateo, CA 94404.

Proprietary Information

Siebel Systems, Inc. considers information included in this documentation and in Siebel eBusiness Applications Online Help to be Confidential Information. Your access to and use of this Confidential Information are subject to the terms and conditions of: (1) the applicable Siebel Systems software license agreement, which has been executed and with which you agree to comply; and (2) the proprietary and restricted rights notices included in this documentation.

Contents

Introduction

How This Guide Is Organized	12
Revision History	12

Chapter 1. Security Resources

Managing Security in Corporate Networks	13
Using Industry Standards	15
Siebel Security Architecture	16
User Authentication for Secure System Access	16
End-to-End Encryption for Data Confidentiality	19
Authorization to Control Data Visibility	21
Auditing for Data Continuity	22
Secure Physical Deployment to Prevent Intrusion	23
Security for Mobile Solutions	24

Chapter 2. Configuring for Security - An Overview

Security Roadmap	25
Changing Default Passwords	27
Changing the SADMIN Password on Windows	28
Changing the Table Owner (DBO) Password	30
Changing the Siebel Local (DBA) Password	33

Chapter 3. Physical Deployment and Auditing

Firewall Support 37
 Recommended Placement 37
Resonate Support 39
Port Numbers 40
Restricting Access 42
 Physical Security of the Client Device 42
 Database Server Access 42
 File System Access 42
Auditing for Data Continuity 43

Chapter 4. Communications and Data Encryption

Types of Encryption 46
Configuring for Encryption 49
 Configuring Siebel Server for Encryption 49
 Configuring Web Clients for Encryption 50
Key Exchange in Siebel Applications 52
 Session Cookies 52
Password Encryption 53
Business Component Encryption 54
 Setting Encryption User Properties 54
RC2 Encryption Administration 56
 Using Key Database Manager 57
 If You are Upgrading 61
Unicode Support 61

Chapter 5. User Authentication

About User Authentication	65
Siebel Authentication Manager	67
Authentication Manager Overview	68
Authentication Manager Process Detail	68
Database Authentication Overview	70
Implementing Database Authentication	72

Chapter 6. Security Adapter Authentication

Siebel Security Adapters	73
Directory Requirements	75
ADSI Adapter Requirements	78
Siebel Security Adapters and the Siebel Dedicated Web Client	79
Security Adapter Deployment Options	80
LDAP and ADSI Security Adapter Authentication	81
Implementing LDAP and ADSI Security Adapter Authentication	83
Task Overview	83
Siebel Security Adapter Authentication and the Siebel Dedicated Web Client	84
Deployment Options for Siebel LDAP and ADSI Security Adapter Authentication	84
Setting Up Security Adapter Authentication: A Scenario	85

Chapter 7. Web Single Sign-On and Remote Authentication

Web SSO	104
Implementing Web SSO Authentication	106
Deployment Options for Web SSO	107
Digital Certificate Authentication	108
Setting Up Web SSO: A Scenario	108
Remote Authentication	126

Chapter 8. Authentication Details

Using the LDAP/ADSI Configuration Utility	129
Authentication Options	137
Roles	137
Secure Login	139
User Password Encryption	140
Credentials Password Encryption	143
Application User	145
Checksum Validation	149
Remote Configuration	150
Secure Adapter Communications	152
Shared Database Account	153
Adapter-Defined User Name	154
User Specification Source	157
Anonymous User	158
Secure Views	159
Digital Certificate Authentication	160
Configuration Parameters Related to Authentication	161
Eapps.cfg Parameters	162
Siebel Application Configuration File Parameters	164
Siebel Name Server Parameters	172
System Preferences	175
Login Features	177
Remember My User ID and Password	178
Forgot Your Password?	178
Account Policies	179
URL Login	179
Cookies and Session Management	181
Session Cookie	181
Auto Login Cookie	182
Cookieless Sessions	182

Chapter 9. User Administration

Overview of User Registration	183
Requirements	184
Seed Data	184
Unregistered Users and Anonymous Browsing	185
Implementing Anonymous Browsing	185
Self-Registration	188
The End User Experience for Self-Registration	188
Implementing Self-Registration	190
Modifying Self-Registration Views and Revising Workflow Processes	195
Forgot Your Password?	212
Internal Administration of Users	224
User Authentication Requirements	224
Adding a User to the Siebel Database	226
The New Responsibility Field	234
External Administration of Users	236
User Authentication Requirements	236
Access Considerations	237
Registering Users	237
Maintaining a User Profile	244
Editing Personal Information	244
Changing a Password	245
Changing the Active Position	245

Chapter 10. Access Control

Access Control Overview	248
Data	249
Parties	252
How Parties Relate to Each Other	265
Access Control Mechanisms	265

Planning for Access Control	277
Business Environment Structure	277
Defining a Company Structure	280
Implementing Basic Access Control	289
Application Level Access Control	290
Responsibilities	291
Business Component View Modes	295
Applet Access Control Properties	299
View Access Control Properties	302
An Example of Flexible View Construction	306
Administering Access Group Access Control	308
A Scenario That Applies Access Group Access Control	309
The User's Experience	313
Administrative Tasks	313
Administering Catalogs of Data	314
Administering Positions, Organizations, and User Lists	314
Administering Access Groups	316
Associating Access Groups With Data	319
Supplemental Access Control	322
Creating and Administering Roles	322
Configuring Visibility of Pop-Up and Pick Applets	331
Merging Organizations	333

Appendix A. Troubleshooting

User Authentication Issues	335
User Registration Issues	337
Access Control Issues	340
Encryption Issues	341

Appendix B. Siebel Application Configuration File Names

Configuration Files 343

Appendix C. Seed Data

Seed Employee 346
Seed Users 347
Seed Responsibilities 348
Seed Position and Organization 349
Seed Database Login 349

Index

Introduction

This guide provides a description of security resources available for Siebel applications. It includes configuration information and guidelines for using these resources.

NOTE: All Siebel MidMarket product names include the phrase *MidMarket Edition* to distinguish these products from other Siebel eBusiness Applications. However, in the interest of brevity, after the first mention of a MidMarket product in this document, the product name will be given in abbreviated form. For example, after Siebel Call Center, MidMarket Edition, has been mentioned once, it will be referred to simply as Siebel Call Center. Such reference to a product using an abbreviated form should be understood as a specific reference to the associated Siebel MidMarket Edition product, and not any other Siebel Systems offering. When contacting Siebel Systems for technical support, sales, or other issues, note the full name of the product to make sure it will be properly identified and handled.

Although job titles and duties at your company may differ from those listed in the following table, the audience for this guide consists primarily of employees in these categories:

Siebel Application Administrators	Persons responsible for planning, setting up, and maintaining Siebel applications.
Siebel Application Developers	Persons who plan, implement, and configure Siebel applications, possibly adding new functionality.
Siebel System Administrators	Persons responsible for the whole system, including installing, maintaining, and upgrading Siebel applications.

This guide assumes you are familiar with the basic design and structure of Siebel applications installed on your corporate network and how Siebel Enterprise components are deployed on the network.

How This Guide Is Organized

Major topics covered in this guide include:

- A description of security resources available for Siebel applications and configuration guidelines to take advantage of these resources. Information on physical deployment, firewalls, data encryption, and network monitoring is included.
- Methods of user authentication available for Siebel applications, including database authentication, LDAP/ADSI authentication, and Single Sign-On. Example scenarios for setting up a user authentication system are provided.
- User administration issues related to managing users on your site. Information on adding users, maintaining user profiles, and self-registration is included.
- Setting up an access control system to define how users view information in Siebel applications. It includes planning strategies for creating an overall business environment structure for your applications.
- Troubleshooting tips for security-related issues.

Revision History

Security Guide for Siebel eBusiness Applications MidMarket Edition, Version 7.5

This book replaces *Authentication and Access Control Administration Guide, MidMarket Edition*.

This section provides an overview of security resources available for Siebel applications.

Managing Security in Corporate Networks

When assessing the security needs of an organization and evaluating security products and policies, the manager responsible for security must systematically define the requirements for security and characterize the approaches to satisfying those requirements.

To create an effective security plan, a manager must consider the following:

- What types of actions or security attacks can compromise the security of information owned by an organization?
- What mechanisms are available to detect, prevent, or recover from a security breach?
- What services are available to enhance the security of data processing systems and information transfers within an organization?

Classifications of security services include:

- **Confidentiality.** Confidentiality makes sure that stored and transmitted information is accessible only for reading by the appropriate parties.
- **Authentication.** Authentication makes sure that the origin of a message or electronic document is correctly identified, with an assurance that the identity is correct.
- **Integrity.** Integrity makes sure that only authorized parties are able to modify computer system assets and transmitted information.
- **Nonrepudiation.** Nonrepudiation requires that neither the sender or receiver of a message be able to deny the transmission.
- **Access control.** Access control requires that access to information resources can be controlled by the target system.

This guide describes security services available on the Siebel network. These services are intended to counter security attacks and use one or more security mechanisms to provide the service.

Using Industry Standards

Siebel eBusiness Applications adhere to common security standards to facilitate the integration of its applications into the customer environment. Siebel Systems is not a vendor of specific security components; instead, its applications are designed so that customers can choose a security infrastructure that best suits their specific business needs. Supported standards include:

- SSL—Protection of Siebel HTML applications by leveraging the SSL capabilities of supported Web servers (such as Microsoft IIS).
- LDAP—Siebel Systems provides preconfigured integration with LDAP. Integration is currently certified with Microsoft Active Directory. Siebel Systems also includes Novell NDS certification.
- RSA—Communication between Siebel components can be encrypted on the NT platform using RSA algorithms in the form of Microsoft MSCrypto. Siebel Systems has cross-platform support for this feature using RSA BSAFE. RSA BSAFE is FIPS 140-1 certified.
- x.509—Siebel applications use the SSL capabilities of the supported Web servers to enable authentication based on x.509 client certificates.

To further augment the security of customer's overall deployment, Siebel Systems has alliances with other leading security providers including Baltimore, Oblix, Entrust, and Netegrity.

Siebel Security Architecture

The components of Siebel security architecture include:

- User authentication for secure system access
- End-to-end encryption for data confidentiality
- Authorization for appropriate data visibility
- Audit trail for data continuity
- Secure physical deployment to prevent intrusion
- Security for mobile devices

User Authentication for Secure System Access

Siebel Systems has developed an open authentication architecture that integrates with a customer's selected authentication infrastructure. Siebel Systems supports three primary types of authentication:

- Native database authentication
- Security adapters for external authentication
- Web Single Sign-On

These authentication mechanisms apply whether users access the Siebel application from within a local area network, a wide area network, or remotely. [Figure 1](#) shows the three primary types of user authentication within a Siebel site.

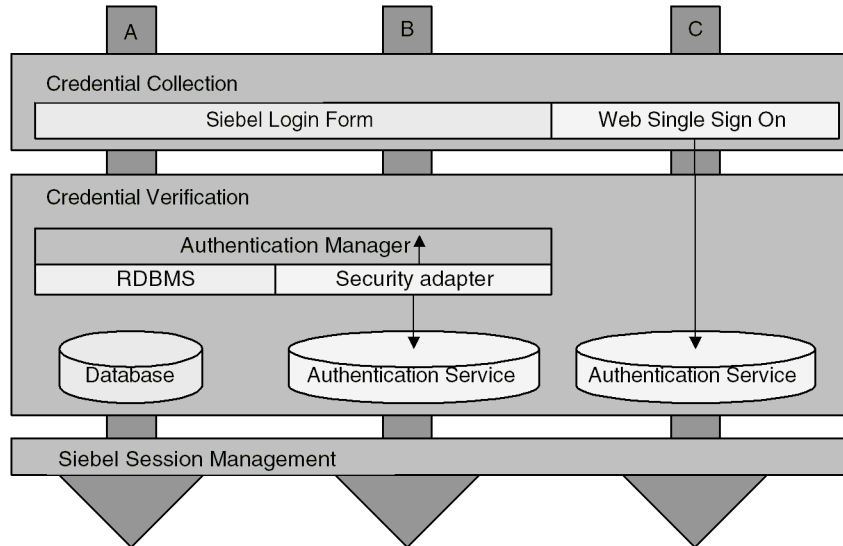


Figure 1. Methods of User Authentication Within a Siebel Site

Database Authentication

For employee applications, Siebel Systems provides internal mechanisms for credential collection and verification. The default login form collects Siebel username and password credentials. The underlying security systems of the database verify users' credentials. Each user must have a valid database account in order to access the Siebel application. The internal authentication deployment supports password encryption for protection against hacker attacks.

Security Adapters for External Authentication

For employee or customer applications, Siebel Systems includes a preconfigured security adapter interface to allow organizations to externalize credential verification. The interface connects to a security adapter, which contains the logic to validate credentials to a specific authentication service.

Siebel Systems customers can therefore verify user credentials with security standards like the lightweight directory access protocol (LDAP). Siebel Systems has developed security adapters for the leading authentication services: Novell NDS and Microsoft Active Directory.

Siebel Systems also offers a documented application programming interface and a software developer's toolkit to allow companies to build additional adapters to support other authentication technologies such as digital certificates, biometrics, or smart cards. For example, the RSA Secure ID is a portable token that provides users a key that changes every minute; only by supplying both the key and their password can a user gain access to the Siebel application.

The security adapter interface is critical to the Siebel architecture because for most Siebel Systems customers, authentication has become an enterprise decision, rather than an application-specific decision. The authentication service can be a shared resource within the enterprise, thereby centralizing user administration.

Web Single Sign-On

Siebel Systems offers customers the capability to enable a single login across multiple Web applications – also known as Web Single Sign-On (SSO). Siebel Systems provides a configurable mechanism for communicating with Web SSO infrastructures, identifying users, and logging users into Siebel applications.

With Web SSO, users are authenticated independently of Siebel applications, such as through a third-party authentication service, or through the Web server (such as Microsoft IIS). The following authentication service solutions have been validated to work with Siebel products in Web SSO integration: Netegrity SiteMinder, IBM Tivoli Policy Director, Oblix NetPoint, and Entrust GetAccess.

End-to-End Encryption for Data Confidentiality

Encryption converts data into a ciphered form for transmission over a network. It safeguards data from unauthorized access. Stored data as well as transmitted data must be protected from intrusive techniques (such as sniffer programs) that can capture data and monitor network activity.

End-to-end encryption protects confidentiality along the entire data path: from the client browser, to the Web server, to the Siebel application server, to the database. [Figure 2](#) shows the types of data encryption available in the Siebel environment.

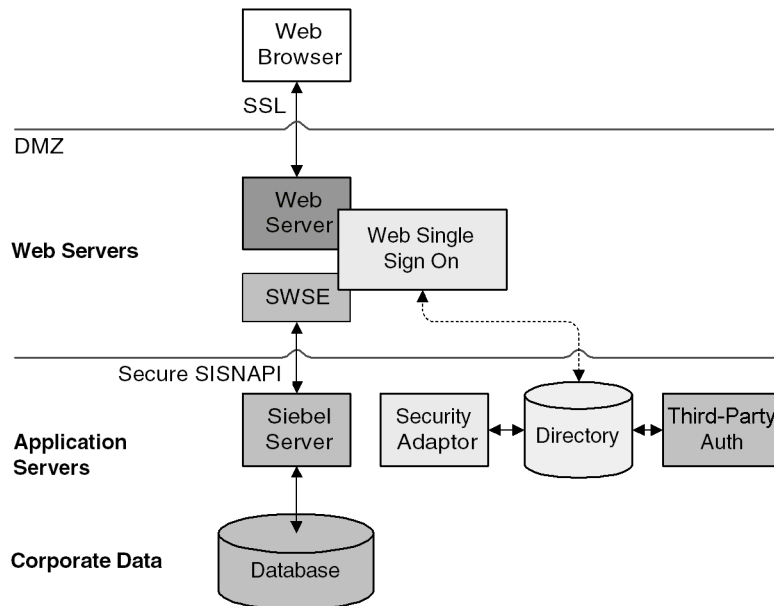


Figure 2. Data Encryption in the Siebel Environment

Client Browser to Web Server

Siebel Systems provides zero-footprint Web applications that run in a standard Web browser. When a user accesses a Siebel application, a Web session is established between the browser and Siebel server. Secure socket layer (SSL) protects against session hijacking when sensitive data is transmitted. Siebel applications support 128-bit SSL data encryption, an extremely secure level of protection for Internet communications.

Siebel customers can configure which Web pages (known as *views*) within the Siebel application use SSL. SSL can be configured on a page-by-page basis. For example, some customers use SSL only on the login screen to protect the password transmission while other customers apply SSL to an entire application.

Web Server to Siebel Server

Siebel software components communicate over the network using a Siebel TCP/IP-based protocol called SISNAPI (Siebel Internet Session API). Customers have the option to secure SISNAPI using embedded encryption from either RSA or Microsoft (MSCrypto). In both cases, these technologies allow data to be transmitted securely between the Web server and the Siebel application server without fear of intrusion.

Siebel Server to Database

For secure transmission between the database and the Siebel application server, data can be encrypted using the proprietary security protocols specific to the database that a customer is using. To provide an additional level of security at this stage, Siebel applications support data encryption through integration with RSA Bsafe Crypto.

Database Storage

Siebel applications allow customers to encrypt sensitive information stored in the database so that it cannot be viewed without access to the Siebel application. Customers can configure Siebel software to encrypt a field of data before it is written to the database and decrypt the same data when it is retrieved. This prevents attempts to view sensitive data directly from the database.

Authorization to Control Data Visibility

Authorization refers to the privileges or resources that a user is entitled to within Siebel applications. Even among authenticated users, organizations generally want to restrict visibility to system data. Siebel applications use two primary access control mechanisms:

- View level access control to manage which functions a user can access.
- Record level access control to manage which data items are visible to each user.

Access control provides Siebel customers with unified administration for access to millions of content items for millions of users.

View Level Access Control

Organizations are generally arranged around functions, with employees being assigned one or more functions. View level access control determines what parts of the Siebel application a user can access, based on the functions assigned to that user. In Siebel applications, these functions are called *responsibilities*.

Responsibilities define the collection of views to which a user has access. An employee assigned to one responsibility may not have access to parts of the Siebel applications associated with another set of responsibilities. For example, typically a system administrator has access to view and manage user profiles, while other employees do not.

Record Level Access Control

Record level access control assigns permissions to individual data items within an application. This allows Siebel customers to authorize only those authenticated users that need to view particular data records to access that information.

Siebel applications use three types of record level access: position-based, organization-based, and access group-based.

When a particular position, organization, or access group is assigned to a data record, only employees within that position, organization, or access group can view that record.

A position represents a place in the organizational structure, much like a job title. Typically a single employee occupies a position; however, it is possible for multiple employees to share a position. Position access allows Siebel customers to classify users so that the hierarchy between them can be used for access to data. For example, a supervisor would have access to much of the data that a subordinate has access to; the same applies to others who report to the same boss.

Similarly, an organization – such as a branch of an agency or a division of a company – is a hierarchy of positions. Those employees assigned to a position within a certain organization are granted access to the data that has been assigned to that organization. Employees cannot see data outside their own organization.

An access group is a less-structured collections of users, such as a task force. Groups can be based on some common attribute of users, or even created on an ad hoc basis, pulling together users from across different organizations and granting them access to the same data.

Auditing for Data Continuity

Siebel Systems supports various degrees of auditing.

- At the simplest level, each data record has created and last updated fields (when and by whom). Second, with configuration, you can generate an activity for additional levels of auditing. This is best used when there are limited needs for auditing (just a few areas to track).
- Siebel applications can maintain an audit trail of information that tells when business component fields have been changed, who made the change, and what has been changed.
- Siebel customers can also rely on database auditing that is included with all supported databases. All vendors support high levels of audits: B3 or C2 Orange book levels. (Database auditing requires additional space and a security person to review the audit information.)
- Siebel's Business Process Administration allows you to configure workflow processes to save information on changes to specific business components.
- You can also attach scripts to the business component Write_Record event and save information about the transaction.

Secure Physical Deployment to Prevent Intrusion

Access to the physical devices that host Siebel applications must also be protected. If these devices are compromised, the security of all applications on the machine are at risk. Utilities that provide machine-level security, by either enforcing machine passwords or encrypting the machine hard drive, can be used and are transparent to the Siebel application.

In employee application deployment, clients as well as servers are often sitting behind a firewall. In customer or partner application deployment, or in employee application deployment where employees accessing the application are sitting outside of the firewall, the Siebel application server is deployed behind a firewall and resides in a *demilitarized zone* (DMZ).

A Web server sits in the DMZ, with clients outside the firewall accessing the Web server and Siebel application server through a secure connection. Siebel Systems also supports reverse proxy configuration to further enhance the DMZ security. Increasingly, firewall vendors are offering virtual private network (VPN) capabilities. VPNs provide a protected means of connecting to the Siebel application for workers who require remote access.

Siebel works with leading third-party security providers to provide additional physical security measures, such as attack prevention, data back-up, and disaster recovery. For example, Resonate protects against denial of service attacks by handling the TCP connections and catching incoming attacks before they ever reach the Siebel server. Furthermore, with Resonate, only one IP address and one port need to be opened on the firewall between Web server and Siebel server.

Additionally, Siebel Systems architecture takes advantage of technologies such as Microsoft Cluster Services, that allow multiple computers to function as one by spreading the load across multiple systems. Cluster Services addresses the need for failover and catastrophic recovery management.

Security for Mobile Solutions

Siebel Systems also provides a broad suite of mobile solutions that allow remote access to data within Siebel eBusiness applications. These solutions support a wide variety of mobile platforms, that includes laptop computers. Siebel Systems provides security for customers using these devices to access Siebel applications. Siebel Systems also works with a range of alliance partners to provide the latest in security for mobile computers.

Device User Authentication

Devices themselves must be secure. If a device falls into the wrong hands, organizations need assurance that sensitive data will not be compromised. Siebel applications are fully compatible with the embedded security within these devices, as authentication is generally a device-level decision, rather than an application-specific one.

This section provides guidelines on how to configure your Siebel applications to take advantage of Siebel security resources. It includes information on changing default passwords.

Security Roadmap

This section provides an overview of the tasks you can perform to take advantage of Siebel's security resources. Use this as a checklist for setting up security in your Siebel environment.

Each task includes a pointer for more information on how to perform the task. Pointers include references to the remaining sections in this guide as well as other Siebel eBusiness Applications guides on the *Siebel Bookshelf*.

- 1** During Siebel Systems installation, install Resonate Central Dispatch to manage port numbers and provide firewall protection on your network. See [“Physical Deployment and Auditing” on page 35](#) and *Siebel Server Installation Guide*.
- 2** After you install your Siebel site, change the default passwords for Siebel accounts. See [“Changing Default Passwords” on page 27](#).
 - Change the SYSADM password.
 - Change the DBO and DBA passwords.
- 3** Make sure communications and important data is encrypted. See [“Communications and Data Encryption” on page 45](#).
 - Enable encryption for SISNAPI communications between Siebel components. See [“Configuring for Encryption” on page 49](#).
 - Make sure important data such as passwords or credit card numbers are encrypted. See [“Password Encryption” on page 53](#) and [“Business Component Encryption” on page 54](#).

- 4** Implement security adapter authentication or Web Single Sign-On to validate users. For more information, see [“User Authentication” on page 63](#).
 - Configure the Siebel Web Engine to use HTTPS protocol to transmit user credentials from the browser to the Web server. See [“Secure Login” on page 139](#).
 - Require URLs to use HTTPS protocol for some (or all) views in your Siebel applications. See [“Secure Views” on page 159](#).
 - Manage database access by creating a single Application User account and encrypt the Application User password. See [“Application User” on page 145](#).
 - If you are using Web Single Sign-On, enable X.509 digital certificate authentication and change the default TrustToken setting. See [“Digital Certificate Authentication” on page 160](#).
 - For LDAP/ADSI authentication, turn on password syntax check, password expiration, and user account lockout (if available). See [“Account Policies” on page 179](#).
- 5** Set up an access control system to control visibility of data records and views to each individual user. For more information, see [“Access Control” on page 247](#).
- 6** Create an audit trail to monitor database updates and changes. See [“Auditing for Data Continuity” on page 43](#). Also see *Applications Administration Guide, MidMarket Edition*.
- 7** Make sure communications between mobile Web clients and your Siebel site are secure.
 - Change the DBA password. See [“Changing the Siebel Local \(DBA\) Password” on page 33](#).
 - Enable encryption for mobile Web clients. See [“Configuring Web Clients for Encryption” on page 50](#).

Also see *Siebel Remote Administration Guide, MidMarket Edition*.

Changing Default Passwords

The Siebel installer and seed data provided with Siebel Server and Siebel eBusiness Applications creates a number of default accounts on your site. These accounts are used to manage and maintain your Siebel network. To safeguard the security of your site, make sure you change the default passwords for these accounts. The following sections include procedures for changing account passwords.

Figure 3 shows the Password and Table Owner fields used to store passwords.

The figure consists of two screenshots of Siebel configuration windows. The top window is titled 'Server Parameters' and shows a table of parameters. The 'Password' parameter is highlighted in yellow. The bottom window is titled 'Enterprise Parameters' and shows a table of parameters. The 'Table Owner Password' parameter is highlighted in yellow.

Parameter	Type	Effective Immediate	Current Value	Value on Restart	Subsystem	Description
Comm Template Name List	String	✓			Communications Out	Package(s)
OM - Proxy Employee	String	✓			Object Manager	Login Name
ParametricSearchResultsView	String	✓	Parametric Search Results Vie	Parametric Search F	Infrastructure Shop	Parametric
Password	String	✓	*****	*****	Database Access	Database
PersistentShoppingCart	String	✓	FALSE	FALSE	Infrastructure Shop	Persistent
PostAddToCartLogic	String	✓			Infrastructure Shop	PostAddTo
Price Item Cache Size	Integer	✓	100	100	Infrastructure Pricin	The price

Parameter	Datatype	Value	Default Value	Subsystem	Required?	Description
TABLEID	String			Data Dictionary Manager		Table Id
Table Groupings File	String			Database Access		Table groupings file
Tablespace Name	String			Database Access		Tablespace name for the S
Table Owner	String	SIEBEL	Siebel	Database Access		Table owner for the Siebel
Table Owner Password	String	*****	*****	Database Access		Database password for the
Test Executable Search Path	String			Testing Subsystem		List of directories to search
Test Input Data Search Path	String			Testing Subsystem		List of directories to search

Figure 3. Changing Default Passwords

Changing the SADMIN Password on Windows

The Siebel database server installation script creates a Siebel administrator account that you can use to perform administrative tasks. The default user ID and password for this account are SADMIN and SADMIN (case sensitive).

The steps required to change the Siebel Administrator's password depend on whether the Windows login user name is the same as the username for the Siebel Administrator's database account.

Same Login Name

When the Windows login user name is the same as the username for the Siebel Administrator's database account, use the following procedure to change the password.

To change the Siebel Administrator's password

- 1** Change the Windows domain login password.

For more information on changing domain passwords, refer to your Windows documentation.

- 2** Change the password for the Siebel server system service in the Windows Control Panel.
 - a** In the Windows NT Control Panel, double-click Services. In Windows 2000, choose Start > Programs > Administrative Tools > Services.
 - b** Select the Siebel Server System Service and click Startup.
 - c** Change the password in the Password and Confirm Password fields, and click OK.
- 3** Change the password in Server Manager.
 - a** Log in to a Siebel employee application (such as Siebel Call Center) and choose View > Site Map > Server Administration > Servers.
 - b** In the Siebel servers list, select the appropriate Siebel server. Then, click the Server Parameters tab.
 - c** In the Server Parameters list, locate Password.
 - d** In the Current Value field, type in the new password, and then click Save.

- 4** If you are using Resonate Central Dispatch, you may also wish to change the password used to log in to Resonate.
 - a** In a Siebel employee application, choose View > Site Map > Server Administration > Enterprise Configuration > Enterprise Parameters.
 - b** In the Enterprise Parameters list, select Resonate password. Then, type in the new password and click Save.
- 5** Change the password in the database.

For more information, refer to your RDBMS documentation on changing passwords.
- 6** If you changed the Resonate password, stop and restart the Resonate service.
- 7** Stop and restart the Siebel server service.

Different Login Name

When the Windows login user name is different from the user name for the Siebel Administrator's database account, use the following procedure for changing the password.

To change the Siebel Administrator password

- 1** Complete [Step 1](#) and [Step 2 on page 28](#).
- 2** Stop and restart the Siebel server service.

Changing the Table Owner (DBO) Password

The Siebel database server installation script also creates a database Table Owner (DBO) account used to modify the Siebel database tables. The default user ID and password for this account are SIEBEL and SIEBEL (case sensitive).

To change the Table Owner password on Windows

- 1** Change the password in Server Manager.
 - a** Log in to a Siebel employee application, such as Siebel Call Center.
 - b** Choose View > Site Map > Server Administration > Servers.
 - c** In the Siebel servers list, select the appropriate Siebel server. Then click the Server Parameters tab.
 - d** In the Server Parameters list, locate Table Owner Password.
 - e** In the Current Value field, type in the new password, and then click Save.
- 2** Change the password in the database.

For more information on changing passwords, refer to your RDBMS documentation.
- 3** Restart the Siebel server.

- 4** After Siebel server is restarted, check to make sure all server tasks are still running.
 - a** Choose View > Site Map > Server Administration > Servers.
 - b** In the Siebel servers list, select the appropriate Siebel server.
 - c** Click the Server Tasks tab and check to see if any server tasks have an error.

The following figure shows an example of the Call Center Object Manager task with an error.

The screenshot shows a table with columns: Task, Component, Task State, Status, PID, and Start Time. The 'Server Tasks' tab is selected. Task 2230, 'Call Center Object M', is in an 'Error' state. Task 2228, 'Call Center Object M', is in a 'Running' state with a status of 'Waiting for comman'.

Task	Component	Task State	Status	PID	Start Time
2233	Server Manager	Running	Processing "List Ta	2,344	7/26/2002 12:36:37
2232	Sales Object Manag	Running	Handling Request	2,568	7/26/2002 12:35:28
2231	Sales Object Manag	Completed			7/26/2002 12:34:48
2230	Call Center Object M	Error			7/26/2002 12:34:21
2229	Call Center Object M	Completed			7/26/2002 12:33:22
2228	Call Center Object M	Running	Waiting for comman	2,696	7/26/2002 12:32:48
2227	Communications Se	Completed			7/26/2002 12:24:54

- 5** For each Server Task that displays an error, update both the SYSADM and Table Owner Password for that task.
 - a** Choose View > Site Map > Server Administration > Enterprise Configuration.
 - b** Click the Component Definitions tab and select the component that initiated the failed task.

The following figure shows the Call Center Object Manager component associated with a failed task. It also shows the Password parameter for the Call Center Object Manager.

The screenshot displays two windows from the Siebel Enterprise Configuration tool. The top window, titled 'Component Definitions', shows a table of system components. The bottom window, titled 'Query Results', shows the parameters for the selected component.

Name	Component Type	Definition State	Component Group	Description	Alias	Run Mode
Appointment Booking Engine	Appointment Bookin	Active	Field Service	Book appointments	ApptBook	Batch
Assignment Manager	AsgnSrvr	Active	Assignment Manage	Assigns positions a	AsgnSrvr	Batch
Batch Assignment	AsgnBatch	Active	Assignment Manage	Batch assigns posit	AsgnBatch	Batch
Business Integration Batch Manager	EAI Business Integr	Active	Enterprise Applicati	Manages Business	BusIntBatchMgr	Batch
Business Integration Manager	EAI Business Integr	Active	Enterprise Applicati	Executes Business	BusIntMgr	Batch
Call Center Object Manager (ENU)	AppObjMgr	Active	Siebel Call Center	Siebel Call Center O	SCCObjMgr_enu	Interactive
Client Administration	Client Administration	Active	System Managemer	Manages license en	ClientAdmin	Background

Parameter	Fixed	Value	Data Type	Parameter Type	Description
Password		*****	String	Subsystem	Database user password

- c** When the list of Parameters for the component appears, locate the Password parameter and enter the new SADMIN password.
- d** Then locate the Table Owner Password and enter the new Table Owner password.

Changing the Siebel Local (DBA) Password

For security purposes, you may want to change the local DBA password on mobile Web clients. To accomplish this task, you should change the DBA password in the database template file before generating the new database template.

The following is an overview of how to change the DBA password in the SQL Anywhere environment. You can use this as a model for changing the password in your own environment. For details, see *Siebel Remote Administration Guide, MidMarket Edition*.

To change the local DBA password on mobile Web clients

- 1 Run the Interactive SQL utility (dbisqlc.exe) on the server machine.

- a Change to the bin directory in the Siebel server root directory:

```
cd \<SiebelServerRoot>\bin
```

- b Start the utility by entering:

```
dbisqlc -c "UID=DBA;PWD=SQL;DBF=siebel\dbtempl\my_templ.dbf"
```

- 2 Enter the following command:

```
grant connect to user_id identified by new_password
```

For example, to set a new password of MYPASSWORD for the user DBA, enter:

```
grant connect to DBA identified by MYPASSWORD
```

NOTE: You must use upper case for every password in SQL Anywhere.

- 3 Click Execute.
- 4 Run the Generate New Database component using the new DBA password.

For more information on running the Generate New Database component, see *Siebel Remote Administration Guide, MidMarket Edition*.

- 5 Run a Database Extract for mobile Web clients and notify mobile users to initialize their databases.

For information about extracting the database and initializing a local database, see *Siebel Remote Administration Guide, MidMarket Edition*.

Physical Deployment and Auditing

3

Where and how network computing resources reside, as well as how they work in connection with the Internet and other machines on the local network, can have a significant impact on network security.

This section describes security issues related to physical deployment of Siebel components on the network. For more information, see the *Siebel Server Installation Guide* for the operating system you are using.

Figure 4 shows the basic components included in a Siebel Systems network.

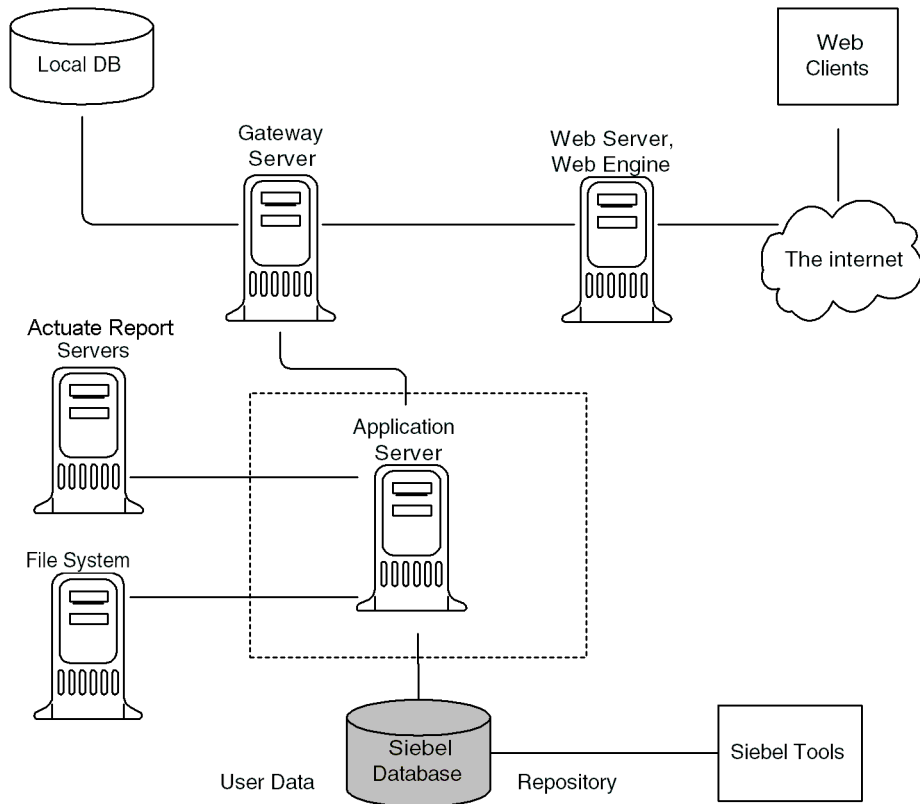


Figure 4. Siebel Network Components

Firewall Support

A firewall separates a company's public Web clients from its internal network and controls network traffic between the two domains. A firewall defines a focal point to keep unauthorized users out of a protected network, prohibits vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.

Firewalls simplify system security by consolidating security resources. Firewalls often include one or more of the following capabilities:

- **Proxy.** A proxy (also known as an application-level gateway) acts as an intermediary to prevent direct connection between a local corporate network and the outside world. Proxy services shield internal IP addresses from the Internet.
- **Network Address Translation (NAT).** NAT technology transparently rewrites the IP addresses of Internet connections as they move across the firewall boundary. This allows multiple computers in a local network to hide behind a single IP address on the Internet.
- **Virtual Private Networks (VPN).** VPN is a technique that allows computers outside the firewall to tunnel traffic through a firewall, then appear as if they are connected inside the firewall. VPN technology allows employees working at home or on the road to access many corporate intranets (for example, mail servers, file shares, and so on) which otherwise would not be sufficiently secured to be placed outside the firewall.

Recommended Placement

This section describes a placement of firewalls with respect to Siebel network components. A Siebel network typically has four zones:

- The Internet zone where Web clients reside.
- The Web Server zone where Siebel Web servers and Web server load balancers reside. Sometimes called the DMZ (demilitarized zone), this zone is where the external network first interacts with the Siebel environment.

- The Application Server zone where components that reside inside this zone include Siebel application servers, the gateway name server, a connection broker (such as Resonate Central Dispatch scheduler), and the authentication server.
- The Data Server zone where the Siebel Database and Siebel file system and database server reside. Typically, this is where the most critical corporate assets reside. Access to this zone should be limited to authorized application administrators and database administrators only.

Siebel network architecture allows you to install firewalls between each of these zones. However, for optimum performance, Siebel Systems does not recommend installing a firewall between the Application Server zone and the Data Server zone. Siebel Systems also does not recommend installing a firewall between the Siebel Database and the Siebel database server. [Figure 5](#) shows the recommended placement for firewalls in Siebel networks.

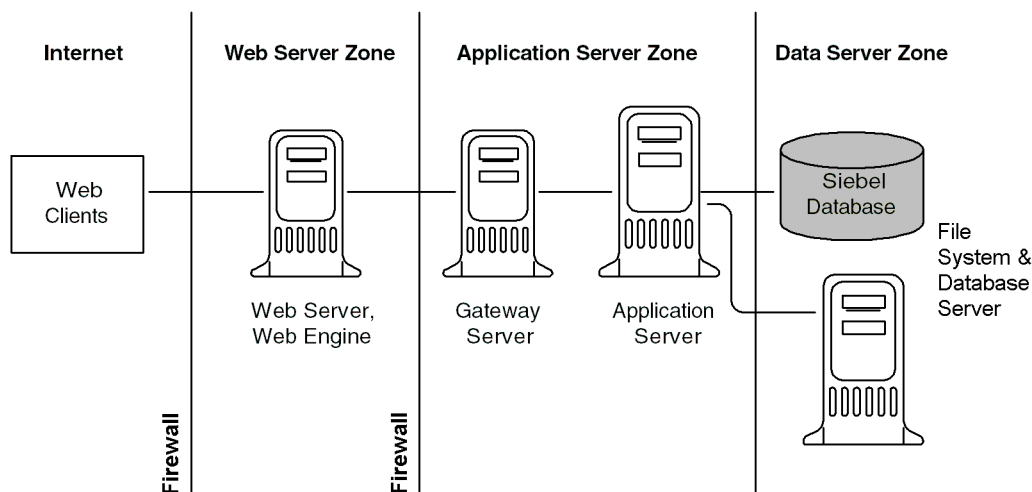


Figure 5. Firewalls in Siebel Networks

For additional security, Siebel Systems recommends installing an additional Web server to act as a proxy to handle traffic between the Web clients and the Web server that contains the Siebel Web Server Extension (SWSE).

Resonate Support

Siebel Systems works with Resonate, a leading third-party supplier of security products to provide additional physical security measures. Resonate minimizes the number of ports and addresses that need to be opened on the firewall between the Web server and Siebel server. Resonate can be configured to use only one IP (VIP) and one port (Virtual Port) for all Siebel to Web server communications.

Single port exposure allows you to consolidate network access for better port monitoring and security. It also provides simplified firewall configuration. You only have to configure one virtual port, not many.

Additional Resonate security features include:

- **Denial of Service (DoS) Attack prevention.** In a DoS attack, Resonate helps handle the TCP connections. Incoming attacks can be cached at the scheduler before they ever reach the Siebel server. Resonate Central Dispatch has built-in mechanism to stop DoS attacks right at the point of entry.
- **Virtual IP addressing.** Resonate's VIP shields hackers from accessing the Siebel servers directly. Because it is an IP alias, no physical addresses are ever exposed. Web Servers in the DMZ communicates with the VIP only.
- **TCP Handshake protection.** The TCP handshake is replayed from the Resonate Scheduler to the Siebel server rather than directly from the Web server to the Siebel server.
- **NAT firewall.** Resonate allows you to install a Network Address Translation (NAT) firewall between the Siebel server and the Web server.

For information on configuring and installing Resonate Central Dispatch on your Siebel site, see the *Siebel Server Installation Guide* for the operating system you are using.

Port Numbers

Unless your network requires static ports, use dynamic ports for simplified installation and configuration as well as enhanced security.

If you use Resonate Central Dispatch, the scheduler uses a single port (default is 2320) to handle communications between the Siebel server and the Web Server. Otherwise, TCP ports 49152 (and higher) are used for Siebel components.

Some important planning issues for using port numbers include the following:

- To establish SSL communication for Siebel communications traffic between the Web browser and the Web server, specify an HTTPS port (default is 443) when you install the Siebel Web Server Extension.
- If you are setting up an LDAP/ADS directory server to use with your Siebel applications, use port 635 for secure transmission instead of port 389 for standard transmission.
- To allow users to access to Siebel applications across a firewall, make sure the Web server is accessible externally and that it can communicate with Siebel server using port 2320 (default) for TCP traffic.

If you are using Resonate, make sure the Web server can access the Gateway/Central Dispatch (through port 2320). The Central Dispatch Server must reside inside your corporate firewall and use a dynamic port (VIP) to communicate with Siebel server.

Once firewall access is available, users can be authenticated using LDAP or any other Siebel-supported method. For more information, see [“User Authentication” on page 63](#).

- Authorized vendors and remote users outside the firewall can use the standard Web server port (default is 80) to access Siebel Web applications. You can configure your firewall so that it will not pass traffic on anything other than port 80. If your Web server needs to support HTTP over SSL, you can open port 443.

NOTE: Siebel Remote deployment options do not rely on Telnet connections to the server. Telnet connections for remote users can be configured in the Siebel environment. However, because of possible security risks, Siebel Systems does not recommend it.

The COM data control and the Java DataBean both communicate using SISNAPI. COM data control supports both types of encryption. Java DataBean supports RSA encryption, but not MSCrypto.

- Port numbers for communications between the Siebel server and the Siebel database are database-specific. For example, the default TCP port number for communications with an Oracle database is 1521.
- Port numbers for communications between Siebel server and the Siebel file system and Database server are dependent on the file system type. The default TCP port number is 139. The default UDP port numbers are 137 and 138.

For more information, see the *Siebel Server Installation Guide* for the operating system you are using.

Restricting Access

This section describes security issues related to the physical deployment of products that interact with Siebel components.

Physical Security of the Client Device

The physical security of the client device is handled outside of the Siebel application. You can use utilities that provide machine-level security by either enforcing machine passwords or encrypting the machine hard drive.

Database Server Access

Customers should define stringent policies for database access both at the account login level and at the network visibility level. Only authorized users (for example, approved database administrators (DBAs) should have system accounts (for root usage) and remote access to the server. To restrict privileges to Siebel Server processes, assign an operating system account specific to the Siebel Server. This account should only have access to files, processes, and executables required by Siebel applications. The Siebel server account should not be the root administrator.

File System Access

The Siebel Database file system consists of a shared directory that is network-accessible to the Siebel Database Server and contains physical files used by Siebel clients. This file system stores documents, images, and other file attachments associated with Siebel applications.

Requests for access by Siebel user accounts are processed by Siebel servers, which then use the Siebel File System Manager to access the file system. The File System Manager processes these requests by interacting with the file system directory. To prevent direct access to Siebel files from outside the Siebel application environment, only the Siebel Service owner should have access rights to the Siebel file system directory. The Siebel server processes and components use the Siebel Service owner account to operate.

Auditing for Data Continuity

To maintain data continuity and monitor activity on a Siebel site, Siebel applications can maintain an audit trail of information that indicates when business component fields have been changed, who made the change, and what has been changed.

Audit Trail is a utility that creates a history of the changes that have been made to various types of information in various Siebel applications. An audit trail is a record showing who has accessed an item, which operation was performed, when it was performed, and how the value was changed. Therefore, it is useful for maintaining security and documenting modifications for future analysis and record keeping. Audit Trail logs information without requiring any interaction with, or input from users.

Companies can use Audit Trail to track data history in compliance with government directives, to analyze performance, and to improve service quality. Companies that use Audit Trail to track every change to every record to comply with government regulations must consider the performance ramifications of such massive auditing.

For Siebel Remote users making changes to records, Audit Trail records not only successfully committed transactions, but also transactions that did not get synchronized to the server because of conflicts.

For information on using Audit Trail, see *Applications Administration Guide, MidMarket Edition*.

Communications and Data Encryption

4

This section provides an overview of communications paths between Siebel Enterprise components and how to configure components for secure communications. It also describes encryption technologies available for transmitting and storing Siebel application data.

Types of Encryption

Encryption is a method of encoding data for security purposes. Some methods of encrypting, such as 128-bit encryption, are so difficult to break that U.S. export laws permit them to be used only within the United States. To avoid legal restrictions, Siebel Systems does not embed any encryption technology in its products. Instead, Siebel applications support industry standards for secure Web communications and encryption of sensitive data such as passwords.

To make sure that information remains private, the Siebel Smart Web Architecture uses the following encryption technology for transmitting and storing data:

- For data security over the Internet, Siebel uses the Secure Socket Layer (SSL) capabilities of its supported Web server platforms to secure transmission of data between the Web browser and the Web server and for connection to LDAP/ADS directories. Siebel applications can be configured to run completely under HTTPS, have specific pages run under HTTPS, or simply handle log in requests under HTTPS.

NOTE: With SSL enabled between Siebel and the LDAP Server, only the iPlanet LDAP Server has been completely tested by Siebel Systems. IBM Secureway and Novell eDirectory have not been tested with SSL and hence support for them with SSL turned on is limited.

- For communications between Siebel components, Siebel administrators can enable encryption for SISNAPI. SISNAPI is a TCP/IP-based Siebel Communications protocol that provides a security and compression mechanism for network communications. SISNAPI encryption can be based on either the MSCrypto API or RSA algorithms and works across multiple OS platforms.

- For database data encryption, Siebel applications allow customers to encrypt sensitive information (for example, credit card numbers, Social Security numbers, birth dates, and so on) so that it cannot be viewed without access to the Siebel application. Customers can configure Siebel software to encrypt a field of data before it is written to the database and decrypt the same data when it is retrieved. This prevents attempts to view sensitive data directly from the database.

For example, sensitive data can be encrypted using the RC2 Encryptor. RC2 encryption can be enabled for business component fields using Siebel Tools. For more information on using the RC2 Encryptor, see [“RC2 Encryption Administration” on page 56](#).

- For user authentication, Siebel administrators can also enable password and credentials encryption. This invalidates the user ID and password to unauthorized external applications and prevents direct SQL access to the data by anything other than Siebel eBusiness Applications. For more information, see [“Password Encryption” on page 53](#).

Figure 6 shows the types of encryption available in the Siebel application environment.

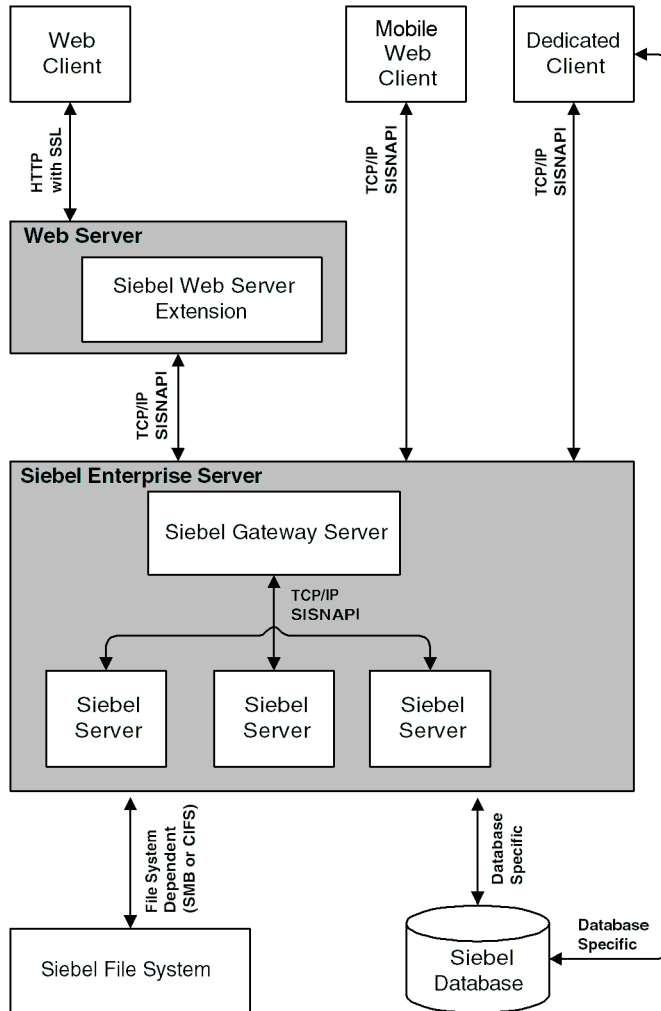


Figure 6. Communications Encryption in the Siebel Application Environment

Configuring for Encryption

The following sections provide an overview of how to set up encryption for communication between components in the Siebel environment.

Encryption is configured at the component level for data traffic between the server and the Web client. It is not used to encrypt the database or the data in it. Also, it is not used for communication with the database—check with your database vendor for that.

Configuring Siebel Server for Encryption

To enable encryption between Siebel server and the Web server

- 1 Start the Siebel Server Configuration Utility.

This utility appears when you first install Siebel server or you can launch it directly. For more information, see *Siebel Server Installation Guide* for the operating system you are using.

- 2 Enter the name of the Siebel server you want to configure.

The changes you make with the configuration utility are applied to the Siebel Application Object Manager. You can also use the utility to configure the Web Server extension.

- 3 Page to the Encryption Type screen in the utility and choose one of the following encryption settings:

MCRYPTO. Microsoft-encrypted communications protocol for communications between Siebel components.

RSA. A required protocol if you are using the RSA Security Systems 128-bit strong encryption feature for Siebel components.

- 4 Apply your settings and restart the server.

Repeat this procedure for each Siebel server in your application environment. Make sure you configure both the Siebel Application Object Manager and the Siebel Web Server extension. Set the same encryption type for all components.

Configuring Web Clients for Encryption

To use encryption, both the server and the client must enforce encryption in their connection parameters. If these parameters do not match, connection errors will occur.

Siebel eBusiness Applications support the following Web clients:

- **Siebel Web Client.** This client runs in a standard browser from the client personal computer and does not require any additional persistent software installed on the client.

This type of client uses configuration files located on the server. Encryption settings you make to the Siebel Web Server extension are automatically recognized by this Web client. For more information, see [“Configuring Siebel Server for Encryption” on page 49](#).

- **Siebel Mobile Web Client.** This client is designed for local data access, without the need to be connected to a server. Periodically, the client must access the Siebel Remote server using a modem, WAN, LAN or other network to synchronize data. For information on setting encryption for transmissions between mobile Web client and Siebel Remote server, see [“Encryption in Synchronization Networking” on page 50](#).
- **Siebel Dedicated Web Client.** This client connects directly to a database server for all data access. It does not store any Siebel data locally. With the exception of the database, all layers of the Siebel eBusiness Applications architecture reside on the user’s personal computer.

Encryption in Synchronization Networking

You can turn on encryption during the transfer of DX files between the Siebel server and mobile clients. DX files use SISNAPI messages to transfer information between mobile clients and Siebel server.

The Siebel mobile Web client reads configuration parameters in the Siebel configuration file (for example siebel.cfg used by Siebel Sales) to determine the type of encryption to use during synchronization. Encryption is the fifth parameter in the DockConnString.

To enable encryption on the mobile Web client

- 1 Open the configuration file you wish to edit. You can use any plain text editor to make changes to the file.

NOTE: When you edit configuration files, do not use a text editor that adds additional, non text characters to the file. For example, use Microsoft Notepad instead of Microsoft Word or WordPad.

- Configuration files for a client are stored in the client’s bin\ENU directory.
- When synchronization is performed within an application (using File > Synchronize > Database), configuration is read from the .cfg file associated with the application (for example, esales.cfg).

For a list of configuration files associated with Siebel applications, see [“Siebel Application Configuration File Names” on page 343](#).

- 2 Locate the DockConnString parameter in the [Local] section of the file.

This parameter specifies the name of the Siebel server used to synchronize with the client. It has the following format:

```
siebel server name:network protocol:sync port
#:service:encryption
```

Encryption is the fifth parameter in the DockConnString. It indicates the type of encryption used during synchronization.

An example of a DockConnString would be:

```
SEIBSPPI:TCPIP:40400:SMI:RSA
```

- 3 Override the default NONE and set encryption to MSCRYPTO or RSA.

The encryption you specify must match the encryption used by the Siebel server. If no value is specified (or the value is NONE), encryption is not enabled.

For example, to configure for RSA encryption, you could use either

```
AASRVR:TCPIP:40400:DOCK:RSA OR APPSRV: :RSA.
```

- 4 Save your changes and exit the file.

For more information about editing configuration files for Siebel Remote, see *Siebel Remote Administration Guide, MidMarket Edition*.

Key Exchange in Siebel Applications

The following steps explain how Siebel encryption keys are exchanged between the client and the server.

- 1 The client (for example, the Web server) generates a private/public key pair. The public key is sent as part of the Hello SISNAPI message to the Siebel server.
- 2 When the server receives a Hello message, it generates an RC4-based symmetrical session key and encrypts the symmetrical session key using the client's public key from the Hello message. The encrypted session key is sent back to the client as part of the Hello Acknowledge message.
- 3 The client uses its private key to decrypt the server-generated session key. From this point on, both the client and the server use the server-generated session key to encrypt and decrypt messages.
- 4 The session key is good for the lifetime of the connection.

Session Cookies

The Application Object Manager in the Siebel server communicates with the Siebel Web Client through the Web Server using TCP/IP protocol. An independent session is established to serve incoming connection requests from each client.

Siebel applications use session cookies to track the session state. These cookies persist only within the browser session and are deleted when the browser exits or the user logs off. A session cookie attaches requests and logoff operations to the user session which started at the login page.

Instead of storing the session ID in clear text in the client's browser, Siebel applications create an encrypted session ID and attach an encryption key index to the encrypted session ID. Session cookie encryption is based on the RSA B-Safe Crypto standard and uses a 56-bit key default.

In Siebel Remote, the encryption algorithm and key exchange are the same as session-based components.

Session cookie encryption prevents *session spoofing* (deriving a valid session ID from an invalid session ID).

Password Encryption

For user authentication security, user or credentials passwords can be encrypted. Encrypted passwords are stored in the Active Directory, LDAP directory, or the database, depending on which type of user authentication is being used.

- User password encryption can be implemented for both database and Siebel security adapter authentication, but not Web Single Sign-On authentication.
- Credentials password encryption can be implemented for Web Single Sign-On authentication and Siebel security adapter authentication, but not database authentication.

For more information on user password encryption, see [“User Password Encryption” on page 140](#). For more information on credentials password encryption, see [“Credentials Password Encryption” on page 143](#).

Siebel Systems provides a password encryption utility (shipped on separate CD-ROM) that can be used to encrypt passwords. This utility uses a proprietary hash function to encrypt passwords. Some things to remember about password encryption include:

- The password encryption utility does not automatically store hashed passwords in the Siebel database or directory. Instead, the administrator is responsible for setting up database accounts using the hashed passwords.
- Instead of using a Siebel-supplied algorithm, customers can use the Security Adapter SDK (Software Developers Kit) to access their own encryption or hash algorithms.

Business Component Encryption

For database data encryption, Siebel applications allow customers to encrypt sensitive information (for example, credit card numbers, Social Security numbers, birth dates, and so on) so that it cannot be viewed without access to the Siebel application. For example, you can encrypt sensitive data using the RC2 Encryptor.

- This section describes how to use Siebel Tools to enable and disable encryption for business components fields. (For more information, see *Siebel Tools Reference, MidMarket Edition*.)
- The following section, “[RC2 Encryption Administration](#),” describes how to use the RC2 Encryptor to add encryption keys to the keyfile and change the keyfile password.

Setting Encryption User Properties

Application developers can encrypt fields in a business component by setting the encryption user properties. A field is encrypted by setting the ID, encryption flag, and encryption service. Siebel provides two methods you can use to encrypt data fields:

- Standard Encryptor, based on a proprietary algorithm
- RC2 Encryptor, based on RSA encryption

CAUTION: Using Siebel standard encryption in a Unicode environment can result in irrecoverable data loss. Make sure you use RC2 encryption for your Siebel Unicode sites.

When encryption is turned on, data written to the field is encrypted and data read from the field is decrypted. Therefore, all business component fields that are mapped to the same database column must have encryption turned on with consistent user property settings.

To turn on encryption

- 1 Start Siebel Tools.
- 2 Select the business component that contains the field you want to encrypt.

- 3 In the field user properties, set the following encryption values:

Field User Property	Value	Description
Encrypted	Yes	Yes indicates the field is encrypted. No indicates the field is not encrypted.
Encrypt Service Name	RC2 Encryptor or Standard Encryptor	Sets the type of encryption to use for the field. For Unicode sites, use RC2 Encryptor.
Encrypt Key Field	<KeyIndexField>	The default setting is ID. If you are using the Standard Encryptor, set this value to ID. If you are using the RC2 Encryptor, specify the field on the business component where the encryption key index is stored. See Table 1 for some examples of Key Index Fields for business components.

Table 1. Encryption Key Index Fields

Business Component	Field	Key Index Field
Auction Invoice	Credit Card Number	Credit Card Number Key Index
FS Invoice	Credit Card Number	Credit Card Number Key Index
Order Entry - Orders	Credit Card Number	Credit Card Number Key Index
Personal Payment Profile	Account Number	Account Number Key Index
Quote	Credit Card Number	Credit Card Number Key Index
Cfg Favorites Quote Item	Credit Card Number	< Create new field >
Get Users Data	PayAcctNum	< Create new field >

RC2 Encryption Administration

You can encrypt sensitive data, such as customer credit card numbers, using the RC2 Encryptor. RC2 encryption can be enabled for business component fields using Siebel Tools. When encryption is enabled for a component, unencrypted data from the business component field is sent through the RC2 Encryptor. The RC2 Encryptor encrypts the data using an encryption key stored in the keyfile.

After the data is encrypted, it is sent back to the business component field to be stored in the database. When a user accesses this data, the encrypted data is sent through the RC2 Encryptor again to be decrypted. The data is decrypted using the same encryption key from the keyfile that was used for encryption. The decrypted data is then sent back to the business component field to be displayed in the application.

The keyfile stores a number of encryption keys that encrypt and decrypt data. The keyfile is named `keyfile.bin` and is located in the `admin` subdirectory of the Siebel server directory. Additional encryption keys can be added to the keyfile. For security, this file is encrypted using an encryption key generated from the keyfile password. To generate a new encryption key to encrypt the keyfile, change the keyfile password.

This section describes how to use the Key Database Manager to add encryption keys and to change the keyfile password. For information on how to enable and disable RC2 encryption for business components fields, see *Siebel Tools Reference, MidMarket Edition*.

NOTE: Siebel Systems does not support RC2 encryption for numeric data, but you can use the encryptor for information such as credit card numbers, which are stored as strings in the database. For more information on encrypting numeric data, see [“Encryption Issues” on page 341](#).

CAUTION: If you are upgrading from 56-bit encryption to 128-bit encryption, make sure you read [“If You are Upgrading” on page 61](#) before installing the Siebel Strong Encryption Package. For more information on the Siebel Strong Encryption Package, see the *Upgrade Guide* for the operating system you are using.

Using Key Database Manager

The Key Database Manager utility allows you to add new encryption keys to the keyfile and to change the keyfile password. The Key Database Manager utility is named `keydbmgr.exe` and is located in the `bin` subdirectory of the Siebel server directory.

Running Key Database Manager

Before running the Key Database Manager, make sure that the Siebel Name Server is running. The encryption key cache version used by the business components is stored in the Siebel Name server.

CAUTION: You must back up the keyfile before making changes to it. If the keyfile is lost or damaged, it may not be possible to recover the encrypted data without a backup keyfile.

To run the Key Database Manager

- 1 Shut down any server components that are configured to use RC2 encryption.

For information on shutting down server components, see *Siebel Server Administration Guide, MidMarket Edition*.

- 2 From the `bin` subdirectory in the Siebel server directory, run `keydbmgr.exe` using the following syntax:

```
keydbmgr /u db_username /p db_password /l language /c config_file
```

For descriptions of the flags and parameters, see [Table 2 on page 58](#).

- 3 When prompted, enter the keyfile password.

To add a new encryption key, see [“Adding New Encryption Keys” on page 58](#).

- 4 To change the keyfile password, see [“Changing the Keyfile Password” on page 59](#).

- 5 To quit the utility, enter 3.

- Restart any server components that were shut down in [Step 1 on page 57](#).

For information on starting server components, see *Siebel Server Administration Guide, MidMarket Edition*.

[Table 2](#) lists the flags and parameters for the Key Database Manager utility.

Table 2. Keydbmgr.exe Flags and Parameters

Flag	Parameter	Description
/u	<i>db_username</i>	Username for the database user
/p	<i>db_password</i>	Password for the database user
/l	<i>language</i>	Language type
/c	<i>config_file</i>	Full path to the siebel.cfg file

Adding New Encryption Keys

You can add new encryption keys to the keyfile. The RC2 Encryptor will use the latest key in the keyfile to encrypt new data; existing data will be decrypted using the original key that was used for encryption, even if a newer key is available. There is no limit to the number of encryption keys that you can store in the keyfile.

CAUTION: You must back up the keyfile before making changes to it. If the keyfile is lost or damaged, it may not be possible to recover the encrypted data without a backup keyfile.

To add new encryption keys

- Run the keydbmgr.exe utility from the bin subdirectory in the Siebel server root directory.

For information on running the keydbmgr.exe, see [“Running Key Database Manager” on page 57](#).

- To add an encryption key to the keyfile, enter 2.
- Enter a seed to generate a new encryption key.

The key must be at least 7 characters in length.

4 Quit the keydbmgr.exe utility.

When exiting the keydbmgr.exe utility, monitor any error messages that may be generated. If an error occurred, you may need to restore the backup version of the keyfile.

5 Distribute the new keyfile to all Siebel servers by copying the file to the admin subdirectory in the Siebel server root directory.

NOTE: Field-level RC2 encryption is not supported for mobile Web clients or dedicated clients.

Every Siebel server in a deployment must use the same version of the keyfile. Inconsistent keyfiles may result in application errors. Make sure keyfiles are distributed to all machines when a new encryption key is added.

Changing the Keyfile Password

The keyfile is encrypted using an encryption key generated from a keyfile password. To prevent unauthorized access, you can change the keyfile password using the Key Database Manager utility. The keyfile will be re-encrypted using a new encryption key generated from the new keyfile password.

Before using RC2 encryption for the first time, you need to change the keyfile password because all versions of the Key Database Manager utility are shipped with the same default password. The default keyfile password is kdbpass. You should also consider changing the keyfile password regularly to make sure the file is secured.

CAUTION: You must back up the keyfile before making changes to it. If the keyfile is lost or damaged, it may not be possible to recover the encrypted data without a backup keyfile.

To change the keyfile password

- 1** Run the keydbmgr.exe utility from the bin subdirectory in the Siebel server root directory.

For information on running the keydbmgr.exe, see [“Running Key Database Manager” on page 57](#).

- 2** To change the keyfile password, enter 1.
- 3** Enter the new password.
- 4** Confirm the new password.
- 5** Quit the keydbmgr.exe utility.

When exiting the keydbmgr.exe utility, monitor any error messages that may be generated. If an error occurred, you may need to restore the backup version of the keyfile.

- 6** Distribute the new keyfile to all Siebel servers by copying the file to the admin subdirectory in the Siebel server root directory.

NOTE: Field-level RC2 encryption is not supported for mobile Web clients or dedicated clients.

Every Siebel server in a deployment must use the same version of the keyfile. Inconsistent keyfiles may result in application errors. Make sure keyfiles are distributed to all machines when a new encryption key is added.

Every Siebel server in a deployment must use the same version of the keyfile. Inconsistent keyfiles may result in application errors. Make sure keyfiles are distributed to all machines when any changes are made.

If You are Upgrading

The Siebel Strong Encryption Package upgrades Siebel applications from 56-bit encryption to 128-bit encryption. This package includes an upgrade utility (keydbupgrade.exe) that decrypts the key database (which was encrypted with the 56-bit key) and then encrypts the key database with a new 128-bit key.

Before you install the Strong Encryption Package:

- 1 Make a backup of your existing keyfile.
- 2 Run the keydbmgr.exe utility and change the keyfile password.

Unicode Support

Version 7.5 of Siebel applications includes Unicode support. For complete Unicode compliance, consider the following encryption and authentication issues.

Using non-ASCII characters in a Unicode environment

- For database authentication, the user ID and password must use characters that are supported by the Siebel database.
- Login problems may occur if you login to a Unicode Siebel site, then use Web Single Sign-On to access a third-party Web page that does not support Unicode. Make sure all applications accessible from Web Single Sign-On are Unicode-compliant.

Logging In to a Siebel Application

- If you use a form login mechanism for your Siebel applications, make sure that the characters used in the login form are supported by the Siebel database.
- If you use a URL login mechanism for your Siebel applications, the characters used in the login form must be in ASCII.

Encrypted data

If you use embedded data encryption to store sensitive information such as credit card numbers, make sure you use RC2 encryption (instead of Siebel standard encryption) for your Unicode site.

CAUTION: Using Siebel standard encryption in a Unicode environment can result in irrecoverable data loss.

To upgrade from standard encryption to RC2

- Use the Encryption Upgrade Utility provided by Siebel Systems to convert to RC2 encryption. For more information, follow the encryption upgrade procedures in the *Upgrade Guide*.
- Use Siebel Tools and reset the field user properties for the business component to RC2 encryption. For more information, see [“Business Component Encryption” on page 54](#).

This section presents information and instructions on setting up your authentication infrastructure. Its content includes:

- An overview of authentication strategies.
- A summary of centralized information locations: configuration parameters and seed data that you use throughout the section.
- A section about database authentication and its implementation.

Additional sections in this book are provided with information on:

- External authentication and security adapters.
- Two principle external authentication strategies, including a scenario in each that describes the setup of a specific authentication architecture.
- Instructions for implementing all available authentication options.
- Referential information about parameters that are provided to implement various authentication strategies and options.
- Login features and cookies.

To implement your authentication infrastructure, use these sections in the following way:

- If you are undecided about the basic authentication strategy to implement, read the general overview material and the overview material in the section for each authentication strategy.
- If you are unfamiliar with or undecided about the components and options to implement in your authentication architecture, read the descriptions of available options for security adapters, each authentication strategy, and, optionally, the section on implementing authentication options.

- Use the setup scenarios in the sections for each external authentication strategy as an aid to set up your own authentication architecture.
- When you set up your authentication strategy in a development environment, use the referential information about parameters and seed data as needed.

Referential and procedural information in each of the following topics relates to all three authentication strategies. Much of the specific information in these topics applies to more than one authentication strategy. Some of the information applies to both authentication and user administration.

- **Seed data.** When you install your Siebel eBusiness Applications, you are provided seed data that is related to authentication, to user registration, and to user access to Siebel applications. For detailed information on the seed data that is provided and for procedures for viewing and editing seed data, see [“Seed Data” on page 345](#).
- **Configuration parameters related to authentication.** Configuration parameter values determine how your authentication architecture components interact. For information about the purposes of configuration parameters and procedures for setting their values, see [“Configuration Parameters Related to Authentication” on page 161](#).
- **Authentication options.** Each authentication strategy has options in the way it can be implemented. For information about the authentication options and procedures for implementing them, see [“Authentication Options” on page 137](#).

About User Authentication

Authentication is the process of verifying the identity of a user. Siebel supports three approaches for authenticating users: database authentication, security adapter authentication, and Web SSO.

You must choose one of three fundamental authentication architectures for your Siebel application users:

- **Database authentication.** This approach relies on the underlying application database for user authentication.
- **Security adapter authentication.** Siebel applications support authentication to Microsoft Active Directory Server and LDAP-compliant directories using a Siebel-provided security adapter or a custom adapter you provide. In this architecture, the adapter authenticates users against the directory.
- **Web Single Sign-On (Web SSO).** This approach uses an external authentication service to authenticate users before they access the Siebel application. In this architecture, a Siebel-provided security adapter or a custom adapter you provide does not authenticate the user. The security adapter simply looks up and retrieves a user's Siebel user ID and database account from the directory based on the identity key that is accepted from the external authentication service.

User Authentication

About User Authentication

You may choose the approach for user authentication individually for each application in your environment based on the specific application requirements. However, there are administrative benefits to using a consistent approach across all of your Siebel applications because a consistent approach lowers the overall complexity of the deployment. [Table 3](#) highlights the capabilities of each authentication approach to help guide your decision.

Table 3. Comparison of Authentication Approaches

Desired Deployment or Functionality	Database	Security Adapter	Web SSO	Comments
Does not require additional infrastructure components.	X			
Centralizes storage of user credentials and roles.		X	X	
Limits number of database accounts on the application database.		X	X	
Supports dynamic user registration. Users are created in real-time through self-registration or administrative views.		X	(X)	For Web SSO, user registration is the responsibility of the third-party authentication architecture. It is not logically handled by the Siebel architecture.
Supports account policy. You can set policies such as password expiration, password syntax, and account lockout.		X	(X)	For Web SSO, account policy enforcement is handled by the third-party infrastructure.
Supports Web Single Sign-On, the capability to log in once and access all the applications within a Web site or portal.			X	

You have several options available for each of the basic strategies.

Siebel Authentication Manager

The authentication manager runs within the Siebel object manager. It is responsible for verifying credentials and establishing a connection to the application database. The three authentication approaches discussed in this section are invoked by configuring the authentication manager properly.

Figure 7 provides a high-level view of the logic that determines how user credentials are processed.

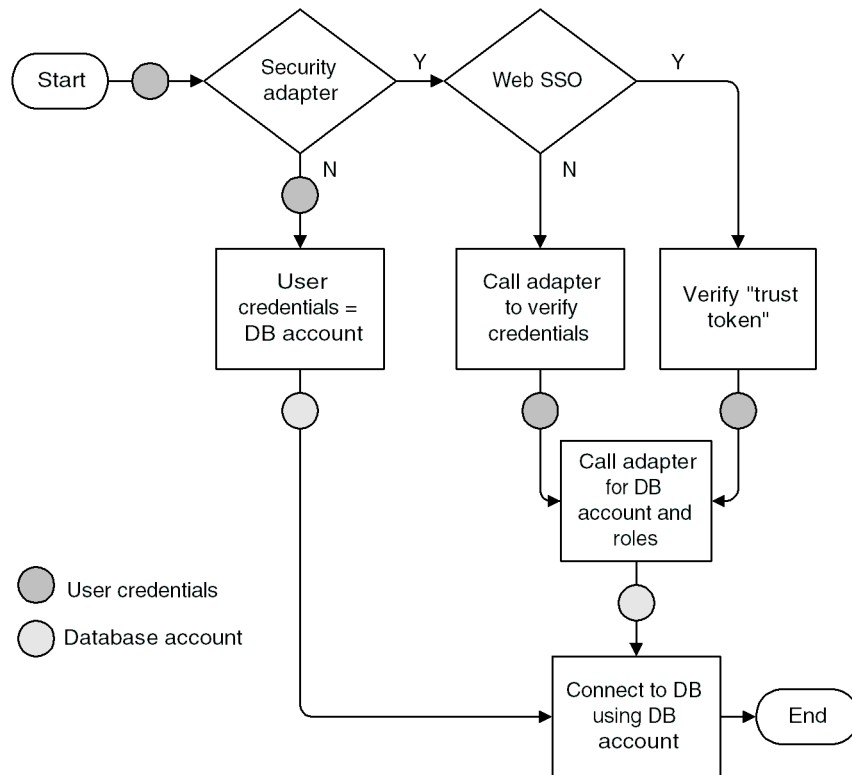


Figure 7. Siebel Authentication Manager Process

Authentication Manager Overview

The authentication manager receives user credentials from a source determined by the authentication strategy that is implemented. [Figure 7 on page 67](#) provides a high-level view of the logic that determines the way the authentication manager processes the user credentials it receives.

The authentication manager branches its processing of the identity key by evaluating conditions based on the values of these options:

- **No security adapter is identified.** The authentication manager concludes that database authentication is implemented and that the identity key is a set of credentials provided by the user. The authentication manager interprets the user credentials as a database account and passes them to the application object manager. The object manager opens a database connection using the account, and identifies the user by the account.
- **A security adapter is identified, but Web SSO is not specified.** The authentication manager concludes that external authentication by a security adapter is implemented and that the identity key is a set of credentials provided by the user. The authentication manager invokes the security adapter to authenticate the user credentials through the directory and to return a database account, a Siebel user ID, and possibly roles. The object manager opens a database connection using the account and identifies the user by the user ID.
- **A security adapter is identified, and Web SSO is specified.** The authentication manager concludes that Web SSO is implemented and that the user credentials identify a user who is preauthenticated by a third party. The authentication manager invokes the security adapter to verify that the credentials come from a trusted source and to return a database account, a Siebel user ID, and, possibly roles from the directory. The object manager opens a database connection using the database account and identifies the user by the Siebel user ID.

Authentication Manager Process Detail

[Figure 8 on page 69](#) presents the detailed logic of the process flow when the authentication manager is presented credentials and a request for access to a Siebel application.

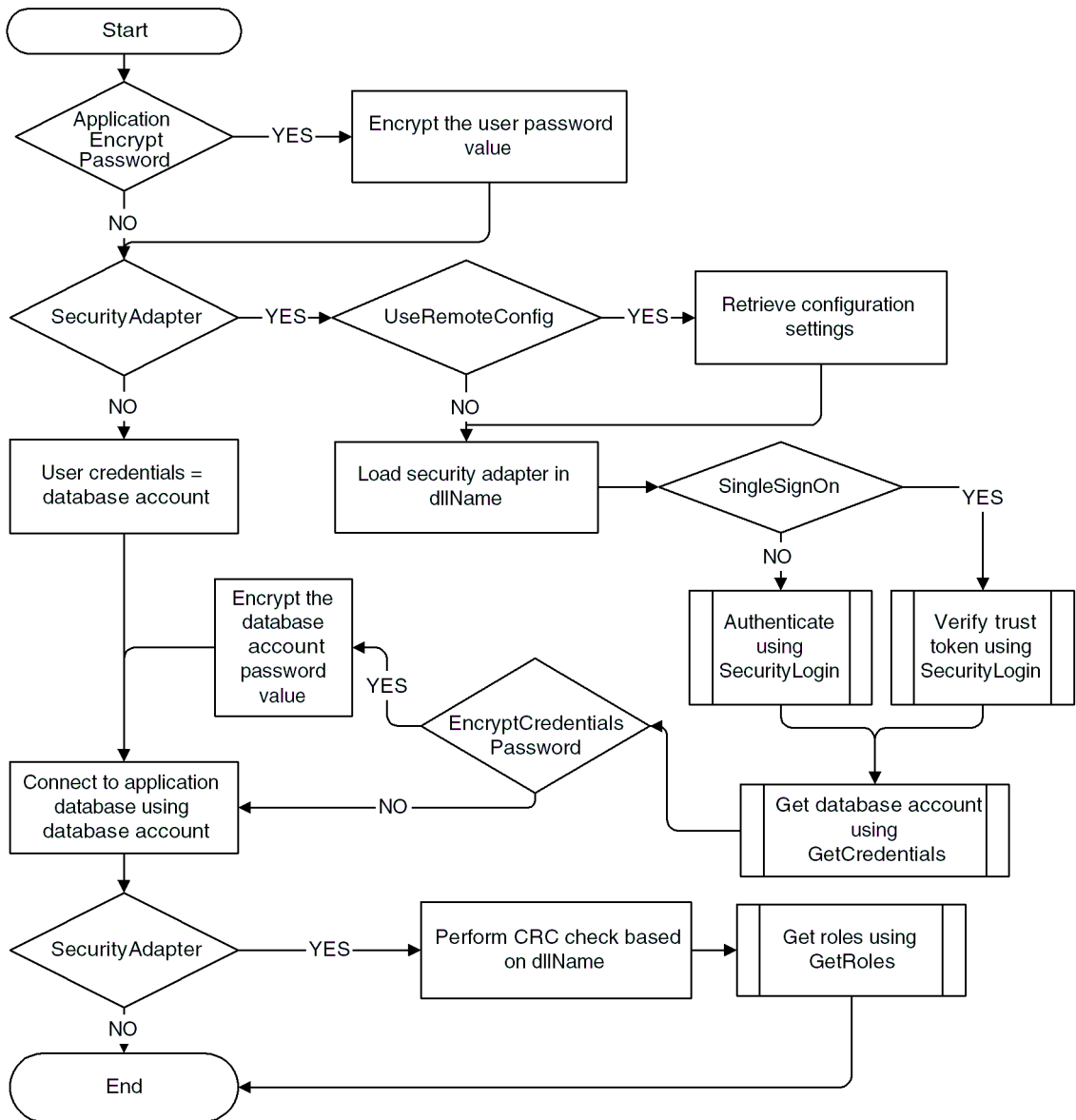


Figure 8. Authentication Manager Process Flow

Database Authentication Overview

If you do not use an external authentication system, then you must create a unique database account for each user. When an administrator adds a new user to the database, the User ID field must match the username for a database account. The user enters the database username and password when the user logs in to a Siebel application.

Figure 9 shows the authentication structure in an implementation using database authentication.

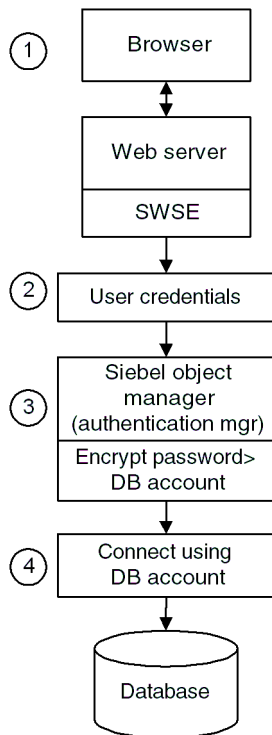


Figure 9. Database Authentication

The steps in a database authentication process are:

- 1** The user enters a database account's username and password to a Siebel application login form.
- 2** The Siebel Web Server Extension (SWSE) passes the user credentials to the authentication manager.
- 3** The authentication manager interprets the credentials and passes them to the Siebel application's object manager.
- 4** If the user credentials match a database account, the user is logged into the database and is identified with a particular user record whose user ID is the same as the database account's username.

Database authentication is the easiest to implement of the authentication approaches presented in this section.

Some of the features that other authentication strategies provide are not available with database authentication, including:

- Authentication that is independent of the database
- A single user authentication that is valid for Siebel applications and other applications on a Web site
- User self-registration
- External delegated administration of users
- Automated creation of users from the User Administration screen

Implementing Database Authentication

If you implement database authentication, it will typically be for a Siebel employee application, such as Siebel Call Center, MidMarket Edition or Siebel Sales, MidMarket Edition.

To allow database authentication to be implemented, you must make sure that the Security Adapter Name parameter at all applicable levels in the Siebel name server does not indicate that a security adapter is being used. For information about setting name server parameter values and the purposes of the parameters, see [“Siebel Name Server Parameters” on page 172](#).

An administrator must perform the following tasks to provide a new user with access to Siebel applications and the Siebel database in a database authentication environment:

- Create a database account for the user. Use your database management features to create a database account for each user.
- Create a record for the user in the Siebel database in which the user ID matches the user name for the database account.

The way you add a user to the database depends on the application to which you are granting the user access. In all cases you add users to the database through an employee application, such as Siebel Call Center.

For information about adding users to the database, see [“Internal Administration of Users” on page 224](#).

The following options are available if you implement database authentication:

- **User Password Encryption.** Maintains an unexposed, encrypted password to a database account, while an unencrypted version of the password is provided to the user for logging in.
- **Secure Login.** Transmits user credentials entered to a login form over Secure Socket Layer (SSL).

This section describes how to set up security adapter authentication for Siebel applications. It includes information on LDAP and ADSI security adapter authentication.

Siebel Security Adapters

A directory is a store in which the information that is required to allow users to connect to the database, such as database accounts and Siebel user IDs, is maintained external to the Siebel database.

The security adapter is a plug-in to the authentication manager. The security adapter uses the user credentials entered by a user or supplied by an authentication service to retrieve the Siebel user ID, a database account, and, optionally, a set of roles from the directory.

In general, Security Adapter authentication includes the following principal stages:

- The user provides identification credentials.
- The user's identity is verified.
- The user's Siebel user ID and database account are retrieved from a directory.
- The user is granted access to the Siebel application and the Siebel database.

When you install your Siebel eBusiness Applications, two security adapters are also installed, an Active Directory Services Interface (ADSI) adapter and a Lightweight Directory Access Protocol (LDAP) adapter.

For specific information about third-party directory servers supported by Siebel security adapters, see the system requirements and supported platforms documentation for your Siebel application.

You can implement a security adapter other than the Siebel LDAP adapter or ADSI adapter. To support the functionality described in this section for the Siebel adapters, the adapter you implement must support the *Siebel Security Adapter Software Developers Kit 7* on the Siebel SupportWeb site.

Depending on how you configure your authentication architecture, the security adapter may function in one of the following modes:

- **With authentication (LDAP or ADSI security adapter authentication mode).** The adapter uses credentials entered by the user to verify the user's existence in the directory. If the user exists, the adapter retrieves the user's Siebel user ID, a database account, and, optionally, a set of roles which are passed to the application's object manager to grant the user access to the Siebel application and the database. This adapter functionality is typical in a security adapter authentication implementation.
- **Without authentication (Web SSO mode).** The adapter passes an identity key supplied by a separate authentication service to the directory. Using the identity key to identify the user in the directory, the adapter retrieves the user's Siebel user ID, a database account, and, optionally, a set of roles that are passed to the application's object manager to grant the user access to the Siebel application and the database. This adapter functionality is typical in a Web SSO implementation.

NOTE: To protect against Web Server spoofing attacks, the security adapter verifies the Web engine's trust token before authentication takes place.

In a security adapter authentication environment, a Siebel-compliant security adapter also provides the function of creating a record in the directory when the user is created in the Siebel database.

Directory Requirements

You must provide your directory, whether it is one of the servers supported by Siebel security adapters or another directory of your choice. If you provide one of the Siebel-supported servers, you may use a Siebel-compliant security adapter or another adapter of your choice. If you provide a directory other than those supported by the Siebel security adapters, then you are responsible for supporting the directory with the security adapter you implement.

For specific information about third-party products supported by Siebel eBusiness Applications, see the system requirements and supported platforms documentation for your Siebel application.

Your directory must store, at a minimum, the following data for each user: (Each piece of data is contained in an attribute of the directory.)

- **Siebel user ID.** This attribute value must match the value in the user ID field for the user's Person record in the Siebel database. It is used to identify the user's database record for access control purposes.
- **Database account.** This attribute value must be of the form `username=U password=P type=T`, where *U* and *P* are credentials for a database account. The type value *T* is the name of a data source, such as `server` or `sample`, and is case-insensitive. There may also be a single credential of the form `username=U password=P`. This default credential is used when a user tries to connect to a data source for which no credential has a matching type value. There may be any amount of white space between the two `key=value` pairs and no space within each pair. The keywords `username`, `password`, and `type` must be lowercase.
- **Username.** This attribute value is the key passed to the directory which identifies the user. In a simple implementation, it may be the Siebel user ID, and so it may not need to be a separate attribute.

- **Password.** The storage of a user's login password differs between LDAP servers and Active Directory Server (ADS).
- **LDAP.** If the user authenticates through the directory, such as in a security adapter authentication implementation, then the login password must be stored in an attribute. If the user is authenticated by an external authentication service, as might be the case in a Web SSO implementation, a password attribute is not required.
- **ADS.** ADS does not store the password as an attribute. The password can be entered at the directory level as a function of the client, or the Siebel ADSI security adapter can use ADS methods to create or modify a password. If the user authenticates through the directory, such as in a security adapter authentication implementation, then the login password must be stored. If the user is authenticated by an external authentication service, as might be the case in a Web SSO implementation, a password is not required.

You can use other user attributes to store whatever data you want, such as first and last name. Authentication options that you choose may require that you commit additional attributes.

An additional piece of information, *roles*, is supported by Siebel object managers, but is not required. Roles are an alternate means of associating Siebel responsibilities with users. Responsibilities are typically associated with users in the Siebel database, but they can instead be stored in the directory. Leave role values empty to administer responsibilities from within Siebel applications. For information about roles, see [“Roles” on page 137](#).

CAUTION: Do not confuse roles defined by an LDAP or ADS directory with roles defined in the Siebel application interface. Roles in LDAP or ADS directories are collections of responsibilities that strictly enforce access to views and data records within Siebel applications. Roles defined in the application interface allow application administrators to increase the usability and deployability of the application by tailoring the product to groups of users. For more information about roles defined in an application interface, see [“Creating and Administering Roles” on page 322](#).

User Privileges

Depending on your authentication and registration strategies and the options that you implement within your strategy, you must define users in the directory that read and may possibly write user information in the directory. It is critical that users who read or write data in the directory have appropriate search and write privileges to the directory. Depending on your authentication and registration strategies, these users may include:

- The application user. If you implement the application user, then the application user is the only user that must be able to search and write records to the directory.

For information about the application user, see [“Application User” on page 145](#).

- The anonymous user. If you do not implement an application user and you allow user self-registration, then the anonymous user must have search and write privileges to the directory.

NOTE: User self-registration is not available for all Siebel applications.

For information about the anonymous user, see [“Anonymous User” on page 158](#).

For information about user self-registration, see [“Implementing Self-Registration” on page 190](#).

- The internal administrators and delegated administrators. If you do not implement an application user, then each user who creates or modifies other users must have search and write privileges to the directory. Internal administrators and delegated administrators may be included in this group.

For information about internal and external registration of users, see [“Internal Administration of Users” on page 224](#) and [“External Administration of Users” on page 236](#).

ADSI Adapter Requirements

If you are running the Siebel Object Manager on Windows NT, you must confirm that an ADSI client, supported by the Siebel ADSI adapter, is installed. If a supported client is not installed, then you must manually install one.

For information about ADSI client versions supported by Siebel security adapters, see the system requirements and supported platforms documentation for your Siebel application.

To confirm successful installation of a Siebel-supported ADSI client

- 1** Navigate to the system32 subdirectory of the installation location for the operating system (usually C:\WINNT).
- 2** Verify that all of the DLLs for the supported ADSI clients listed in the system requirements, and the supported platforms documentation for your Siebel application, are present in the subdirectory.

For example, Windows 2000 requires the adsiis.dll and the adsiisex.dll.

- 3** For each DLL, right click on the file and choose Properties.
- 4** Click the Version tab to see the version number.

NOTE: To perform user management in the ADS directory through the Siebel client, it is strongly recommended that you configure ADS at the server level for SSL communications between the Active Directory client and server. This is different from SSL communications between the security adapter and the directory, which is configured through Siebel applications and is discussed in [“Secure Adapter Communications” on page 152](#).

Siebel Security Adapters and the Siebel Dedicated Web Client

The Siebel Dedicated Web Client relocates business logic from the Siebel server to the client. The authentication architecture for the Siebel Dedicated Web Client differs from the authentication architecture for the standard Web client because it locates the following components on the client instead of a Siebel server:

- Application object managers
- Application configuration files
- Authentication manager

When you configure a particular application to implement external authentication, you must observe the following principles to include Siebel Dedicated Web Clients:

- It is strongly recommended that you use the remote configuration option so that all clients use the same configuration settings. Alternatively, make sure that authentication parameters in the application configuration files on client machines contain the same values as the corresponding application configuration files on the Siebel servers. Distribute appropriate configuration files to Siebel Dedicated Web Client users.

For information about setting parameters in Siebel application configuration files on both the Siebel server and on the Siebel Dedicated Web Client, see [“Siebel Application Configuration File Parameters” on page 164](#).

For information about remote configuration, see [“Remote Configuration” on page 150](#).

- It is strongly recommended that you use checksum validation to make sure that the appropriate security adapter provides user credentials to the authentication manager for all users who request access.

For information about checksum validation, see [“Checksum Validation” on page 149](#).

- In a security adapter authentication implementation, you must set Siebel system preferences if you want to implement:
 - Security adapter authentication of Siebel Dedicated Web Client users
 - Propagation of user data from the Siebel Dedicated Web Client to the directory

For information about setting authentication-related Siebel system preferences, see [“System Preferences” on page 175](#).

For more information about the Siebel Dedicated Web Client, see *Siebel Web Client Administration Guide, MidMarket Edition*.

Security Adapter Deployment Options

This section describes security adapter options that can be implemented in a security adapter authentication environment or in a Web SSO environment. Unless noted otherwise, these options are supported by the Siebel LDAP and ADSI adapters and by adapters that comply with *Siebel Security Adapter Software Developers Kit 7*.

- **Remote configuration.** The configuration parameters for a security adapter are stored in a centralized file that can be accessed on the network.
- **Checksum validation.** Verifies that the security adapter loaded by the authentication manager is the correct version.
- **User Password Encryption.** Maintains an unexposed, encrypted password in the directory, while an unencrypted version of the password is provided to the user for logging in.
- **Credentials password encryption.** The password set for the database account is encrypted, while an unencrypted version is stored in the directory and is used elsewhere in the authentication process.
- **Application user.** A designated entry in the directory is the only user with search and write privileges to the directory.
- **Application User Password Encryption.** You can maintain an unexposed password for the application user in the directory, while an encrypted version of the password is used in other phases of the authentication process.

Additionally, you can choose to store users' Siebel responsibilities as roles in a directory attribute instead of in the Siebel database.

For information about the authentication options and procedures for implementing them, see [“Authentication Options” on page 137](#).

LDAP and ADSI Security Adapter Authentication

Siebel eBusiness Applications includes security adapters that are based on the LDAP and ADSI standards, allowing customers to use LDAP directories or Microsoft Active Directory for user authentication.

In an implementation using Siebel LDAP or ADSI security adapter authentication, a Siebel security adapter or a Siebel-compliant adapter authenticates a user's credentials against the directory and retrieves login credentials from the directory. The security adapter functions as the authentication service in this architecture.

Security adapter authentication provides a user with access to a single Siebel application only. The authentication does not serve for other applications on the Web Site.

Figure 10 shows a security adapter authentication architecture.

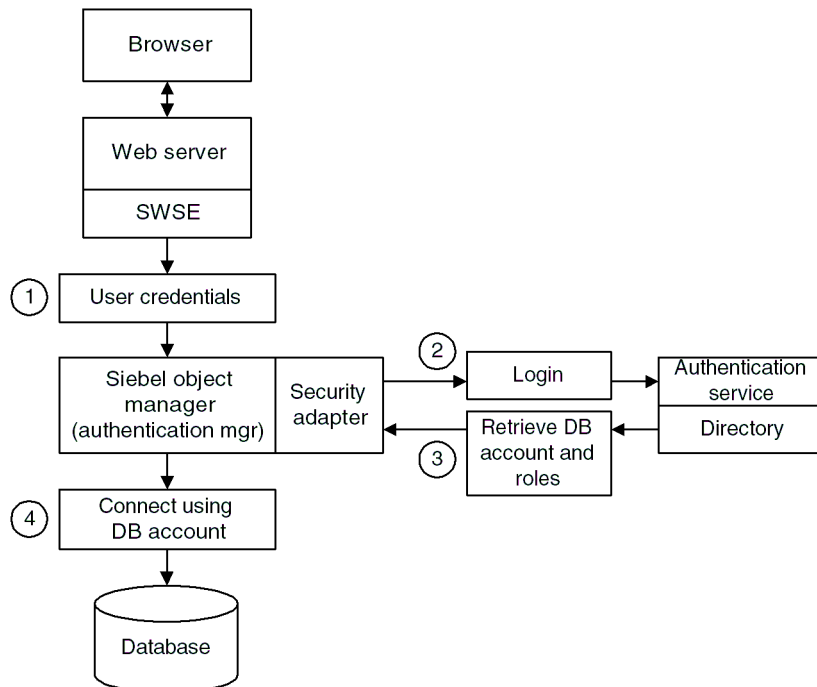


Figure 10. Security Adapter Authentication

The steps in the security adapter authentication process are:

- 1** The user enters credentials to a Siebel application login form. These user credentials (a username and password) can vary depending on the way you configure the security adapter. For example, the username could be the Siebel user ID or an identifier such as an account or telephone number. The user credentials pass to the Siebel Web Server Extension (SWSE) and then to the authentication manager, a component of the Siebel Object Manager.
- 2** The authentication manager determines how to process the user credentials and calls the security adapter to provide authentication against the directory.
- 3** The security adapter returns the Siebel user ID and a database account to the authentication manager. (If roles are used, they are also returned to the authentication manager.)
- 4** The object manager uses the returned credentials to connect the user to the database and to identify the user.

Security adapter authentication can offer the following benefits:

- Automatic updating of the directory with new or modified user information entered through the Siebel application interface by an internal administrator, a delegated administrator, or a self-registering user
- User self-registration
- Registration of users by delegated administrators through the Web site
- User authentication external to the database

Security adapter authentication does not provide for Web SSO. Web SSO is the capability for a user's authentication on your Web site to serve for access to other applications on the Web site, including Siebel applications.

Implementing LDAP and ADSI Security Adapter Authentication

You can set up your authentication architecture to authenticate a user for access to a single Siebel application when the user does either of the following:

- Attempts to access a protected view (one specified for explicit login), such as a checkout view in Siebel eSales, MidMarket Edition
- Logs in while on an unprotected view, such as a Siebel application's home page

CAUTION: For a particular Siebel application, you must use the same authentication method for mobile users connecting to the server that you use for other Web client users. That is, database authentication must be implemented for all users of the application or one of the external authentication strategies must be implemented for all users of the application. Because most mobile users are employees, this applies mainly to Siebel employee applications such as Siebel Call Center.

To provide user access to a Siebel application on a Web site implementing security adapter authentication, the Siebel application must be able to extract the following from the directory:

- Credentials to access the database
- The user's Siebel user ID

Task Overview

You must do the following tasks to set up a typical security adapter authentication architecture:

- Set up a directory from which a database account and a Siebel user ID can be retrieved for each user.
- Set up a security adapter as a plug-in to the Siebel application's object manager.
- Edit the eapps.cfg file to provide authentication parameter values.
- Edit the configuration file for each application's object manager to provide authentication parameter values.
- Edit authentication-related parameters in the Siebel name server.

- Set authentication-related system preferences.
- Restart the Siebel server and the Web server.

NOTE: Siebel provides an LDAP/ADSI Configuration Utility to help you configure a directory service for your Siebel applications. For more information, see [“Using the LDAP/ADSI Configuration Utility” on page 129](#).

Siebel Security Adapter Authentication and the Siebel Dedicated Web Client

In a Siebel LDAP or ADSI security adapter authentication implementation, you must set Siebel system preferences to provide the following capabilities:

- Security adapter authentication of Siebel Dedicated Web Client users
- Propagation of user data from the Siebel Dedicated Web Client to the directory

For information about setting authentication-related Siebel system preferences, see [“System Preferences” on page 175](#).

Deployment Options for Siebel LDAP and ADSI Security Adapter Authentication

This section describes options that you can implement in a security adapter authentication environment that uses the Siebel LDAP or ADSI adapter only.

In addition to the options described here, you can also implement any of the options that are described in [“Security Adapter Deployment Options” on page 80](#).

- **Adapter-defined user name.** You can configure a Siebel application so that the username presented by the user is a value other than the Siebel user ID; for example, a Social Security number. The security adapter returns the Siebel user ID of the authenticated user and a database account from the directory to the authentication manager.
- **Shared database account.** A designated entry in the directory contains a database account that is shared by other users.

- **Secure adapter communications.** You can use a secure socket layer (SSL) to transmit data between a Siebel LDAP or ADSI security adapter and the directory.
- **Secure Login.** Transmit user credentials entered to a login form over secure socket layer (SSL).

For information about authentication options and procedures for implementing them, see [“Authentication Options” on page 137](#).

Setting Up Security Adapter Authentication: A Scenario

This section provides instructions to implement security adapter authentication for a single Siebel application. The implementation uses either the Siebel LDAP adapter or the Siebel ADSI adapter with one of the supported directories described in the system requirements and supported platforms documentation for your Siebel application.

Your implementation may include more than one Siebel application, and you may implement components and options that are not included here.

These instructions are intended to allow you to confirm successful implementation of the security adapter with the directory. You should implement this architecture in a development environment before deploying it in a production environment. You can repeat the appropriate instructions here to provide security adapter authentication for additional Siebel applications.

These instructions implement the following basic configuration:

- The directory is a Siebel-supported LDAP server or Active Directory Server (ADS).
- The Siebel LDAP adapter or ADSI adapter is used to communicate between the authentication manager and the directory.
- A user is authenticated by the user’s Siebel user ID and a password.

To implement authentication options not included in this implementation, see [“Authentication Options” on page 137](#).

For information about special considerations to implementing user authentication, see [“User Authentication Issues” on page 335](#).

If you use a non-Siebel security adapter, it must support the *Siebel Security Adapter Software Developers Kit 7* on the Siebel SupportWeb site. You must adapt the applicable parts of the following implementation to your security adapter.

The following installations must be completed before you set up this security adapter authentication environment.

- Your Web server is installed.
- Your directory is installed.
- Your Siebel applications are installed, including the Siebel Gateway Server and the Siebel server.
- A URL or hyperlink is available with which users can access the login form for the Siebel application you are configuring.

These instructions assume that you are experienced with administering the directory. That is, you can perform tasks such as creating and modifying user storage subdirectories, creating attributes, creating users, and providing privileges to users.

You must perform the following process to implement and test your directory with a Siebel security adapter.

- Create a database login.
- Set up the attributes for users in the directory.
- Create three users in the directory: a regular user, the anonymous user, and the application user.
- Add user records in the Siebel database corresponding to two users in the directory.
- Edit eapps.cfg file parameters.
- Edit the Siebel application's configuration file parameters.
- Edit the name server parameters.
- Set system preferences.

- Restart the Siebel server and the Web server.
- Test the implementation.

Creating a Database Login

One database login must exist for all users who are authenticated externally. This login must not be assigned to any real person. A seed database login is provided for this purpose when you install your Siebel eBusiness Applications, as described in [“Seed Data” on page 345](#). Its login name is `LDAPUSER`, and its default password, `LDAPUSER`, should be changed by an administrator. If this login is not present, create it.

Setting Up the Directory

For purposes of testing the security adapter, this test implementation:

- Authenticates users through the directory.
- Allows self-registration.
- Uses the Siebel User Id as the username.

Determine the base DN, a subdirectory in the directory, to store users. You cannot distribute the users of a single Siebel application in more than one base DN. However, you may store multiple Siebel applications’ users in one base DN. For this example, users are stored in the People base DN under the domain level in the sample LDAP directories, or in the Users base DN under the domain level in the sample ADS directory.

Define the attributes to use for the following user data. Create new attributes if you do not want to use existing attributes. For this example, attributes are suggested. Some of the suggested attributes are default attributes in one or more of the supported directories.

- Data: Siebel user ID. Suggested attribute: `uid` for LDAP or `sAMAccountName` for ADS.
- Data: Database account. Suggested attribute: `dbaccount`.
- Data: Password. Suggested attribute for LDAP only: `userPassword`. ADS does not use an attribute to store a user’s password.

Optionally, use other attributes to represent first name, surname, or other user data.

NOTE: To perform user management in the ADS directory through the Siebel client, it is strongly recommended that you configure ADS at the server level for SSL communications between the Active Directory client and server. This is different from SSL communications between the security adapter and the directory, which is configured through Siebel applications and is discussed in [“Secure Adapter Communications” on page 152](#).

Creating Users in the Directory

Create three users in the directory as described in [Table 4 on page 89](#). The attribute names, such as uid and userPassword in an LDAP directory, are those suggested in this example. Your entries may vary depending on the way that you make attribute assignments in [“Setting Up the Directory” on page 87](#).

The uid or sAMAccountName entries for the application user and test user and the password entry for the test user are only suggested. You may vary those entries.

This example implements a shared credential. The database account for all users is stored in one object in the directory. In this example, the shared database account is stored in the anonymous user record. The database account must match the database account you reserve for externally-authenticated users described in [“Creating a Database Login” on page 87](#). The P symbol represents the password in that database account.

NOTE: In a production environment, do not use the anonymous user as the directory object that contains the shared credential.

For information about formatting requirements for the database account attribute entry, see [“Directory Requirements” on page 75](#).

CAUTION: Make sure the anonymous user and the application user have write privileges to the directory. (The anonymous user must have write privileges because it is a component of self-registration.) In addition, the application user must have privileges to search all user records.

Table 4. Directory Records

Type of User	Siebel User ID Attribute (Uid for LDAP or sAMAccountName for ADSI)	Password (UserPassword Attribute for LDAP or ADS Password for ADSI)	Database Account Attribute (Dbaccount)
Anonymous user	<p>Enter the user ID of the anonymous user record for the Siebel application you are implementing.</p> <ul style="list-style-type: none"> ■ You can use a seed data anonymous user record for a Siebel customer or partner application. For example, if you implement Siebel eService, MidMarket Edition, enter GUESTCST. ■ You can create a new user record or adapt a seed anonymous user record for a Siebel employee application. ■ The anonymous user is required even if the application does not allow access by unregistered users. For more information, see “Anonymous User” on page 158. 	GUESTPW or a password of your choice	username = LDAPUSER password = P
Application user	APPUSER or a name of your choice	APPUSERPW or a password of your choice	Database account is not required for the application user.
A test user	TESTUSER or a name of your choice	TESTPW or a password of your choice	Database account is not required for any user record, except the anonymous user.

Optionally, complete other attribute entries for each user.

Adding User Records in the Siebel Database

You must create a record in the Siebel database that corresponds to the test user you create in [“Creating Users in the Directory” on page 88](#).

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in [Table 22 on page 347](#). This record must also match the anonymous user you created in [“Creating Users in the Directory” on page 88](#).

You can adapt a seed data anonymous user or create a new anonymous user for a Siebel employee application. To adapt a seed anonymous user for a Siebel employee application, add any views to the anonymous user’s responsibility that would be required for the employee application, such as a home page view in which a login form is embedded.

For purposes of confirming connectivity to the database, you can use the following procedure to add the test user for any Siebel application. However, if you are configuring a Siebel employee or partner application, and you want the user to be an employee or partner user, complete with position, division, and organization, see the instructions for adding such users in [“Internal Administration of Users” on page 224](#).

To add user records to the database

- 1** Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
- 2** From the application-level menu, choose View > Site Map > User Administration > Users.

The All Users list appears.
- 3** In the All Users list, click the menu button and choose New Record.

A new All Users form appears.

- 4 Use the following guidelines to complete the field entries for the test user, and then click Save. Suggested entries are for this example. You can complete other fields, but they are not required.

Field	Suggested Entry	Guideline
Last Name		Required. Enter any name.
First Name		Required. Enter any name.
User ID	TESTUSER	Required. This entry must match the uid (LDAP) or sAMAccountName (ADS) attribute value for the test user in the directory. If you used another attribute, it must match that value.
Responsibility		Required. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. If an appropriate seed responsibility does not exist, such as for a Siebel employee application, assign an appropriate responsibility that you create.
New Responsibility		Optional. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. This responsibility is automatically assigned to new users created by this test user.

- 5 Verify that the seed data User record exists for anonymous users of the Siebel application you implement, as described in [Table 22 on page 347](#). For example, verify that the seed data User record with user ID GUESTCST exists if you are implementing Siebel eService. If the record is not present, create it using the field values in [Table 22 on page 347](#). You can complete other fields, but they are not required.

Editing the Eapps.cfg Parameters

Provide the parameter values in the eapps.cfg file as indicated by the guidelines in [Table 5](#).

For information about editing eapps.cfg parameters and about the purposes for the parameters, see “[Eapps.cfg Parameters](#)” on page 162.

Table 5. Eapps.cfg Parameter Values

Section	Parameter	Suggested Entry	Guideline
[defaults]	SingleSignOn TrustToken UserSpec UserSpecSource		If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.
The section particular to your application, such as [/eservice], [/echannel], or [/callcenter]	AnonUserName		Enter the user ID of the seed data User record provided for the application that you implement or of the User record you create for the anonymous user. This entry also matches the uid (LDAP) or SAMAccountName (ADS) entry for the anonymous user record in the directory. For example, enter GUESTCST for Siebel eService.
	AnonPassword		Enter the password you created in the directory for the anonymous user.
	AnonUserPool	100, or another positive number	
	SingleSignOn TrustToken UserSpec UserSpecSource ProtectedVirtualDirectory		If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Editing the Siebel Application's Configuration File Parameters

Provide the parameter values as indicated by the guidelines in [Table 6](#) in the configuration file for the Siebel application you are implementing. (For a list of Siebel application configuration files, see [“Siebel Application Configuration File Names” on page 343](#).)

NOTE: You can use a text editor to make changes to an application configuration file or you can use the LDAP/ADSI Configuration Utility to make these changes. For more information on using the Configuration Utility see [“Using the LDAP/ADSI Configuration Utility” on page 129](#).

For information about editing an application's configuration file and about the purposes for the parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

Table 6. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
[SWE]	AllowAnonUsers	Enter TRUE for LDAP and ADSI.
	SecureLogin	Enter TRUE or FALSE. If TRUE, the login request (HTTP POST) from the login form is transmitted using HTTPS. For information about other requirements for secure login, see “Secure Login” on page 139 .
[SecurityAdapters]	Add a line for each security adapter you may implement; most likely there is only one.	<ul style="list-style-type: none"> ■ LDAP suggested entry is LDAP. ■ ADSI suggested entry is ADSI.
The section for the particular security adapter you implement, for example [LDAP] or [ADSI]	DllName	<ul style="list-style-type: none"> ■ For LDAP, enter <code>sscfldap.dll</code> ■ For ADSI, enter <code>sscfadsi.dll</code>

Table 6. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
	ServerName	LDAP and ADS, enter the name of the machine on which the LDAP or ADS server runs.
	Port	<ul style="list-style-type: none"> ■ The LDAP suggested entry is 389. Typically, use port 389 for standard transmission or port 636 for secure transmission. ■ For ADSI, you set the port at the ADS directory level, not as a configuration parameter. If this parameter is present, comment it out, or you can delete the line from the file.
	BaseDN	<p>The Base Distinguished Name is the root of the tree under which users are stored. Users can be added directly or indirectly below this directory.</p> <ul style="list-style-type: none"> ■ LDAP suggested entry (including quotes): <code>"ou=People, o = domain name"</code> <p>In the example, "o" denotes "organization" and is the domain name system (DNS) name for this server, such as <code>machine.company.com</code>. "ou" denotes "organization unit" and is the subdirectory in which users are stored.</p> <ul style="list-style-type: none"> ■ ADSI suggested entry (including quotes): <code>"CN=Users,DC=machine,DC=domain,DC=com"</code> <p>Domain Controller (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for the user objects in the directory. Therefore, adjust the number of CN and DC entries to represent your architecture.</p>

Table 6. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
	UserNameAttributeType	<ul style="list-style-type: none"> ■ The LDAP suggested entry is <code>uid</code> ■ The ADSI suggested entry is <code>sAMAccountName</code> <p>If you use a different attribute in the directory for the Siebel user ID, enter that attribute name.</p>
	PasswordAttributeType	<ul style="list-style-type: none"> ■ The LDAP suggested entry is <code>userPassword</code> <p>If you use a different attribute in the directory for the login password, enter that attribute name.</p> <ul style="list-style-type: none"> ■ ADS does not store the password in an attribute. If this parameter is present, comment it out, or you can delete the line from the file.
	CredentialsAttributeType	<p>The LDAP and ADSI suggested entry is <code>dbaccount</code></p> <p>If you used a different attribute in the directory for the database account, enter that attribute name.</p>
	ApplicationUser	<ul style="list-style-type: none"> ■ LDAP suggested entry (including quotes): <code>"uid=APPUSER, ou=People, o=domain name"</code> ■ ADSI suggested entry (including quotes): <code>"CN=APPUSER, CN=Users, DC=machine, DC=domain, DC=com"</code> <p>Adjust your entry if your implementation uses a different attribute for the user name, a different user name for the application user, or a different base DN.</p>
	ApplicationPassword	<p>For LDAP and ADSI, enter <code>APPUSERPW</code> or the password you assigned to the application user.</p>

Table 6. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
	SharedCredentialsDN	<ul style="list-style-type: none"> ■ LDAP suggested entry (including quotes): <code>"uid=<i>anonymous user User ID</i>,ou=People, o = <i>domain name</i>"</code> For example: <code>"uid=GUESTCST, ou = People, o=siebel.com"</code> ■ ADSI suggested entry (including quotes): <code>"CN=<i>anonymous user User ID</i>,CN=Users,DC=<i>machine</i>,DC=<i>domain</i>,DC=com"</code> For example: <code>"CN=GUESTCST, CN=Users,DC=<i>gal</i>,DC=siebel,DC=com"</code>
	RolesAttributeType SslDatabase UseSSL EncryptCredentialsPassword EncryptApplicationPassword SingleSignOn TrustToken UseAdapterUsername SiebelUsernameAttributeType UseRemoteConfig	If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Editing the Name Server Parameters

Set each name server parameter listed in [Table 7](#) for the component that corresponds to the object manager for the application you are implementing, such as Call Center Object Manager or eService Object Manager. Set the parameters at the component level and follow the guidelines provided in the table.

For information about setting name server parameters, see [“Siebel Name Server Parameters” on page 172](#).

Table 7. Siebel Name Server Parameters

Subsystem	Parameter	Guideline
Object Manager	OM - Configuration File	Name of configuration file for the application you implement, such as <code>eservice.cfg</code> .
	OM - Data Source	Enter the data source for the server on which this Siebel application runs, such as <code>ServerDataSrc</code> .
	OM - Proxy Employee	Enter <code>PROXYE</code> .
	Security Adapter Name	The name of the security adapter you implement as it appears in the <code>[SecurityAdapters]</code> section in the application configuration file; for example, <code>LDAP</code> or <code>ADSI</code> .
	OM - Username BC Field	Leave empty.
Infrastructure Objmgr configu	Application Encrypt Password	Enter <code>FALSE</code> .

Setting System Preferences

Set each system preference using the guidelines in [Table 8](#).

For information about setting system preferences, see “[System Preferences](#)” on [page 175](#).

Table 8. System Preferences

System Preference	Suggested Entry	Guideline
SecExternalUserAdministration	Enter FALSE.	An entry of FALSE allows administration of the directory through the Siebel application.
SecThickClientExtAuthent	Enter FALSE.	You set this parameter to TRUE to allow dedicated clients to use a security adapter.
Security Adapter CRC		Calculate the checksum value for your security adapter DLL as described in “ Checksum Validation ” on page 149 . Enter the calculated value here.

Restarting Servers

You must stop and restart the following Windows NT services on the Web server machine to activate changes you make to Siebel Object Manager configuration files.

- Stop the IIS Admin service, and then restart the Worldwide Web Publishing Service. The IIS Admin service also starts because the Worldwide Web Publishing Service is a subservice of the IIS Admin service.
- Siebel server. Choose Start > Settings > Control Panel, and then double-click Services to administer the services.

Testing the External Authentication System

The following tests confirm that the Siebel security adapter, your directory, and the Siebel application you are implementing work together to:

- Provide a Web page on which the user can log in.
- Allow an authenticated user to log in.
- Allow a user to browse anonymously, if applicable to your Siebel application.
- Allow a user to self-register, if applicable to your Siebel application.

To test your external authentication system

- 1 On a Web browser, enter the URL to your Siebel application, such as <http://www.mycompany.com/eservice>.

A Web page with a login form should appear, confirming that the anonymous user can successfully access the login page.

The following figure shows the login form for Siebel eService. It includes user ID and password fields and screen tabs for anonymous browsing.



- 2** If you see screen tabs, such as the ones shown for Siebel eService, click on various tabs to access screens intended for anonymous browsing. Employee applications, such as Siebel Call Center, typically do not allow anonymous browsing, while most other Siebel applications do.
- 3** Navigate back to the Web page that contains the login text boxes, and then log in with the user ID and the password for the test user you created. Enter `TESTUSER` or the user ID you created and `TESTPW` or the password you created.

More screen tabs should appear, indicating that the test user is authenticated successfully and the user record in the database is providing views through the expanded responsibility of this registered user.
- 4** Click Logout.
- 5** Repeat [Step 1 on page 99](#) to access the login page again. If a New User button is present, click it. If a New User button is not present, your Siebel application, without additional configuration, does not allow users to self-register.

The Personal Information form appears.

- 6** Complete the required fields on the Personal Information form, and then submit the form. You can complete other fields, but they are not required.

Field	Description
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous login name.
Password	Required. Enter a simple contiguous login password and record it.
Verify Password	Required.
Challenge Question	Required. Enter a phrase for which there is an “answer.” If you later click <i>Forgot Your Password?</i> , this phrase is displayed, and you must enter the correct answer to receive a new password.
Answer to Challenge Question	Required. Enter a word or phrase that is considered the correct answer to the challenge question.

- 7** Navigate to the page containing the login text fields.
- 8** Login using the user ID and password you created in [Step 6](#).

You should log in successfully and be able to navigate in screens provided for registered users.

Security Adapter Authentication

Implementing LDAP and ADSI Security Adapter Authentication

Web Single Sign-On and Remote Authentication

7

This section describes how to implement Web SSO for user authentication. It also provides a brief overview to remote authentication and describes the processing steps that occur to authenticate a remote user during synchronization.

Web SSO

In a Web SSO implementation, users are authenticated by a third party at the Web site level. Siebel applications support this mode of authentication by providing an interface that allows the third party to pass user information to a Siebel application. Once authenticated by the third party, a user does not have to explicitly log in to the Siebel application. Web SSO allows you to deploy Siebel applications into existing Web sites or portals.

Web SSO architecture is appropriate for Web sites on which only approved registered users can gain access to sensitive data, such as a Web site on which you share data with your channel partners.

Figure 11 shows an example of authentication architecture for Web SSO.

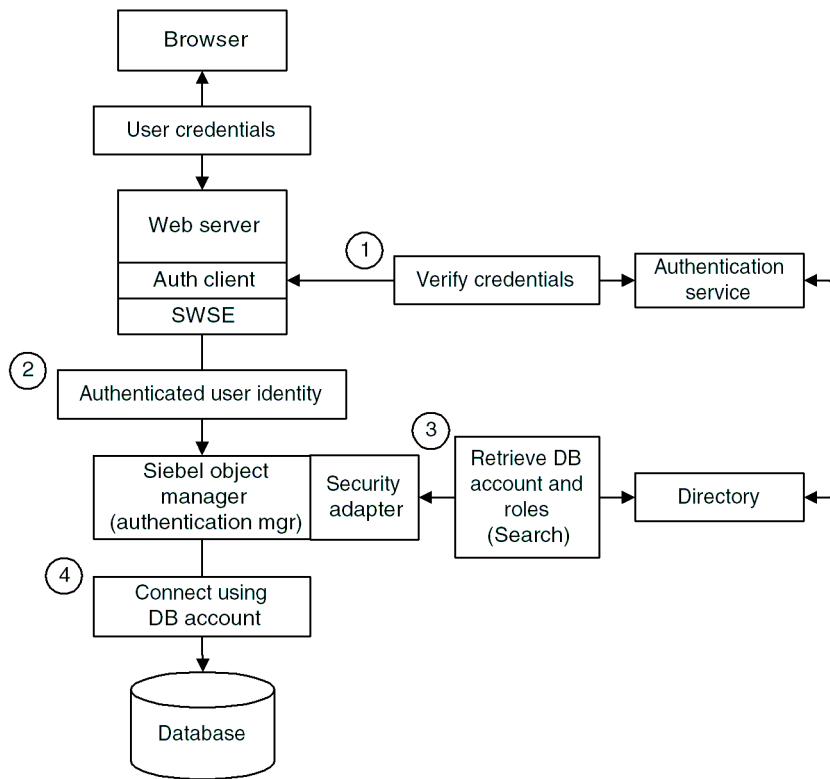


Figure 11. Web SSO Authentication

The steps in Web SSO authentication process shown are:

- 1** The user enters credentials at the Web site that are passed to the Web server. A third-party authentication client on the Web server passes the user credentials to the third-party authentication service. The third-party authentication service verifies the user credentials and passes the authenticated user's username to the Siebel Web Server Extension (SWSE).
- 2** The Siebel Web Server Extension (SWSE) passes the authenticated user's username to the authentication manager, a component of the Siebel Object Manager. The username can be the Siebel user ID or another attribute.
- 3** The security adapter provides the authenticated user's username to a directory, from which the user's Siebel user ID, a database account, and, optionally roles are returned to the authentication manager.
- 4** The object manager uses the returned credentials to connect the user to the database and to identify the user.

Because Web SSO deployments assume that user authentication and user management are the responsibility of the third-party security infrastructure, 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
- Logout links
- Change password

Following are some implementation considerations for a Web SSO strategy:

- Users are authenticated independently of Siebel applications, such as through a third-party authentication service or through the Web server.
- You must synchronize users in the authentication system and users in the Siebel database at the Web site level.

- You must configure user administration functionality, such as self-registration, at the Web site level.
- A delegated administrator can add users to the Siebel database, but not to the authentication system.

To get more detailed information about integrating third-party authentication software with Siebel eBusiness Applications, see Siebel's SupportWeb site or contact the Siebel Alliance Group.

Implementing Web SSO Authentication

To provide user access to Siebel applications on a Web site implementing Web SSO, the Siebel applications must be able to determine the following from the authentication system:

- Verification that the user has been authenticated
- A user credential that can be passed to the directory, from which the user's Siebel user ID and database account can be retrieved

CAUTION: For a particular Siebel application, you must use the same authentication method for mobile users connecting to the server that you use for other Web client users. You must implement database authentication for all users of the application, or you must implement one of the external authentication strategies for all users of the application. Because most mobile users are employees, this applies mainly to Siebel employee applications such as Siebel Call Center.

Depending on the components and options you implement, you must perform some or all of the following tasks to set up a Web SSO authentication architecture:

- Create protected virtual directories for Siebel applications.
- Set up third-party Web server authentication.
- Set up a directory from which database accounts and the user's Siebel user ID can be retrieved.
- Create a database login for users who are authenticated externally.

- Create user records in the authentication service, in the directory, and in the Siebel database.
- Set up a security adapter as a plug-in to the Siebel applications' object managers.
- Edit the eapps.cfg file to provide authentication parameter values.
- Edit the configuration file for each application's object manager to provide authentication parameter values.
- Edit authentication-related parameters in the Siebel name server.
- Set system preferences.
- Restart the Siebel server and the Web server.

Deployment Options for Web SSO

This section describes options that you can implement only in a Web SSO environment that uses a Siebel-compliant security adapter.

- **User specification source.** You must specify the source from which the Siebel Web Engine derives the user's identity key: a Web server environment variable or an HTTP request header variable.
- You can also implement any of the options that are described in [“Security Adapter Deployment Options” on page 80](#).

In a Web SSO environment, you must also provide your authentication service. If the authentication service does not include an authentication client, you may have to provide an authentication client.

For information about authentication options and procedures for implementing them, see [“Authentication Options” on page 137](#).

For information about special considerations to implementing user authentication, see [“User Authentication Issues” on page 335](#).

Digital Certificate Authentication

A digital certificate is a digital document that includes the public key bound to an individual, organization, or machine. Certificates are issued by certificate authorities (CAs) who have documented policies for determining owner identity and distributing certificates.

X.509 digital certificate authentication is a standards-based security framework that is used to secure private information and transaction processing. Certificates are exchanged in a manner that makes sure the presenter of a certificate possesses the private-key associated with the public-key contained in the certificate.

Siebel supports X.509 digital certificate authentication by the Web server. The Web server performs the digital certificate authentication and Siebel accepts the authentication result in the form of Web SSO.

For information on implementing digital certificate authentication for Web SSO, see [“Digital Certificate Authentication” on page 160](#).

Setting Up Web SSO: A Scenario

This section provides instruction to set up a Web SSO architecture for a single Siebel application. Your implementation may include more than one Siebel application, and you may implement options that are not included here.

Make sure you implement Web SSO in a development environment before deploying it in a production environment. You can repeat the appropriate instructions here to provide Web SSO access to additional Siebel applications. To implement other options, see [“Authentication Options” on page 137](#).

These instructions implement the following basic configuration:

- IIS Web server is deployed on Windows NT. The IIS Web server functions as the authentication service.
- An Active Directory Server (ADS) and the Web server are installed on different machines.
- The ADS serves as a directory of users for the following functions:
 - It authenticates Web server users.
 - It provides the Siebel user ID and the database account for authenticated Web server users.

- The Siebel ADSI adapter is used to communicate between the authentication manager and the ADS.
- The Siebel server that deploys your Siebel Web-based applications, including their object managers, resides on the Web server machine.

NOTE: The instructions in this section describe a minimal, baseline configuration. In a production environment, Siebel does not recommend installing Siebel server on the same machine as the Web server.

If you use a non-Siebel security adapter, it must support the *Siebel Security Adapter Software Developers Kit 7* available on the Siebel SupportWeb site. You must adapt the applicable parts of the following implementation to your security adapter.

The following installations must be completed before you set up this Web SSO authentication environment.

- Your Web server and the ADS are installed on different machines.
- The Siebel applications, including the Siebel Gateway Server and the Siebel server are installed. The Siebel server, including affected applications' object managers, is installed on the Web server machine.

These instructions assume that you are experienced with administering the ADS. You can perform tasks such as creating and modifying user storage subdirectories, creating attributes, creating users, and providing privileges to users.

You must complete the following tasks to implement Web SSO in this environment:

- Create protected virtual directories for Siebel applications on the Web server machine.
- Create a database login for users who are authenticated externally.
- Set up the ADS.
- Create three users in the ADS directory: a regular user, the anonymous user, and the application user.
- Add user records in the Siebel database corresponding to the regular user and the anonymous user in the directory.

- Edit eapps.cfg file parameters.
- Edit the Siebel application's configuration file parameters.
- Edit the name server parameters.
- Set system preferences.
- Restart the Siebel server and the Web server.
- Test the implementation.

Creating Protected Virtual Directories

Protected virtual directories are used with Siebel applications that support anonymous browsing. By making parts of the application available under two Web server virtual directories you are able to configure the third-party authentication client to protect one virtual directory while leaving the other unprotected, and thus accessible for anonymous browsing. When a user requests a Siebel view that requires explicit login, the request is automatically redirected to the protected virtual directory.

You must perform the following tasks to specify to the Web server a virtual directory for a Siebel application. You must repeat both stages of this process for each Siebel application that users access through the Web server.

- Create the virtual directory.
- Specify to the Web server a particular DLL file that allows the Siebel Web Server Extension (a component of the Siebel Web Engine) to communicate with the Web server.

The actual path for each virtual directory and the DLL file are identical for every Siebel application.

To create a virtual directory on Microsoft Internet Information Server

- 1 From the Start menu choose Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Service > Internet Service Manager.

The Internet Service Manager explorer appears.

- 2 Right click the default Web site, and then choose New > Virtual directory.

The New Virtual Directory wizard appears.

- 3 Enter a virtual directory name for a Siebel application, and then click Next. For example, enter `p_eservice` as a virtual directory for Siebel eService.
- 4 Enter the full path to the `\SWEApp\public` directory in the Siebel root directory, which contains the contents to publish to the site, and then click Next. For example, enter

`D:\Siebel root directory name\SWEApp\public.`

- 5 Check the following check boxes and leave all others empty, and then click Finish.
 - Allow Read Access
 - Allow Script Access
 - Allow Execute Access

The Internet Service Manager explorer appears, with the new virtual directory appearing in the hierarchy.

To allow the Siebel Web Server Extension to communicate with the Web server

- 1 In the Internet Service Manager explorer, right click the virtual directory you created, and then choose Properties.

The Properties dialog box appears.

- 2 Click Configuration.

The Application Configuration dialog box appears.

- 3 Click Add.

The Add/Edit Application Extension Mapping dialog box appears.

- 4 Click Browse, navigate to and select the `sweeis.dll` file in the `\SWEApp\bin` directory in the Siebel root directory, and then click Open.

The Add/Edit Application Extension Mapping dialog box appears, including the path to the `sweeis.dll` file.

- 5 Enter `.swe` for the extension, check the Script engine check box only, and then click OK.

The Application Configuration dialog box appears.

- 6 Click Apply, and then click OK.

The Properties dialog box appears.

- 7 Click the Directory Security tab.

- 8 Click Edit in the Anonymous Access and Authentication Control section.

The Authentication Methods dialog box appears.

- 9 Check the Basic Authentication check box, and uncheck all others.

- 10 Click Yes on the Internet Service Manager caution dialog, and then click OK when you return to the Authentication Methods dialog box.

The Directory Security tab in the Properties dialog box appears.

- 11 Click Apply, and then click OK.

Creating a Database Login

One database login must exist for all users who are authenticated externally. This login must not be assigned to any real person. A seed database login is provided for this purpose when you install your Siebel eBusiness Applications, as described in [“Seed Data” on page 345](#). Its login name is LDAPUSER, and its default password, LDAPUSER, should be changed by an administrator. If this login is not present, create it.

Setting Up the Active Directory Server

In this example, the ADS server performs two functions that may be handled by two separate entities in other Web SSO implementations.

- Users are authenticated through the ADS performing its function as the IIS Web server directory.
- The ADS is the directory from which an authenticated user’s Siebel user ID and database account are retrieved.

You must perform separate configuration tasks for the following purposes:

- Configure the ADS as the directory which provides the user IDs and the Siebel database account for authenticated users.
- Configure IIS Web server to authenticate against the ADS.

Configuring the Active Directory Server as the Directory

Determine a subdirectory in the ADS directory to store users. You cannot distribute the users of a single Siebel application in more than one subdirectory. However, you may store multiple Siebel applications' users in one subdirectory. For this example, users are stored in the Users subdirectory under the domain level directory in the ADS.

Define the attributes to use for the following user data. Create new attributes if you do not want to use existing attributes. For this example, attributes are suggested. Some of the suggested attributes exist, without additional configuration, in the ADS directory.

- Data: Siebel user ID. Suggested attribute: sAMAccountName.
- Data: Database account. Suggested attribute: dbaccount.

Additionally, a user password is assigned to each user using the ADS user management tools. The user password is not stored as an attribute.

NOTE: A user password is required for the ADS for its role as the IIS Web server directory, which is the authentication service in this configuration. A user password attribute is not required for ADS as the directory. In other configurations in which the authentication service is physically independent of the directory, the directory is not required to have a user password assigned to each user.

For purposes of IIS Web server authentication, provide attributes as needed to store the username, first name, last name, or other user data.

Configuring IIS Web Server

You must configure the IIS Web server to authenticate against the Active Directory Server.

You can configure your IIS Web server to use Basic authentication.

For information about setting authentication modes for IIS Web server, see your IIS Web server documentation.

For purposes of testing this Web SSO implementation, configure your Web site to require users to log in at an entry point to the Web site.

Creating Users in the Directory

Create three users in the directory as described in [Table 9](#). The attribute names, sAMAccountName and userPassword, are those suggested in this example. Your entries may vary depending on how you make attribute assignments in [“Setting Up the Active Directory Server” on page 112](#).

The sAMAccountName and Password entries for the application user and test user are only suggested. You may vary those entries.

The database account for all three users is the same, and must match the database account reserved for externally-authenticated users described in [“Creating a Database Login” on page 112](#). *P* represents the password in that database account.

For information about formatting the database account attribute entry, see [“Directory Requirements” on page 75](#).

CAUTION: Make sure the application user has privileges to search all records in the directory.

Table 9. Directory Records

User	SAMAccountName	Password	Database Account
Anonymous user	<ul style="list-style-type: none"> ■ Enter the user ID of the anonymous user record for the Siebel application you are implementing. You can use a seed data anonymous user record, as described in “Seed Data” on page 345, for a Siebel customer or partner application. For example, if you implement Siebel eService, enter GUESTCST. ■ You can create a new user record or adapt a seed anonymous user record for a Siebel employee application. 	GUESTPW or a password of your choice	username = LDA PUSER password = P
Application user	APPUSER or a name of your choice	APPUSERPW or a password of your choice	Database account is not required for application user.
A test user	TESTUSER or a name of your choice.	TESTPW or a password of your choice	username = LDA PUSER password = P

Complete other attribute fields for each user as are needed.

Adding User Records in the Siebel Database

You must create a record in the Siebel database that corresponds to the test user you create in [“Creating Users in the Directory” on page 114](#).

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in [Table 22 on page 347](#). This record must also match the anonymous user you create in [“Creating Users in the Directory” on page 114](#).

You can adapt a seed data anonymous user or create a new anonymous user for a Siebel employee application.

For purposes of confirming connectivity to the database, you can use the following procedure to add the test user for any Siebel application. However, if you are configuring a Siebel employee or partner application, and you want the user to be an employee or partner user, complete with position, division, and organization, see the instructions for adding such users in [“Internal Administration of Users” on page 224](#).

To add user records to the database

- 1** Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
- 2** From the application-level menu, choose View > Site Map > User Administration > Users.

The All Users list appears.
- 3** In the All Users list, click the menu button and choose New Record.

A new All Users form appears.
- 4** Use the following guidelines to complete the field entries for the test user, and then click Save. Suggested entries are for this example. You can complete other fields, but they are not required.

Field	Suggested Entry	Guideline
Last Name		Required. Enter any name.
First Name		Required. Enter any name.

Field	Suggested Entry	Guideline
User ID	TESTUSER	Required. This entry must match the sAMAccountName attribute value for the test user in the directory. If you used another attribute instead of sAMAccountName, it must match that value.
Responsibility		Required. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for Siebel eService. If an appropriate seed responsibility does not exist, such as for a Siebel employee application, assign an appropriate responsibility that you create.
New Responsibility		Optional. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for Siebel eService. This responsibility is automatically assigned to new users created by this test user.

- 5 Verify that the seed data User record exists for anonymous users of the Siebel application you implement, as described in [Table 22 on page 347](#). For example, verify that the seed data User record with user ID GUESTCST exists if you are implementing Siebel eService. If the record is not present, create it using the field values in [Table 22 on page 347](#). You can complete other fields, but they are not required.

Editing Parameter Values in the eapps.cfg File

Provide the parameter values in the eapps.cfg file as indicated by the guidelines in [Table 10](#).

For information about editing eapps.cfg parameters and about the purposes for the parameters, see “[Eapps.cfg Parameters](#)” on [page 162](#).

Table 10. Eapps.cfg Parameter Values

Section	Parameter	Suggested Entry	Guideline
[defaults]			The values of the parameters in this section are overridden by the parameter values you set in the sections for individual applications.
The section particular to your application, such as [/eservice], [/echannel], or [/callcenter]	AnonUserName		Enter the user ID of the seed data User record provided for the application that you implement or of the User record you create for the anonymous user. This entry also matches the sAMAccountName entry for the anonymous user record in the directory. For example, enter GUESTCST for Siebel eService.
	AnonPassword		Enter the password you created in the directory for the anonymous user.
	SingleSignOn	Enter TRUE.	
	TrustToken		Enter HELLO, or a contiguous string of your choice.
	UserSpec	Enter REMOTE_USER.	REMOTE_USER is the default Web server variable in which the user's identity key is placed for retrieval by the authentication manager.
	UserSpecSource	Enter Server.	REMOTE_USER is a Web server variable.

Table 10. Eapps.cfg Parameter Values

Section	Parameter	Suggested Entry	Guideline
	ProtectedVirtualDirectory		<p>Enter the name of the protected virtual directory that you created in “Creating Protected Virtual Directories” on page 110. For example, enter / p_eservice if you used the suggested name for the eService protected virtual directory.</p> <p>If your SSO installation is not configured for anonymous browsing, set this value to the same directory as your application. For example:</p> <pre>[/eSales] ProtectedVirtualDirectory =/eSales</pre> <p>Otherwise, a “Web Authentication Failed” message may appear in the application’s log file.</p>
	AnonUserPool		<p>If this parameter is present, comment it out with a semicolon at the beginning of the line. Alternatively, you can delete this parameter line from the file.</p>

CAUTION: If your implementation uses a header variable to pass a user’s identity key from the third-party authentication service, then it is the responsibility of your third-party or custom authentication client to set the header variable correctly. The header variable should only be set after the user is authenticated, and it should be cleared when appropriate by the authentication client. If a header variable passes an identity key to the Siebel authentication manager, and the trust token is also verified, then the user is accepted as authenticated.

Editing the Siebel Application's Configuration File Parameters

Provide the parameter values as indicated by the guidelines in [Table 11](#) in the configuration file for the Siebel application you are implementing. (For a list of Siebel application configuration files, see [“Siebel Application Configuration File Names” on page 343](#).)

NOTE: You can use a text editor to make changes to an application configuration file or you can use the LDAP/ADSI Configuration Utility to make these changes. For more information on using the Configuration Utility see [“Using the LDAP/ADSI Configuration Utility” on page 129](#).

For information about editing an application's configuration file and about the purposes for the parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

Table 11. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
[SWE]	SecureLogin	Enter TRUE or FALSE. If TRUE, the login form completed by the user is transmitted over a secure socket layer (SSL). For information about other requirements for secure login, see “Secure Login” on page 139 .
[SecurityAdapters]	Add a line for each security adapter you may implement; most likely there is only one.	Suggested entry ADSI = ADSI

Table 11. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
The section for the particular security adapter you implement, for example [ADSI]	DllName	Enter <code>sscfadsi.dll</code>
	ServerName	Enter the name of the machine on which the ADS server runs.
	Port	You set the port at the ADS directory level, not as a configuration parameter. If this parameter is present, comment it out, or you can delete the line from the file.
	BaseDN	<ul style="list-style-type: none"> ■ The Base Distinguished Name is the root of the tree under which users are stored. Users can be added directly or indirectly below this subdirectory. ■ Suggested entry (including quotes): <code>"CN=Users,DC=machine,DC=domain,DC=com"</code> ■ Domain Component (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for the user objects in the directory. Therefore, adjust the number of CN and DC entries to represent your architecture.

Table 11. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
	UserNameAttributeType	<ul style="list-style-type: none">■ Suggested entry: <code>sAMAccountName</code> <p>If you use a different attribute in the directory for the Siebel user ID, enter that attribute name.</p>
	PasswordAttributeType	<p>ADS does not store the password in an attribute. If this parameter is present, comment it out, or you can delete the line from the file.</p>
	CredentialsAttributeType	<p>Suggested entry: <code>dbaccount</code></p> <p>If you used a different attribute in the directory for the database account, enter that attribute name.</p>
	ApplicationUser	<ul style="list-style-type: none">■ Suggested entry (including quotes): <code>"CN=APPUSER,CN=Users,DC=machine,DC=domain,DC=com"</code>■ Adjust your entry if your implementation uses a different attribute for the user name, a different user name for the application user, or a different base DN.
	ApplicationPassword	<p>Enter <code>APPUSERPW</code> or the password you assigned to the application user.</p>
	SingleSignOn	<p>Enter <code>TRUE</code>.</p>

Table 11. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
	TrustToken	Enter the TrustToken value that you provided for the same variable in the eapps.cfg file.
	AllowAnonUsers RolesAttributeType SslDatabase UseSSL EncryptCredentialsPassword EncryptApplicationPassword SharedCredentialsDN UseAdapterUsername SiebelUsernameAttributeType UseRemoteConfig	If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Editing the Name Server Parameters

Set each name server parameter listed in [Table 12](#) for the component that corresponds to the object manager for the application you are implementing, such as Call Center Object Manager or eService Object Manager. Set the parameters at the component level and follow the guidelines provided in the table.

For information about setting name server parameters and the purposes for the parameters, see [“Siebel Name Server Parameters” on page 172.](#)

Table 12. Siebel Name Server Parameters

Subsystem	Parameter	Guideline
Object Manager	OM - Configuration File	Name of configuration file for the application you implement, such as eservice.cfg.
	OM - Data Source	Enter the data source for the server on which this Siebel application runs, such as ServerDataSrc.
	OM - Proxy Employee	Enter PROXYE.
	Security Adapter Name	The name of the security adapter you implement as it appears in the [SecurityAdapters] section in the application configuration file; for example, ADSI.
	OM - Username BC Field	Leave empty.
Infrastructure Objmgr configu	Application Encrypt Password	Enter FALSE.

Setting System Preferences

Set each system preference using the guidelines in [Table 13.](#)

For information about setting system preferences and the purposes for the preferences, see [“System Preferences” on page 175.](#)

Table 13. System Preferences

System Preference	Suggested Entry	Guideline
SecExternalUserAdministration	Enter TRUE.	An entry of TRUE provides that the directory cannot be administered from within Siebel applications.
SecThickClientExtAuthent.	Enter FALSE.	This parameter is not applicable in a Web SSO environment.
Security Adapter CRC	Leave empty.	Checksum validation is not implemented.

Restarting Servers

You must stop and restart the following Windows NT services on the Web server machine to activate changes you make to Siebel Object Manager configuration files.

- Stop the IIS Admin service, and then restart the Worldwide Web Publishing Service. The IIS Admin service also starts because the Worldwide Web Publishing Service is a subservice of the IIS Admin service.
- Stop and restart Siebel server. Choose Start > Settings > Control Panel, and then double-click Services to administer the services.

Testing the External Authentication System

The following tests confirm that the Web SSO components work together to:

- Allow a user to log in to the Web site.
- Allow a user who is authenticated at the Web site level to gain access to the Siebel application without requiring an additional login.

To test your external authentication system

- 1** On a Web browser, enter the URL to your Web site, such as `http://www.mycompany.com`.

A Web page with a login form for the Web site should appear.

- 2** Login with the user ID and the password for the test user you created. Enter `TESTUSER` or the user ID you created and `TESTPW` or the password you created.

You should gain access to the Web site.

- 3** On a Web browser, enter the URL to your Siebel application, such as `http://www.mycompany.com/eservice`. Alternatively, if you provide a link on the Web site, click it.

You should get access to the Siebel application as a registered user without having to log in.

Remote Authentication

This section describes the processing steps that occur to authenticate a remote user during synchronization. For details on remote computing in the Siebel environment, see *Siebel Remote Administration Guide, MidMarket Edition*.

Some things to remember about remote users includes:

- Remote users do not connect to the Web server. When remote users synchronize, they connect directly to the Siebel Remote server – the application server allocated for remote users.
- Only one user ID and password can be used to access a local database. Local databases cannot belong to more than one user.
- A single user can have multiple Web mobile clients, such as two clients on two separate computers.

To synchronize

1 The Siebel remote user connects to the local database on their laptop and makes transaction modifications. To do this:

- a** The user launches the Siebel icon on the laptop, and then enters a user ID and password.
- b** In the Connect To parameter, choose Local.

The user ID and password are validated by the local database residing on the laptop.

The Siebel application appears in the Web browser and the user navigates through the application making changes as desired.

2 Later, the user decides to synchronize the local database changes and download updates from the Siebel Remote server. To do this:

- a** The remote user connects to the Siebel Remote server using a dial-up modem or LAN/WAN connection.
- b** The user launches the Siebel icon on their laptop, and then enters a user ID and password.

- c** In the Connect To parameter, choose Local.

The user ID and password are validated by the local database residing on the laptop.

- 3** When the Siebel application appears in the Web browser, the user chooses File > Synchronize Database.

The user is now accessing the Siebel Remote server for synchronization.

The Siebel Remote Synchronization Manager authenticates incoming mobile Web client requests to make sure that a mobile Web client is valid. The Siebel Remote Synchronization Manager validates the mobile client's user ID against the list of valid mobile clients in the server database and validates that the effective end date is valid or NULL.

The Siebel Remote Synchronization Manager also verifies that the mobile client has connected to the correct Siebel Remote server. If the mobile client connects to the wrong remote server, the Synchronization Manager reconnects the mobile client to another Siebel Remote server and updates the client's local configuration information.

The Siebel Remote Synchronization Manager validates the mobile client's password by using one of the following authentication methods, represented by a parameter name. The Siebel administrator uses the Siebel Server Manager to set these parameters for the Synchronization Manager. For more information, see *Siebel Remote Administration Guide, MidMarket Edition*.

- **None.** Does not validate the mobile client's password. This is the default setting.
- **Database.** Uses the mobile client's user name and password to connect mobile Web clients to the server database.

NOTE: You cannot use the Database authentication parameter for Web SSO. Also, you cannot use database authentication if you have enabled password encryption because the mobile client would have to use the encrypted password to log in to the local database.

- **Siebel.** Validates the mobile Web client's password against the password stored in the mobile Web client's screen.
 - **AppServer.** Verifies that the password is the same as the user's operating system password on the Siebel server.
- 4 Once the remote user is authenticated, synchronization begins.

This section describes how to use the LDAP/ADSI Configuration Utility to help you configure a directory service for your Siebel applications. It also includes a description of authentication options available for user authentication.

Using the LDAP/ADSI Configuration Utility

Siebel Systems provides an LDAP/ADSI Configuration Utility to help you configure a directory service for your Siebel applications. The utility provides a graphical user interface (GUI) to update parameters in Siebel application configuration files (for example, `eservice.cfg`).

The utility automatically runs as part of the Siebel server installation, but you can also run the utility as a stand-alone program. Run the utility for each Siebel application you wish to set up.

To run the utility

- 1 Use the Start > Run command to run the utility. The utility is located in:

```
<SiebelServerRoot>\ADMIN\CONFIG\config.exe
```

where < SiebelServerRoot > is the root directory for the Siebel application server.

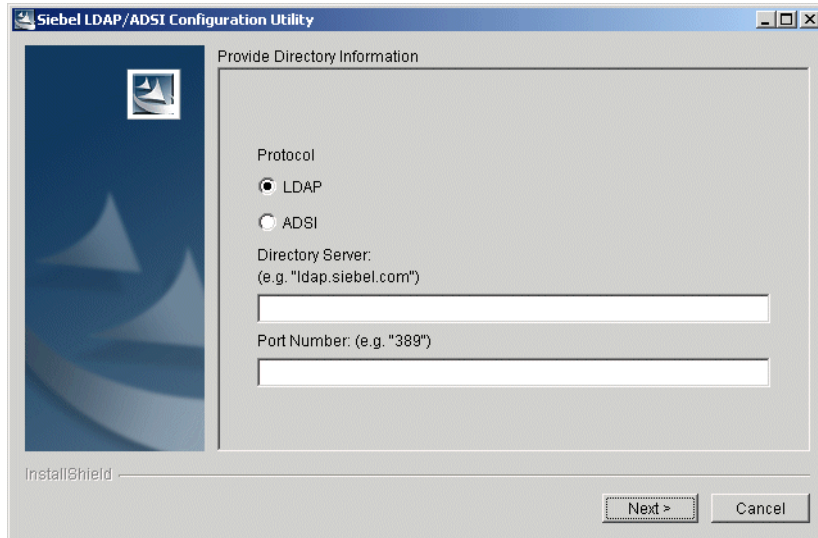
The utility works as a JVM (Java Virtual Machine) executable. There are no special set up requirements to run it.

NOTE: The utility works best if run locally rather than over the network. Therefore, Siebel Systems recommends you run the utility from the machine that hosts the Siebel application you want to configure.

Authentication Details

Using the LDAP/ADSI Configuration Utility

- 2 A series of screens appears with a list of LDAP/ADSI configuration settings. The following figure shows an example of an LDAP/ADSI configuration screen.



The number of screens that appear depends on the configuration options you have chosen. As you enter information, click Next to proceed to the next screen. Click Back to return to a previous screen.

NOTE: The utility sets directory configuration parameters for Siebel applications, but it does not make changes to the directory or directory server. Make sure the configuration information you enter is compatible with your directory server.

3 Configuration information you enter includes:

a Directory Information

- Protocol. The type of directory you are configuring: LDAP or ADSI
- Directory Server. For LDAP, this is the name of the Directory Server (for example, ldap.siebel.com). For ADSI, you can specify a Domain Name in this field. (For domains that contain more than one directory server, specifying a domain name is useful for maintaining load balance across servers.)
- Port Number: The port number used by the Directory Server. This setting applies to LDAP directories only. Use port 389 for standard transmission or port 636 for secure transmission. (ADS ports are set as part of the directory installation, not as a configuration parameter.)

b Attribute Mapping

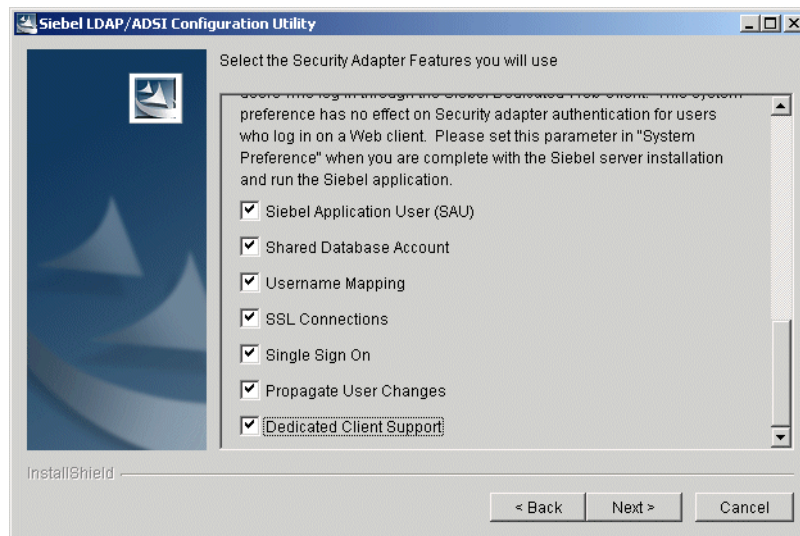
- Username Attribute. The Siebel user ID attribute (UserNameAttributeType) used by the directory. The suggested entry for an LDAP directory is `uid`. The suggested entry for ADSI is `sAMAccountName` (maximum length of 20 characters). If your directory uses a different attribute for the Siebel user ID, enter that attribute instead.
- Database Account Attribute. The CredentialsAttributeType used by the directory. For LDAP and ADSI, the suggested entry is `dbaccount`. If your directory uses a different attribute for the database account, enter that attribute instead.
- Roles Attribute. The attribute type for roles stored in the directory (RolesAttributeType). This setting is required only if you use roles in your directory. For more information on roles, see [“Roles” on page 137](#).

Authentication Details

Using the LDAP/ADSI Configuration Utility

- 4 When the Configuration Options screen appears, scroll to the bottom of the screen to select the options you wish to configure. You can select one or more of the options.

The following figure shows configuration options you can choose for the LDAP/ADSI configuration utility.



After you select options, the number of screens that appear depends on which options you have chosen. The following table describes configuration options and the associated information required for each option.

Option	Description	Required Settings
Siebel Application User (SAU)	Allows you to specify a single directory account that the Siebel application uses to search, update or read directory entries. Creating an SAU account allows you to limit directory access by individual end users. For more information, see “Application User” on page 145 .	<p>This option requires a user name and password for the account:</p> <ul style="list-style-type: none"> ■ SAU Distinguished Name <p>This is the full distinguished name of the Siebel Application User (ApplicationUser). Make sure you include the quotes in the name.</p> <ul style="list-style-type: none"> ■ SAU Password <p>This is the password you specify for the Siebel Application User. If you create a Siebel Application User, make sure you also add this name and password to the directory.</p>
Shared Database Account	This option simplifies directory administration by enabling multiple-user entries in a directory to share the same database account. Without this option, a database account must be created for each user entry in the directory. For more information, see “Shared Database Account” on page 153 .	<p>This option requires specifying the following information:</p> <ul style="list-style-type: none"> ■ Distinguished Name for the Shared Database Account <p>This is the distinguished name (SharedCredentialsDN) for the directory entry that is used to share the database account. For example:</p> <pre>"uid=SHAREENTRY, ou=People, o=xzy.com"</pre> <ul style="list-style-type: none"> ■ Shared Database Account Attribute <p>This is the attribute (CredentialsAttributeType) used to store the database account in the directory (for example, dbaccount).</p>

Authentication Details

Using the LDAP/ADSI Configuration Utility

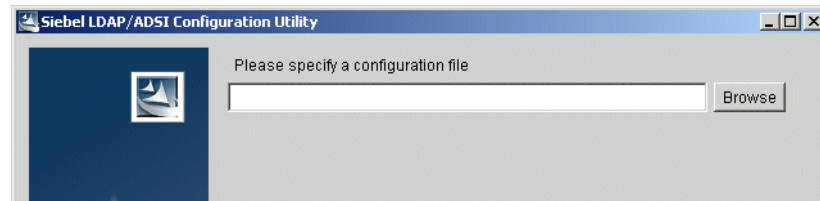
Option	Description	Required Settings
Username Mapping	This option allows users to be authenticated by something other than the Siebel user ID (for example, a social security number, phone number, or email address). As with Siebel user ID, this identifier must be unique. For more information, see “Adapter-Defined User Name” on page 154 .	<p>This option requires specifying:</p> <ul style="list-style-type: none">■ Username Attribute <p>This is the name of the attribute used to authenticate users. The security adapter references this attribute instead of the Siebel user ID attribute (for example, <code>email_ID</code>).</p> <ul style="list-style-type: none">■ Username Field (in Siebel) <p>This is the name of the field in the Siebel interface (OM-Username BC Field Name) that stores the Username Attribute (for example, <code>Email Address</code>).</p> <ul style="list-style-type: none">■ Siebel User ID Attribute <p>This is the attribute (SiebelUsernameAttributeType) used by the security adapter to retrieve the Siebel user ID for an authenticated user (for example <code>uid</code>).</p>
Single Sign-On	This option sets Web SSO. With Web SSO, users can access multiple applications from a single logon screen. When Web SSO is enabled, user credentials are verified by a third-party authentication service instead of the security adapter.	<p>Selecting this option sets the SingleSignOn attribute to TRUE. This option also requires specifying:</p> <ul style="list-style-type: none">■ Shared Secret <p>This is the value of the TrustToken attribute used by the security adapter and the Web server to prevent Web Engine spoofing attacks (for example, <code>HELLO</code>). The value you enter must match TrustToken value used by the Web server.</p>

NOTE: The LDAP/ADSI utility only sets the Web SSO parameters in a Siebel application configuration file. You must also set the parameters in your `eapps.cfg` file. For more information about setting up Web SSO, see [“Implementing Web SSO Authentication” on page 106](#).

Option	Description	Required Settings
Propagate User Changes	This option displays instructions on how to enable Siebel applications to propagate user changes to the directory. When this option is enabled, the directory is updated automatically when users are added or passwords changed in a Siebel application.	To enable this option, use the Applications Administration screen in your Siebel Application to set the System Preference, SecExternalUserAdministration to FALSE. For more information, see “System Preferences” on page 175 .
Dedicated Client Support	This option displays instructions on how to enable security adapter authentication for users who log in through the Siebel Dedicated Web Client.	To enable this option, use the Applications Administration screen in your Siebel Application to set the System Preference, SecThickClientExtAuthent to TRUE. For more information, see “System Preferences” on page 175 .

- When you have finished entering configuration information, a final screen appears. Use this screen to specify a file to store the information you have entered.

The following figure shows the screen you use to specify a file for storing configuration information.



CAUTION: The LDAP/ADSI configuration utility overwrites rather than appends the file you specify. To prevent losing important configuration information, designate a new, empty file, then copy the results to the *.cfg file for your Siebel application.

For more information on where configuration files are located for Siebel eBusiness applications, see [“Siebel Application Configuration File Parameters” on page 164](#).

- 6 Click Next to add configuration information to the file you specify.

The following list is an example of LDAP configuration information produced by the utility.

```
[LDAP]
DllName                = sscfldap.dll
ServerName             = ldapserver.siebel.com
Port                   = 636
BaseDN                 = "ou=people, o=xyz.com"
SharedCredentialsDN    =
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = dbaccount
RolesAttributeType    = roles
SharedCredentialsDn    = "uid=HKIM, ou=people, o=Siebel.com"
SslDatabase            = /suitespot/https-myhost/cert7.db
ApplicationUser        = "uid=APPUSER, ou=people, o=xyz.com"
ApplicationPassword    = teMPass
EncryptApplicationPassword = TRUE
EncryptCredentialsPassword = TRUE
SingleSignOn          = TRUE
TrustToken             = HELLO
UseAdapterUsername     = TRUE
SiebelUsernameAttributeType = PHONE
UseRemoteConfig        = \\myserver\vol\remconf\remote.cfg
```


Authentication Options

For each option in this section, you are instructed to do various implementation tasks, such as running software utilities, providing parameter values, and setting system preferences. Typically, high-level procedures are provided and the goal of each step is stated, such as to set the value of a particular parameter. However, the detailed procedures are not included for each step. Instead of repeating the same procedure many times in this section, each procedure appears once.

For information about:

- The eapps.cfg file parameters, see [“Eapps.cfg Parameters” on page 162](#).
- Application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).
- Siebel name server parameters, see [“Siebel Name Server Parameters” on page 172](#).
- System preferences, see [“System Preferences” on page 175](#).
- Seed data, see [“Seed Data” on page 345](#).

Roles

Roles are an alternate means of associating Siebel responsibilities with users. This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

Responsibilities assigned to each user in Siebel eBusiness Applications provide the user access to views the appropriate view in Siebel applications. Responsibilities are created in the database. One or more responsibilities are typically associated with each user through the user’s Responsibility field in the Siebel user interface.

Roles in the directory are another means of associating Siebel responsibilities with users. Roles are useful for managing large collections of responsibilities. A user has access to all the views contained in all the responsibilities associated with the user's record in the database, and in all the responsibilities listed in the attribute used for roles in the directory.

CAUTION: It is recommended that you assign responsibilities in the database or in the directory, but not in both places. If you define a directory attribute for roles, but you do not use it to associate responsibilities with users, leave the attribute empty.

If you use roles to administer user responsibilities, follow these guidelines:

- Do not assign users any responsibilities through a Siebel application interface.
- To allow assigning more than one responsibility to any user, you must define a directory attribute for roles that is multi-value. Siebel-supported security adapters cannot read more than one responsibility from a single-value attribute.
- The attribute for roles should contain the names of the Siebel responsibilities that you want the user to have. Enter one responsibility name, such as Web Registered User, in each element of the multi-value field. Role names are case-sensitive.

You can configure Siebel-supported security adapters to retrieve roles for a user from the directory. For each Siebel application that uses roles, set the following parameter value in the application's configuration file. For example, edit the `eservice.cfg` file for Siebel eService.

- In the *[Adapter name]* section, for example [LDAP], set
`RolesAttributeType= attribute in which roles are stored`

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

Roles are discussed in a usage context in [“Directory Requirements” on page 75](#).

CAUTION: Do not confuse roles defined by an LDAP or ADS directory with roles defined in the Siebel application interface. Roles in LDAP or ADS directories are collections of responsibilities that strictly enforce access to views and data records within Siebel applications. Roles defined in the application interface allow application administrators to increase the usability and deployability of the application by tailoring the product to groups of users. For more information about roles defined in an application interface, see [“Creating and Administering Roles” on page 322](#).

Secure Login

This option can be implemented in the following authentication strategies:

- Database authentication
- Siebel security adapter authentication
- Web SSO

You can specify to the Siebel Web Engine to transmit user credentials from the browser to the Web server over HTTPS.

To implement secure login

- For each Siebel application that implements secure login, set the following parameter value in the [SWE] section of the application’s configuration file. For example, edit the `eservice.cfg` file for Siebel eService.

```
SecureLogin = TRUE
```

To implement secure login, you must also have a certificate from a certificate authority on the Web server on which the Siebel Web Engine is installed.

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

Secure login is discussed in a usage context in [“Implementing Database Authentication” on page 72](#), and in [“Deployment Options for Siebel LDAP and ADSI Security Adapter Authentication” on page 84](#).

User Password Encryption

This option can be implemented in the following authentication strategies:

- Database authentication
- Siebel security adapter authentication

User password encryption allows you to maintain an unexposed, encrypted password for each user while the user logs in with an unencrypted version of the password.

You can implement user password encryption with the Siebel encryption utility. The Siebel encryption utility is available on the Password Encryption diskette available through Siebel Technical Services.

User password encryption supports the following principles:

- Each password is first encrypted. For example, `siebel` is encrypted as `T>?Be`.
- The encrypted version (`T>?Be`) is stored in one of the following locations:
 - In a database authentication environment, it is set as the valid password for the database account.
 - In an external authentication environment, it is stored in the attribute specified for the user's password.
- The unencrypted version of the password (`siebel`) is given to a user to use at login.

A user is logged into the database by the following process:

- The user logs in with user credentials that include the unencrypted password (`siebel`).
- The authentication manager receives the user credentials, and passes them to the object manager.
- The object manager encrypts the password (`T>?Be`).

- In an external authentication environment:
 - The user credentials, including the encrypted password are passed to the security adapter through the authentication manager.
 - The security adapter verifies that the encrypted password matches the encrypted password stored in the directory for the user, and then returns the database account and the Siebel user ID to the object manager through the authentication manager.
- In a database authentication environment, the object manager verifies that the database account identified by the user credentials exists and that the encrypted user password matches the password for the database account (T>?Be).
- The object manager connects the user to the database and the Siebel application.

To implement user password encryption

- 1 For each user, create and record a username and a password.
- 2 Do one or more of the following:
 - To encrypt an individual password, enter and run the following command at a command prompt:

```
encrypt password
```

The utility encrypts the argument and verifies the results. For example, to encrypt the password “siebel,” enter:

```
encrypt siebel
```

The confirmation from the utility is similar to:

```
Encoding String => siebel <= to => T>?Be <=
```

```
Verify encoding => T>?Be <= to => siebel <=
```

- To encrypt multiple passwords at the command prompt, use the following command-line syntax:

```
encrypt password1 password2 password3 ...
```

- To encrypt multiple passwords using a batch file:

Enter the passwords into a batch file (in this instance, the file is named passwords.txt), and then use the following command-line syntax:

```
encrypt @passwords.txt
```

- 3 For each user, do one of the following:

- In a database authentication environment, set the credentials for a database account to the username and the encrypted password.

For information about setting credentials for database accounts, see your RDBMS documentation.

- In an external authentication environment, set the values in the directory attributes for username and password to the username and the encrypted password.

- 4 Set the Application Encrypt Password parameter in the Siebel name server to TRUE at one of the following levels.

- To implement user password encryption for a single application, set the parameter at the component level for the application's object manager, such as Call Center Object Manager.
- To implement user password encryption for all applications on a particular Siebel server, set the parameter at the server level for the particular Siebel server.

For information about setting Siebel name server parameters, see [“Siebel Name Server Parameters” on page 172](#).

- 5 Provide the username and unencrypted password to the user for logging in.

User password encryption is discussed in a usage context in [“Implementing Database Authentication” on page 72](#) and in [“Security Adapter Deployment Options” on page 80](#).

Credentials Password Encryption

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

Credentials password encryption allows you to maintain an unexposed, encrypted password to a database account, while an unencrypted version of the password is used in other phases of the authentication process.

You can implement credentials password encryption with the Siebel encryption utility. The Siebel encryption utility is available on the Password Encryption diskette available through Siebel Technical Services.

Credentials password encryption supports the following principles:

- For each database account, a password is first encrypted. For example, `siebel` is encrypted as `T>?Be`.
- The encrypted version (`T>?Be`) is stored as the valid password for the database account.
- The unencrypted version of the password (`siebel`) is stored in the attribute containing the database account for each applicable user in the directory.

A user is logged into the database by the following process:

- The authenticated user's database account, stored in the directory, is passed to the authentication manager by the security adapter.
- The object manager receives the user credentials from the authentication manager.
- The object manager encrypts the password (`T>?Be`).
- The object manager verifies that the database account identified by the user credentials exists and has a password that matches the encrypted version (`T>?Be`).

- The object manager connects the user to the database and the Siebel application.

NOTE: You cannot implement credentials password encryption if the data source you are connecting to is undocked. A data source is undocked if `Docked = FALSE` for the data source in the application's configuration file.

To implement credentials password encryption

- 1** For each database account, create and record the login name and a password.

- 2** Do one or more of the following:

- To encrypt an individual password, enter and run the following command at a command prompt:

```
encrypt password
```

The utility encrypts the argument and verifies the results. For example, to encrypt the password "siebel," enter:

```
encrypt siebel
```

The confirmation from the utility is similar to:

```
Encoding String => siebel <= to => T?Be <=
```

```
Verify encoding => T?Be <= to => siebel <=
```

- To encrypt multiple passwords at the command prompt, use the following command-line syntax:

```
encrypt password1 password2 password3 ...
```

- To encrypt multiple passwords using a batch file:

Enter the passwords into a batch file (in this instance, the file is named `passwords.txt`), and then use the following command-line syntax:

```
encrypt @passwords.txt
```

- 3** Assign the encrypted passwords to their corresponding database accounts.

For information about assigning passwords to database accounts, see your RDBMS documentation.

- 4 For each Siebel application that implements credentials password encryption, set the following parameter value in the application's configuration file. For example, edit the `eservice.cfg` file for Siebel eService.

In the *[Adapter name]* section, for example [LDAP]:

```
EncryptCredentialsPassword = TRUE
```

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

- 5 Make sure that the attribute in the directory that contains the database account contains the unencrypted version of the database password.

For information about required attributes in the directory, see [“Directory Requirements” on page 75](#).

Credentials password encryption is discussed in a usage context in [“Security Adapter Deployment Options” on page 80](#).

Application User

This option can be implemented in the following authentication strategies that implement a Siebel security adapter:

- Siebel security adapter authentication
- Web SSO

By setting up an application user as the only user with search and write privileges to the directory, you minimize the level of access of all other users to the directory and the administration required to provide such access.

The application user is a user that you define in the directory with the following qualities:

- This user provides the initial binding of the LDAP or Active Directory server with the object manager when a user requests the login page, else binding defaults to the anonymous user.
- This user has sufficient permissions to read any user's information and do any necessary administration. The application user does all searching and writing to the directory that is requested through the security adapter.

- Unlike other user records in the directory, the application user does not need a database account. The application user does not access the database.

If you do not implement an application user in a Siebel security adapter authentication environment, then:

- The anonymous user must have search and write privileges to the directory if you allow user self-registration.
- Each user who creates or modifies other users must have search and write privileges to the directory. Internal administrators and delegated administrators are included in this group.

It is strongly recommended that you implement an application user.

To implement an application user

- 1 In the directory, define a user that uses the same attributes as other users. Assign values in appropriate attributes that contain the following information:
 - **Username.** Assign a name of your choice. If you implement an adapter-defined username, use that attribute. Otherwise, use the attribute in which you store the Siebel user ID, although the application user does not have a Siebel user ID.
 - **Password.** Assign a password of your choice. You can opt to enter an encrypted password if you implement application password encryption. If you implement an ADS directory, you specify the password using ADS user management tools, not as an attribute.

NOTE: Make sure the application user has, at least, search privileges for all user records in the directory in a Web SSO implementation. Additionally, provide the application user with write privileges in a Siebel security adapter implementation.

- 2 For each Siebel application that implements an application user, set the following parameter values in the application's configuration file, both on the server and in each Siebel Dedicated Web Client. For example, edit the `eservice.cfg` file for Siebel eService.

- In the `[Adapter name]` section, for example `[LDAP]`:

`ApplicationUser = application user's full distinguished name (DN) in the directory`

`ApplicationPassword = encrypted or unencrypted version of the password, depending on whether you implement application user password encryption`

- If you implement application user password encryption:

`EncryptApplicationPassword = TRUE`

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

For information about application user password encryption, see [“Application User Password Encryption”](#) that follows.

The application user is discussed in a usage context in [“Implementing LDAP and ADSI Security Adapter Authentication” on page 83](#) and in [“Implementing Web SSO Authentication” on page 106](#).

Application User Password Encryption

You can maintain an unexposed, unencrypted password for the application user in the directory, while an encrypted version of the password is used in other phases of the authentication process.

You can implement application user password encryption with the Siebel mangle utility. The Siebel mangle utility is included when you install your Siebel applications.

For information about the application user, see [“Application User” on page 145](#).

The following application user password encryption principles and procedures apply to users who access a Siebel application through the Web client or through the Siebel Dedicated Web Client.

To implement application user password encryption

- 1** Create a password and enter it in the attribute in the directory in which the application user's password is stored. If you implement an ADS directory, you specify the password using ADS user management tools, not as an attribute.
- 2** From a command line run `mangle.exe`, located in the `siebsvr\bin` subdirectory in the Siebel root directory, on the password from [Step 1](#). For example, enter `mangle password`.

The command line returns the encrypted version of the password.

- 3** For each Siebel application that implements application user password encryption, set the following parameter values in the application's configuration file. For example, edit the `eservice.cfg` file for Siebel eService.

- In the `[Adapter name]` section, for example `[LDAP]`:

```
ApplicationUser = application user's full distinguished name (DN)
in the directory
```

```
ApplicationPassword = encrypted version of the password
```

```
EncryptApplicationPassword = TRUE
```

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters”](#) on page 164.

Application user password encryption is discussed in a usage context in [“Deployment Options for Siebel LDAP and ADSI Security Adapter Authentication”](#) on page 84.

Application User and Password Expiration Policies

Typically, user administration in an LDAP or ADS server is performed through the application user. In addition, user policies that are set for the entire directory apply to the application user as well as to all other users.

Typically, you do not want the application user's password to expire. If you implement a password expiration policy in the directory, then you must exempt the application user from the policy. To do so, set the application user's password policy explicitly after the application user sets the password policy for the whole directory.

Checksum Validation

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

Checksum validation provides a check that each user who attempts to gain access to the Siebel database has done so through the correct security adapter.

You can implement checksum validation with the Siebel checksum utility that is included when you install your Siebel application.

Checksum validation supports the following principles:

- A checksum value for the required security adapter DLL is stored as a Siebel system preference.
- When a security adapter provides a user identity and database account to the object manager, a checksum value is calculated for that security adapter.
- The user is granted access if the two checksum values are equal.

To implement checksum validation

- 1 Enter and run the following command at a command prompt, using the required security adapter DLL filename as the argument:

```
Checksum -f filename
```

The utility returns the checksum value. For example,

```
Checksum -f sscfldap.dll
```

would return something similar to:

```
CRC checksum for file 'sscfldap.dll' is f49b2be3.
```

NOTE: The checksum value in this procedure is an example only. You must run the checksum utility as is described to generate the value that is valid for your implementation.

- 2 Set the Security Adapter CRC Siebel system preference to the checksum value that is calculated in [Step 1 on page 149](#).

NOTE: You must recalculate the Security Adapter CRC checksum value whenever you upgrade your Siebel eBusiness Applications.

For information about setting Siebel system preferences, see [“System Preferences” on page 175](#).

Checksum validation is discussed in a usage context in [“Security Adapter Deployment Options” on page 80](#).

Remote Configuration

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

You can create a separate text file that defines some or all of the parameter values that configure a security adapter. The parameter values in the remote configuration file supplement or override those for the same adapter in a Siebel application's configuration file.

You can reduce administration by storing configuration parameters in a centralized location. Multiple applications' configuration files, on servers and on dedicated clients, can read parameters from this one location.

You can provide all configuration parameters in the remote configuration file or you can provide some parameters in the applications' configuration files and the balance of the parameters, such as those that are common among applications, in the remote configuration file.

The following example shows how a remote configuration file could be used to provide parameters for a security adapter that is implemented by Siebel eService in a Web SSO environment.

eservice.cfg (partial):

```
[Security Adapters]
LDAP = LDAP

[LDAP]
DllName = sscfldap.dll
ServerName = it_2.siebel.com
Port = 391
BaseDN = "ou=people,o=siebel.com"
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = credentials
SharedCredentials = "uid=shareduser, ou=people, o=siebel.com"
UseRemoteConfig = \\it_3\vol_1\private\ldap_remote.cfg
```

ldap_remote.cfg (complete):

```
[LDAP]
SingleSignOn = TRUE
TrustToken = HELLO
ApplicationUser = "uid=APPUSER,,ou=people,,o=siebel.com"
ApplicationPassword = YT>3#
EncryptApplicationPassword = TRUE
```

To implement remote security configuration, you must follow these guidelines:

- The Siebel application's configuration file must contain a section that corresponds to a security adapter listed in its [SecurityAdapters] section. For example, the [LDAP] section may contain parameters for the LDAP line in the [SecurityAdapters] section, as shown.
 - It must, at least, include the UseRemoteConfig parameter, which provides the path to a remote configuration file in universal naming convention format, that is, \\server\vol\path\filename.cfg.
 - It may include any other parameters typical to this section, or none of them.

- The remote security configuration file contains only a section that defines external authentication integration, such as the [LDAP] section.
 - It has the same name and is of the same format as the corresponding section in the Siebel application's configuration file.
 - It contains authentication parameters that are not represented in the application configuration file and parameters whose values should be overridden.
- The Authentication Manager must have read privileges on the disk directory that contains the remote configuration file.

For information about the Authentication Manager, see [“Siebel Authentication Manager” on page 67](#).

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

Remote configuration is discussed in a usage context in [“Security Adapter Deployment Options” on page 80](#).

Secure Adapter Communications

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

You can encrypt the communications between the Siebel LDAP or ADSI security adapter and the directory using SSL. The setup you must do differs depending on whether you implement the Siebel LDAP adapter or the Siebel ADSI adapter.

To implement SSL for the Siebel LDAP security adapter

- Set the SslDatabase parameter value in the application's configuration file to the absolute path of a Netscape cert7.db file that contains a certificate for the certificate authority that is used by the LDAP server.

To implement SSL for the Siebel ADSI security adapter

- 1 You must set up an enterprise certificate authority in your domain.
- 2 Set up the public key policy so that the Active Directory Server automatically demands a certificate from that certificate authority.
- 3 Set the UseSsl parameter value to TRUE in the application's configuration file.

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

Secure Adapter Communications is discussed in a usage context in [“Security Adapter Deployment Options” on page 80](#).

Shared Database Account

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

You can configure your external authentication system so that a designated directory entry contains a database account that is shared by many users.

By default, the shared database account option is not implemented, and each user's database account exists in an attribute of that user's record in the directory. Because all externally-authenticated users share one or a few database accounts, the same credentials are duplicated many times. If those credentials must be changed, you must edit them for every user. By implementing a shared credential, you can reduce directory administration.

To implement a shared database account

- 1 Create a database account to be shared by all users who log in to a given Siebel application.
- 2 Create a designated entry in the directory, and enter the username and password parameters for the common database account in one of that entry's attributes, such as the dbaccount attribute. You may need to create this attribute.

For information about formatting a directory attribute that contains the database account, see [“Directory Requirements” on page 75](#).

- 3 For each Siebel application that implements this shared database account, set the following parameter values in the application's configuration file. For example, edit the `eservice.cfg` file for Siebel eService.

- In the `[Adapter name]` section, for example `[LDAP]`:

`CredentialsAttributeType= attribute in which the database account is stored in the directory, such as dbaccount`

`SharedCredentialsDN= the distinguished name (including quotes) for the designated entry, such as "uid=SHAREENTRY, ou=People, o=companyname.com"`

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters”](#) on page 164.

The shared database account is discussed in a usage context in [“Deployment Options for Siebel LDAP and ADSI Security Adapter Authentication”](#) on page 84 and in [“Setting Up Security Adapter Authentication: A Scenario”](#) on page 85.

Adapter-Defined User Name

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

You can configure your external authentication system so that the username passed to the directory to retrieve a user's database account is not the Siebel user ID. For example, you may want users to enter an adapter-defined user name, such as their Social Security number or an account number.

When a user logs in with an adapter-defined user name, the user's Siebel user ID must still be provided to the Siebel application's object manager.

The adapter-defined user name must be stored in one attribute in your directory, while the Siebel user ID is stored in another attribute. For example, you may have users enter their telephone number, stored in the `telephonenumber` attribute, while their Siebel user ID is stored in the `uid` attribute.

The `UsernameAttributeType` application configuration parameter defines the directory attribute that stores the user name that is passed to the directory to identify the user, whether it is the Siebel user ID or an adapter-defined user name. The `OM - Username BC Field Name Server` parameter defines the field of the User business component that underlies the attribute specified by `UsernameAttributeType`.

Even if other requirements to administer user attributes in the directory through the Siebel client are met, you must also set the `UsernameAttributeType` and `OM - Username BC Field` parameters. Otherwise, changes through the Siebel client to the underlying field are not propagated to the directory. For example, for users to log in with their work phone number, you must specify `UsernameAttributeType` to be the directory attribute in which the phone number is stored, for example `telephonenumber`, and you must define `OM - Username BC Field` to be `Phone #`, the field in the User business component for work phone number.

NOTE: Because the directory attribute that contains the Siebel user ID cannot be administered from the Siebel client if an adapter-identified user name is implemented, you must duplicate in the directory any change to the Siebel user ID in the database. Also, because the Siebel user ID in the directory cannot be managed from the Siebel client, you cannot implement user self-registration or delegated registration of users if you implement an adapter-defined username.

To implement an adapter-defined user name

- 1 For each Siebel application that implements an adapter-defined user name, set the following parameter values in the application's configuration file. For example, edit the `eservice.cfg` file for Siebel eService.

- In the `[Adapter name]` section, for example `[LDAP]`:

```
UseAdapterUsername = TRUE
```

```
SiebelUserNameAttributeType = attribute in which you store the Siebel user ID, such as uid (LDAP) or sAMAccountName (ADSI).
```

```
UsernameAttributeType = attribute in which you store the adapter-defined user name, such as telephonenumber.
```

- 2 Determine the field on the User business component that is used to populate the attribute in the directory that contains the adapter-defined username.

The object manager parameter to be populated is UsernameBCField.

For information about working with Siebel business components, see *Siebel Tools Reference, MidMarket Edition*.

- 3 In the Siebel name server, enter the User business component field name as the value for the OM - Username BC Field parameter. You can provide this value at the enterprise, server, or component level. If this parameter is not present in the parameters list, add it.

NOTE: If you do not specify a field in the OM - Username BC Field parameter, the Siebel security adapters assume the Login Name field of the User business component (the Siebel user ID) underlies the attribute defined by the UsernameAttributeType parameter.

For information about setting Siebel application configuration file parameters, see [“Siebel Application Configuration File Parameters” on page 164](#).

For information about setting Siebel name server parameters, see [“Siebel Name Server Parameters” on page 172](#).

The adapter defined user name is discussed in a usage context in [“Deployment Options for Siebel LDAP and ADSI Security Adapter Authentication” on page 84](#).

User Specification Source

This option can be implemented in the following authentication strategies:

- Web SSO

In a Web SSO implementation, the Siebel Web Server Extension derives the user's username from either a Web server environment variable or an HTTP request header variable. You must specify one source or the other.

CAUTION: If your implementation uses a header variable to pass a user's identity key from the third-party authentication service, then it is the responsibility of your third-party or custom authentication client to set the header variable correctly. The header variable should only be set after the user is authenticated, and it should be cleared when appropriate by the authentication client. If a header variable passes an identity key to the Siebel authentication manager, and the trust token is also verified, then the user is accepted as authenticated.

To specify the source of the username

- In the eapps.cfg file, provide the following parameter values in either the [defaults] section or the section for each individual application, such as [/eservice].
 - UserSpec = name of the variable, such as REMOTE_USER (a Web server environment variable)
 - UserSpecSource = Server, if you use an Web server environment variable
 - UserSpecSource = Header, if you use an HTTP request header variable

NOTE: If you use a header variable to pass the username from an IIS Web server, first configure the IIS server to allow anonymous access. You make this security setting for the default Web site in the IIS Service Manager.

For information about setting parameters in the eapps.cfg file, see [“Eapps.cfg Parameters” on page 162](#).

The user specification source is discussed in a usage context in [“Deployment Options for Web SSO” on page 107](#) and in [“Setting Up Web SSO: A Scenario” on page 108](#).

Anonymous User

The anonymous user is a Siebel user with very limited access. The anonymous user (defined as a record in the Siebel database) allows a user to access a login page or a page containing a login form. For external authentication, the anonymous user must have a corresponding record in the user directory.

You must define an anonymous user for any Siebel application that implements external authentication.

The anonymous user is required even if your applications do not allow access by unregistered users. When the Object Manager first starts up, it uses the anonymous user account to connect to the database and retrieve information (such as a license key) before presenting the Login screen.

In the `eapps.cfg` file, you can specify that an anonymous user be used for a single application or as the default for all the Siebel applications you deploy. Even if the anonymous user is specified as the default, any single application can override the default.

If you use one anonymous user for most or all of your applications, you may want to define the anonymous user at the defaults level, which requires less administration.

For any parameter's value, including `AnonUserName` and `AnonPassword`, to be a default, make sure it is listed in the `[defaults]` section of the `eapps.cfg` file.

For a parameter to override the default value for an individual application, list it in the application's section, such as the `[/eservice]` section.

The anonymous user is discussed in a usage context in [“Setting Up Security Adapter Authentication: A Scenario” on page 85](#) and in [“Setting Up Web SSO: A Scenario” on page 108](#).

Anonymous Browsing

If you implement security adapter authentication or database authentication, you can allow or disallow unregistered users to browse a subset of an application's views. If you allow anonymous browsing, users can browse views that are not flagged for explicit login. If you do not allow anonymous browsing, unregistered users have no access to any of the application's views.

NOTE: Even if you disallow anonymous browsing, an unregistered user has access to an application's login page.

For information about working with views in Siebel applications, see *Siebel Tools Reference, MidMarket Edition*.

If you allow anonymous browsing, set the following parameter in the application's configuration file (for example, in `eservice.cfg`).

```
[SWE]
AllowAnonUsers = TRUE
```

Unregistered users are not allowed access to this Siebel application if this parameter value is `FALSE`.

For information about setting parameters in application configuration files, see [“Siebel Application Configuration File Parameters” on page 164](#).

Anonymous browsing is discussed in a usage context in [“Setting Up Security Adapter Authentication: A Scenario” on page 85](#).

Secure Views

You can require URLs to use HTTPS protocol for specific views in your Siebel application. The following factors determine whether the Siebel Web Engine verifies that requests for a view use the HTTPS protocol:

- The value (TRUE or FALSE) of the view's Secure attribute. For information about the Secure attribute for a view, see *Siebel Tools Reference, MidMarket Edition*.
- The value of the SecureBrowse parameter in the application's configuration file.

HTTPS is requested for views in the application whose Secure attribute is set to TRUE. If SecureBrowse is set to TRUE or to HTTPS, then HTTPS is requested for all views in the application.

If SecureBrowse is set to ServerDefault, then the Secure attribute setting is taken from Web server.

If you plan to use HTTPS protocol, remember the following:

- You can switch between secure and non-secure views in Siebel customer applications, but not in employee applications (such as Siebel Call Center). To make sure you have secure views in employee applications, set the value of SecureBrowse to TRUE.
- Your Web server must be configured to support HTTPS.

NOTE: For some browsers, even if you have SecureBrowse set to TRUE, the following message may appear when you access a Siebel application, “This page contains both Secure and Non Secure items. Do you want to download non secure items?” Despite this message, Siebel application requests will be processed on HTTPS, not HTTP.

Digital Certificate Authentication

For customers who have an existing PKI (Public Key Infrastructure) with client certificates, Siebel supports the use of X.509 certificates to authenticate users to an application. This is accomplished by using SSL with client authentication capabilities of its supported Web servers for certificate handling.

To implement X.509 digital certificate authentication, you must perform the tasks for implementing Web SSO authentication, as described in [“Implementing Web SSO Authentication” on page 106](#), with the following specific guidelines:

- Enter the following parameters in the [defaults] section of the eapps.cfg file:

```
SingleSignOn = TRUE
TrustToken = HELLO
ClientCertificate = TRUE
```

UserSpec = CERT_SUBJECT	For client authentication on Windows, use CERT_SUBJECT.
SubUserSpec = CN	This parameter value tells the application to extract the username from the certificate name.
UserSpecSource = Server	

- In the configuration file for each affected application, such as `eservice.cfg`, enter the following parameters in the sections indicated:

```
[SWE]
SecureBrowse = ServerDefault
[LDAP] (or other name for your security adapter's section)
SingleSignOn = TRUE
TrustToken = HELLO
```

For additional information about digital certificate implementation, see *Certificate-Based Authentication and Its Application in Siebel 7* on SupportWeb.

Configuration Parameters Related to Authentication

Configuration parameters specify the authentication strategies and options you implement to the Siebel Web Engine and to Siebel applications' object managers.

This section provides referential information about the parameters and procedures for setting their values. Topics that discuss implementing authentication strategies specify the values you should assign these parameters in different scenarios.

You set configuration parameters in the following locations:

- `Eapps.cfg` file
- The configuration file for each Siebel application's object manager
- The Siebel name server
- Siebel eBusiness Applications system preferences

Eapps.cfg Parameters

The SWEApp\bin\eapps.cfg file contains parameters used by the Siebel Web Engine to control all Siebel applications' interactions with the Web engine.

Following list is a portion of a sample eapps.cfg file. This sample includes parameters that may not coexist. They are provided so you can see the full range of authentication-related parameters.

```
[swe]
Language           = enu
Log                = all
LogDirectory       = D:\10638\SWEApp\log
ClientRootDir      = D:\10638\SWEApp
WebPublicRootDir   = D:\10638\SWEApp\public\enu
WebUpdatePassword = test

[defaults]
AnonUserName       = sadmin
AnonPassword       = sadminpw
AnonUserPool       = 1000
StatsPage          = _stats.swe

SingleSignOn       = TRUE
TrustToken         = HELLO
UserSpec           = REMOTE_USER
UserSpecSource     = Server

[/echannel]
AnonUserName       = echuser
AnonPassword       = ech
ProtectedVirtualDirectory = /p_echannel
ConnectString      = siebel.TCPIP.none.NONE://ecollab_bltz:2320/siebel
/eChannelObjMgr/ecollab_bltz
```

The eapps.cfg file includes a [defaults] section and sections for individual Siebel applications, for example [/echannel] and [/callcenter]. Each parameter value in the [defaults] section is used by individual applications unless you override the parameter's value with an entry in an application's own section. In the eapps.cfg sample above, the AnonUserName and AnonPassword values in the [/echannel] section are used by Siebel Partner Portal, MidMarket Edition instead of the values provided in the [defaults] section.

NOTE: You can use a text editor to add parameters and their values or to change values for existing parameters. When you edit configuration files, do not use a text editor that adds additional, non-text characters to the file. For example, use Microsoft Notepad instead of Microsoft Word or WordPad.

In a given eapps.cfg file, some parameters may not appear by default. Changes to the eapps.cfg file are not active until you restart the Siebel server and the Web server.

The following parameters in the eapps.cfg file relate to authentication. They can be implemented in the [defaults] section or in the sections for individual applications.

- **AnonUserName.** This parameter is the user name for an anonymous user that is stored in the directory and also in the Siebel database. This anonymous user provides binding between the directory and the application's object manager to allow a Siebel application home page to display to a user who has not logged in. Similarly, this anonymous user supplies a login so the user can see other pages for which you allow anonymous browsing. The home page that is displayed likely provides an interface for the user to log in.
- **AnonPassword.** This parameter is the authenticated password that is paired with AnonUserName.
- **AnonUserPool.** This parameter sets the maximum number of anonymous user connections that can provide access to login pages. The anonymous user pool applies to the brief, initial actions taken by the user on the login pages before logging in. After users log in, they have a separate connection.
- **SingleSignOn.** The Siebel Web Engine operates in Web SSO mode when TRUE.
- **TrustToken.** This token string is a shared secret between the Siebel Web Engine and the security adapter. It is a measure to protect against Web Engine spoofing attacks. This setting must be the same on both the Web engine and the security adapter.
- **UserSpec.** In a Web SSO implementation, this variable name specifies where the Web engine looks for a user's username within the source given by UserSpecSource. The value, REMOTE_USER by default, is populated by the authentication filter.

If digital certificate authentication is implemented on Windows, use the value CERT_SUBJECT, a variable that contains the certificate name. For example, UserSpec/SubUserSpec would be "CERT_SUBJECT"/"CN".

- **SubUserSpec.** In a Web SSO environment that implements digital certificate authentication, a value of CN specifies that the Siebel user ID should be extracted from the certificate's CN (Common Name) attribute.

- **UserSpecSource.** In a Web SSO implementation, this parameter specifies the source from which the Web engine derives the user credentials: Server, if from the usual Web server user name field; Header, if the variable is within the HTTP request header.
- **ClientCertificate.** When this parameter is set to TRUE in a Web SSO implementation, the user is authenticated through a digital certificate.

The following parameter can be included in the section for each individual Siebel application, but not in the [defaults] section:

- **ProtectedVirtualDirectory.** This parameter specifies the protected virtual directory for a Siebel application. This parameter specifies a Web server virtual directory that represents the protected location of the Siebel application. This parameter must have a value in a Web SSO implementation and is optional in other implementations. The protected directory allows you to configure your Web server or third-party authentication software to require user authentication to access specific Siebel application views. Requests for any views that require explicit login are redirected to this virtual directory.

Siebel Application Configuration File Parameters

A configuration file exists for each Siebel eBusiness application for each language. The parameters in the file determine how the user interacts with the application's object manager and with the security adapter.

The configuration file that controls a particular user session depends on the client with which a user connects.

- **Configuration file on the Siebel server.** For users connecting with the standard Web client, application configuration files are located in the siebsrvr\bin\language subdirectory on the Siebel root directory. For example, eservice.cfg is provided for Siebel eService for implementation in American English in the siebsrvr\bin\ENU directory.
- **Configuration file on the Siebel Dedicated Web Client.** For users connecting through the Siebel Dedicated Web Client, the configuration file is located in the \mwebc\bin\language subdirectory on the client's root directory. For example, eservice.cfg is provided for Siebel eService for implementation in American English in the \mwebc\bin\ENU directory. The Siebel Dedicated Web Client connects directly to the database; it bypasses the Siebel server.

The configuration file names for Siebel applications are listed in [“Siebel Application Configuration File Names” on page 343](#).

You can use a plain text editor to add parameters and their values or to change values for existing parameters. When you edit configuration files, do not use a text editor that adds additional, non text characters to the file. For example, use Microsoft Notepad instead of Microsoft Word or WordPad.

In a given configuration file, some parameters may not appear by default. Others may appear with a preceding semicolon (;), indicating that the parameter is a comment and is not being interpreted. The semicolon must be deleted to make the parameter active. Changes to an application configuration file are not active until you restart the Siebel server.

CAUTION: The parameter values that reference directory attributes that you provide for the Siebel LDAP and ADSI adapters are case sensitive. The values must match the attribute names in the directory.

The following parameters are authentication-related parameters that are present by default or can be added to each application’s configuration file. They are grouped by the labeled sections in which they occur. This listing does not include parameters in an application’s configuration file that are not authentication-related.

[SWE] section:

- **AllowAnonUsers.** (TRUE or FALSE) Unregistered users are not allowed access to this Siebel application if this parameter value is FALSE.
- **SecureLogin.** (TRUE or FALSE) If TRUE, the login form completed by the user is transmitted over secure socket layer (SSL). This requires that you have a certificate from a certificate authority on the Web server on which the Siebel Web Engine is installed.

- **SecureBrowse.** Views in the application whose Secure attribute is set to TRUE are navigated over SSL. When SecureBrowse is set to TRUE or to HTTPS, all views in the application are navigated over SSL.

CAUTION: Siebel customer applications support switching between secure and non-secure views, but employee applications (such as Siebel Call Center) do not. For more information, see [“Secure Views” on page 159](#).

NOTE: For some browsers, even if you have SecureBrowse set to TRUE, the following message may appear when you access a Siebel application, “This page contains both Secure and Non Secure items. Do you want to download non secure items?” Despite this message, Siebel application requests will be processed on HTTPS, not HTTP.

For information about the Secure attribute for a view, see *Siebel Tools Reference, MidMarket Edition*.

[SecurityAdapters] section:

- **Adapter Name, for example “LDAP”.** Each line you enter here refers to a section in this application’s configuration file that contains parameters for a particular security adapter. For example, the line LDAP = LDAP means this entry in the security adapters list, LDAP, points to an [LDAP] section that follows containing configuration parameters for a particular security adapter, such as the Siebel LDAP security adapter. The names you provide are arbitrary.

[*Adapter Name*] section, for example [LDAP]:

Each security adapter’s section, for example [LDAP] or [ADSI], corresponds to the right member of a line in the [SecurityAdapters] section. In each security adapter’s section the set of parameters configures how the security adapter is implemented.

Each authentication-related parameter in an application’s configuration file is interpreted by either the application’s object manager or by the Siebel LDAP security adapter, the Siebel ADSI adapter, or both. If you implement a non-Siebel security adapter, you must configure your adapter to interpret the parameters used by the Siebel adapters if you want to use those parameters.

For information about configuring a non-Siebel security adapter, see *Siebel Security Adapter Software Developers Kit 7* on the Siebel SupportWeb site.

Some parameters apply only in a Web SSO authentication environment.

- **DllName.** This parameter is interpreted by the application object manager. It is the DLL that implements the security adapter API required for integration with Siebel eBusiness applications. For example, `sscldap.dll` implements the Siebel LDAP adapter in a Windows implementation.
- **ServerName.** This parameter is interpreted by Siebel security adapters. It is the name of the machine on which the LDAP or ADS server runs, for example `ldapserversiebel.com`.
- **Port.** This parameter is interpreted by the Siebel LDAP security adapter only. It is the port on the server machine that is used to access the LDAP server. Typically, use 389, the default value, for standard transmission or use 636 for secure transmission. You set the port at the ADS directory level, not as a configuration parameter.
- **BaseDN.** This parameter is interpreted by Siebel security adapters. The Base Distinguished Name is the root of the tree under which users of this Siebel application are stored in the directory. Users can be added directly or indirectly below this directory. A typical entry for an LDAP server might be `BaseDN = "ou=people, o=domain name"`. "o" denotes "organization" and is typically your Web site's domain name. "ou" denotes "organization unit" and is the subdirectory in which users are stored.

A typical entry for an ADS server might be `BaseDN = "CN=Users, DC=qatest, DC=siebel, DC=com"`. Domain Component (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for the user objects in the directory. Therefore, adjust the number of CN and DC entries to represent your architecture.

- **UsernameAttributeType.** This parameter is interpreted by Siebel security adapters. It is the attribute type under which the user's login name is stored in the directory. For example, if `UsernameAttributeType = uid`, then when a user attempts to log in with username HKIM, the security adapter searches for a record in which the uid attribute has the value HKIM. This attribute is the Siebel user ID, unless the `UseAdapterUsername` parameter is TRUE.

NOTE: If you implement an adapter-defined user name (`UseAdapterUsername = TRUE`), then you must set the OM - Username BC Field Name Server parameter appropriately to allow the directory attribute defined by `UsernameAttributeType` to be updated from the Siebel client. For more information about implementing an adapter-defined user name, see [“Adapter-Defined User Name” on page 154](#).

- **PasswordAttributeType.** This parameter is interpreted by the Siebel LDAP security adapter. It is the attribute type under which the user's login password is stored in the directory. For example, if `PasswordAttributeType = userPassword`, then when a user with username HKIM attempts to log in, the security adapter compares the value in the `userPassword` attribute for HKIM with the password the user enters.

ADS does not store the password in an attribute, so this parameter is not used with the Siebel ADSI adapter.

- **CredentialsAttributeType.** This parameter is interpreted by Siebel security adapters. It is the attribute type that stores a database account. For example, if `CredentialsAttributeType = dbaccount`, then when a user with username HKIM is authenticated, the security adapter retrieves the database account from the `dbaccount` attribute for HKIM.

- This attribute value must be of the form `username=U password=P type=T`, where *U* and *P* are credentials for a database account. The type value *T* is the name of a data source, such as `server` or `sample`, and is case-insensitive. There may also be a single credential of the form `username=U password=P`. This default credential is used when a user tries to connect to a data source for which no credential has a matching type value. There may be any amount of white space between the two `key=value` pairs and no space within each pair. The keywords `username`, `password`, and `type` must be lowercase.

NOTE: If you implement LDAP or ADSI security adapter authentication to manage the users in the directory through the Siebel client, then the value of the database account attribute for a new user is inherited from the user who creates the new user. The inheritance is independent of whether you implement a shared database account, but does not override the use of the shared database account. For information on shared database accounts, see [“Shared Database Account” on page 153](#).

- **RolesAttributeType.** This parameter is interpreted by Siebel security adapters. It is the attribute type for roles stored in the directory. For example, if `RolesAttributeType = roles`, then when a user with username `HKIM` is authenticated, the security adapter retrieves the user’s Siebel responsibilities from the roles attribute for `HKIM`.

Responsibilities are typically associated with users in the Siebel database, but they can be stored in the database, in the directory, or in both. The user gets access to all of the views in all of the responsibilities specified in both sources. However, it is recommended that you define responsibilities in the database or in the directory, but not in both places.

- **SslDatabase.** This parameter is interpreted by the Siebel LDAP security adapter only. It determines whether a secure sockets layer (SSL) is used for communication between the LDAP adapter and the directory. If empty, SSL is not used. If not empty, its value must be the absolute path of a Netscape `cert7.db` file that contains a certificate for the certificate authority that is used by the LDAP server.

- **UseSSL.** (TRUE or FALSE) This parameter is interpreted by the Siebel ADSI security adapter only. If it is set to TRUE, a secure sockets layer (SSL) is used for communication between the ADSI adapter and the ADS directory, otherwise SSL is not used.
- **EncryptCredentialsPassword.** (TRUE or FALSE) This parameter is interpreted by the application object manager. If TRUE, the database password in the directory for an authenticated user is encrypted by a Siebel-provided utility before being sent to the object manager. The encrypted version is the valid database login password. This parameter's default value is FALSE.
- **ApplicationUser.** This parameter is interpreted by Siebel security adapters. It is the user name of a record in the directory with sufficient permissions to read any user's information and do any necessary administration.

If this parameter value is not empty, this user provides the initial binding of the LDAP or Active Directory server with the object manager when a user requests the login page, else anonymous browsing of the directory is required.

You enter this parameter as a full distinguished name (DN), for example "uid=APPUSER, ou=People, o=companyname.com", including quotes, for LDAP. The security adapter uses this name to bind.

It is strongly recommended that you implement an application user.

- **ApplicationPassword.** This parameter is interpreted by the Siebel LDAP and ADSI security adapters. It must match the password in the directory for the user defined by the ApplicationUser parameter.

In an LDAP directory, the password is stored in an attribute. In ADS, the password is stored using ADS user management tools. It is not stored in an attribute.

- **EncryptApplicationPassword.** (TRUE or FALSE) This parameter is interpreted by Siebel security adapters. If TRUE, the password in the ApplicationPassword parameter is compared with an encrypted version of the password for the application user in the directory.
- **SingleSignOn.** (TRUE or FALSE) This parameter is interpreted by the application object manager. If TRUE, the security adapter is used in Web SSO mode, instead of using security adapter authentication.

- **TrustToken.** This parameter is interpreted by Siebel security adapters. It applies only in a Web SSO environment. The adapter compares the TrustToken value provided in the request with the value stored in this application configuration file. If they match, the object manager accepts that the request has come from the Siebel Web Engine, that is, from a trusted Web server. This parameter's default value is an empty string.
- **SharedCredentialsDn.** This parameter is interpreted by Siebel security adapters. It is the absolute path (not relative to the BaseDN) of an object in the directory that has the shared database account for the application. If empty, the database account is looked up in the user's DN as usual. If not empty, then the database account for all users is looked up in the shared credentials DN instead. The attribute type is still determined by CredentialsAttributeType. For example, if SharedCredentialsDn = "uid=HKIM, ou=People, o=siebel.com", then when any user is authenticated, the security adapter retrieves the database account from the appropriate attribute in the HKIM record. This parameter's default value is an empty string.
- **UseAdapterUsername.** (TRUE or FALSE) This parameter is interpreted by the application object manager. If TRUE, this parameter indicates that when the user key passed to the security adapter is not the Siebel user ID, the security adapter retrieves the Siebel user ID for authenticated users from an attribute defined by the SiebelUsernameAttributeType parameter. The default value for the UseAdapterUsername is FALSE.
- **SiebelUsernameAttributeType.** This parameter is interpreted by the Siebel security adapters. If UseAdapterUsername = TRUE, this parameter is the attribute from which the security adapter retrieves an authenticated user's Siebel user ID. If this parameter is left empty, the username passed in is assumed to be the Siebel user ID.
- **UseRemoteConfig.** This parameter is interpreted by the application object manager. It is the path to a configuration file that contains only parameters for a security adapter, that is, it contains parameters as they would be formatted if they were included in a section such as [LDAP] in an application's configuration file. The parameter values in the remote configuration file override those in the same section in the application's configuration file. You must provide the path in universal naming convention (UNC) format, that is, \\server\vol\path\filename.cfg.

Siebel Name Server Parameters

Siebel name server parameters can be set at one or more of the enterprise, server, or component levels. They are set in the Server Administration screen of a Siebel employee application such as Siebel Call Center.

Parameters you set at the enterprise level configure all object managers throughout the enterprise. Parameters set at the server level configure all object managers on a specific Siebel server. Parameters set at the component level configure all the tasks, or instances, of a specific component. For purposes of authentication, all of the components of interest are application object managers, such as the Call Center object manager or the eService object manager.

A particular parameter set at a lower level overrides the same parameter set at a higher level. For example, if `Security Adapter Name = LDAP` at the enterprise level, and `Security Adapter Name = ADSI` at the component level for the eService Object Manager component, then the ADSI security adapter is used for Siebel eService.

Table 14 lists the authentication-related parameters in the name server.

Table 14. Siebel Name Server Parameters

Subsystem	Parameter	Description	Set at Enterprise Level	Set at Server Level	Set at Component Level
Object Manager	OM - Configuration File	Name of an application's (object manager) configuration file, such as <code>eservice.cfg</code> , from which other parameter values are applied, as described in "Siebel Application Configuration File Parameters" on page 164 .	X	X	X
	OM - Data Source	The data source, such as <code>ServerDataSrc</code> , in the file specified by OM - Configuration File, to which these parameters apply.	X		X
	OM - Proxy Employee	User ID of the proxy employee. For information about the proxy employee, see "Seed Data" on page 345 .	X	X	X

Table 14. Siebel Name Server Parameters

Subsystem	Parameter	Description	Set at Enterprise Level	Set at Server Level	Set at Component Level
	Security Adapter Name	The name of the security adapter you implement, as it appears as a section in the application configuration file defined by the OM-Configuration File. For example, enter <code>LDAP</code> if the section of security adapter parameters is the [LDAP] section.	X	X	X
	OM - Username BC Field	This parameter is used only if you implement an adapter-defined username. It specifies the field of the User business component that populates the attribute in the directory defined by the UsernameAttributeType parameter in the application's configuration file. That is, when the user ID (LoginName field in the User business component) is not the identity key, this field is. If this parameter is not present in the parameters list, you must add it.	X	X	X

Table 14. Siebel Name Server Parameters

Subsystem	Parameter	Description	Set at Enterprise Level	Set at Server Level	Set at Component Level
Infrastructure Objmgr configu	Application Encrypt Password	If TRUE in a database authentication environment, the password entered by the user at login is encrypted before being passed to the database. If TRUE in an external authentication environment, the password entered by the user or passed to the SWSE by a third-party authentication client is encrypted before being compared with the password stored for the user in the directory. When enabled, a Siebel-supplied encryption algorithm is applied to the password before it is used to authenticate. To function properly, the database account or directory password with which it is compared must also be set up with the encrypted version of the password.		X	X

To set name server parameters

- 1 Log in to a Siebel employee application, such as Siebel Call Center, and make one of the following choices from the application-level menu:
 - To set enterprise level parameters, choose View > Site Map > Server Administration > Enterprise Configuration.
 - To set server level parameters, choose View > Site Map > Server Administration > Servers.
 - To set component level parameters, View > Site Map > Server Administration > Components.
- 2 If you are setting parameters at the server or component level, select the applicable server or component.

- 3 Do one of the following:
 - To set enterprise level parameters, click the Enterprise Parameters view-level tab.
 - To set server level parameters, click the Server Parameters view-level tab.
 - To set component level parameters, click the Component Parameters view-level tab.
- 4 Select a parameter record, edit the Current Value field, and then click Save.
- 5 Restart the Siebel server before the changes take effect.

System Preferences

You can set various authentication-related system preferences for Siebel applications in the Applications Administration screen. System preferences are enterprise-wide settings.

Following are authentication-related system preferences:

- **SecExternalUserAdministration.** (TRUE or FALSE) In a security adapter authentication architecture, you must set this preference to FALSE to allow administration of the directory through Siebel applications. When an administrator then adds a user or changes a password from within a Siebel application or a user self-registers, the change is propagated to the directory.

NOTE: A non Siebel security adapter must support the SetUserInfo and ChangePassword methods to allow dynamic directory administration. For information about implementing a non-Siebel security adapter, see *Siebel Security Adapter Software Developers Kit 7* on the Siebel SupportWeb site.

- **SecThickClientExtAuthent.** (TRUE or FALSE) You must set the SecThickClientExtAuthent system preference to TRUE to allow security adapter authentication for users who log in through the Siebel Dedicated Web Client. This system preference has no effect on security adapter authentication for users who log in on a Web client.

- **Security Adapter CRC.** You can implement checksum validation to verify that each user gains access to the database through the correct security adapter. This preference contains the value calculated by the checksum utility for the applicable security adapter DLL. If you leave this value empty, the system does not perform the check. If you upgrade your system, you must recalculate and replace the value in this system preference.

For information about checksum validation, see [“Checksum Validation” on page 149](#).

To edit a system preference

- 1** Log in as an administrator to a Siebel employee application.
- 2** Navigate to the Application Administration screen.
- 3** From the Show drop-down list, choose System Preferences.
The System Preferences list appears.
- 4** Select a system preference to edit.
- 5** Edit the entry in the System Preference Value column, and then step off of the record to save it.
- 6** Restart the Siebel server.

Login Features

This section describes features and considerations associated with user login to Siebel applications.

A login page or a login form embedded in a Siebel application page is the means by which user credentials are collected. [Figure 12](#) shows a login form embedded in the Siebel eService home page.



The screenshot displays the Siebel eService home page. At the top, there is a "Welcome to Siebel Support!" message with a small image of two people. Below this, a navigation bar contains "Service & Support". The main content area is divided into two sections: "User Log In" and "My Account".

User Log In

- *User ID: [Text Input Field]
- *Password: [Text Input Field]
- Remember User ID and Password
- [OK Button]
- [Forgot Your Password?](#)
- [New User](#)

My Account

- [Check My Order Status](#)
Track whether an order has shipped
- [Check My Service Requests](#)
Track the status of my service requests
- [Submit a Service Request](#)
Get fast, convenient support for products
- [Register My Product](#)
Register a product and receive updates and

Figure 12. Embedded Login Form

A user is required to login, thereby identifying himself or herself as a registered user, to be allowed access to protected views in Siebel applications. Protected views are designated for explicit login. Views that are not designated for explicit login are available for anonymous browsing, if the Siebel application allows anonymous browsing.

For information about setting view properties, see *Siebel Tools Reference, MidMarket Edition*.

For information about anonymous browsing, see [“Anonymous Browsing” on page 159](#).

Siebel applications also provide other features on a login form besides user credentials collection, such as remembering a user name and password and providing forgotten password support.

Alternatively, you can configure a Siebel application to bypass the login form by providing the required user ID and password in the URL that accesses the application.

Remember My User ID and Password

A user can check the Remember My User ID and Password check box when logging in to a Siebel application. By doing so, the user can access the same Siebel application through other browser instances without having to log in again. The functionality is available only during the current Web session.

Remember My User ID and Password uses the auto login cookie that the Siebel Web Engine provides when a session is started. This functionality requires that cookies are enabled.

For information about cookies and session management, see [“Cookies and Session Management” on page 181](#).

Forgot Your Password?

Forgot Your Password? allows a user who has forgotten the login password to get a new password. A seed workflow process provides interactive questions by which the user identifies himself or herself.

For information about Forgot Your Password?, see [“Forgot Your Password?” on page 212](#).

Account Policies

For enhanced security, you may want to implement the following account policies. Account policies are functions of your authentication service. If you want to implement account policies, you are responsible for setting them up through administration features provided by the authentication service vendor.

- Password syntax rules, such as minimum password length. When creating or changing passwords, minimum length requirements and other syntax rules defined in the external directory will be enforced by the Siebel application.
- An account lockout after a specified number of failed attempts to log in. Account lockout protects against password guessing attacks. Siebel applications support lockout conditions for accounts that have been disabled by the external directory.
- Password expiration after a specified period of time. The external directory can be configured to expire passwords and warn users that passwords are about to expire. Password expiration warnings issued by the external directory will be recognized by Siebel applications and users will be notified to change their passwords.

URL Login

Users can log in to a Siebel application by presenting user credentials as parameters in a URL. The user does not have to manually type credentials into a login form.

CAUTION: By using URL login, user passwords are transmitted in clear text over the network.

The easiest, but least secure option for a form of Web SSO to Siebel applications is to make explicit login requests to a Siebel customer or partner application from navigational entry points to the application. This option works best if the number of navigational entry points to the Siebel application is small, if you are not concerned about users knowing their Siebel username and password, and if you are not deploying a full Web SSO infrastructure.

Following is a sample showing the URL syntax:

```
http://yourhost/eservice/  
start.swe?SWECmd=ExecuteLogin&SWEUserName=HKIM&SWEPassword=HKIM
```

NOTE: The parameter names in the URL are case-sensitive.

You can create a single URL that contains a path to a predefined view in addition to a users login credentials. You must use SWEAC as shown in the following example. This example shows a drilldown to a particular service request, after the user is logged in.

```
http://siebel.com/echannel/  
start.swe?SWECmd=ExecuteLogin&SWEUserName=%47%55%45%53%54&SWEPassword=%47%55%45%53%54&SWEAC="SWECmd=InvokeMethod,SWEMethod=Drilldown,SWEView=Service+Request+List+View+(SCW),SWEApplet=Service+Request+List+Applet+(SCW),SWEField=l_SR+Number,SWERowIds=SWERowId0%3d1-15P"
```

NOTE: You must use commas instead of ampersands (&) as delimiters between arguments in an SWEAC expression.

Cookies and Session Management

Four cookies are generated dynamically by the Siebel Web Engine when a Web session starts:

- Session cookie
- Auto login cookie
- SSO for reports cookie
- Mode cookie

The Siebel Web Engine generates cookies as a default feature. No configuration is required. You should not modify any of the cookies.

If a browser does not support cookies or a user disables cookies, Siebel Web Engine manages the session in cookieless mode. You can configure Siebel Web Engine to function in cookieless mode for all sessions.

Session Cookie

The session cookie manages the Web session for a Siebel Web application.

- **Cookie name.** `_sn`
- **Applications.** Siebel employee, partner, and customer applications
- **Format.** `Session ID`
- **Consequence if cookies are disabled.** Siebel Web Engine supports cookieless sessions. The session ID becomes part of the URL.

For information about cookieless sessions, see [“Cookieless Sessions” on page 182](#).

Auto Login Cookie

The auto login cookie underlies the Remember My User ID and Password feature. Encrypted user information is collected to a desktop cookie. If the user subsequently accesses the application URL through another browser, the user information is provided to the application so the user does not have to login again.

- **Cookie name.** start.swe
- **Applications.** Siebel employee, partner, and customer applications
- **Format.** start.swe = *encrypted user information*
- **Consequence if cookies are disabled.** Auto login does not work in cookieless mode.

Cookieless Sessions

A Web session can be managed without cookies. In cookieless mode, the session management information for each page is included in its URL.

Functionality provided by the auto login cookie is not available in cookieless mode.

A cookieless session is invoked when the browser does not send back a session cookie to the Siebel Web Engine. This event can be caused by cookies being disabled by the user or by a browser that does not support cookies.

You may want a Siebel application to function in cookieless mode for all sessions for reasons such as security requirements that do not permit cookies. You can set a Siebel application to function in cookieless mode by setting the URLSession parameter to TRUE for the application in the eapps.cfg file. For information about setting parameter values in the eapps.cfg file, see [“Editing Parameter Values in the eapps.cfg File” on page 118](#).

This section provides information about registering and administering users of Siebel employee, partner, and customer applications.

Overview of User Registration

A user who is not a registered Siebel application user has no authenticated access to the database. Depending on the Siebel application, unregistered users have various levels of access. Minimally, the user can access a login page. By default or by your configuration, unregistered users may have access to some or all of the views of a particular Siebel application.

You typically grant registered users more access to data and features than you grant unregistered users. A user can be registered for some or for all of your Siebel applications. You can grant different registered users different levels of access to the database and features.

Typically, a user is registered when the following tasks are performed.

- Create a user record in the Siebel database.
- Provide the means for the user to be authenticated at login.

Depending on the Siebel application, a user can be registered in one or more of the following ways:

- **Self-registration.** The user can self-register at the Web site.
- **Internal registration.** An administrator at your host company can register users.
- **External registration.** A delegated administrator (a user at a customer or partner company) can register users.

If you implement an external authentication system, then adding a user to the Siebel database, whether by self-registration or by an administrator, may or may not propagate the user's login data to the external authentication system. If the login credentials do not propagate to the authentication system, then you must create the login credentials separately in the authentication system.

If you implement database authentication, then adding the user to the database with the user's user ID and password is enough to allow the user to be authenticated.

For more information about authentication and propagation of user data, see [“User Authentication” on page 63](#).

Requirements

You must complete the following implementations before you can register users:

- Install your Siebel applications.
- Setup and configure your user authentication architecture.
- Create database accounts for users as required by your authentication architecture.

For information about user authentication, see [“User Authentication” on page 63](#).

Seed Data

When you install your Siebel eBusiness Applications, you are provided seed data that is related to user registration, to authentication, and to user access to Siebel applications. The seed data includes users, responsibilities, positions, an organization, and a database login. References to the seed data appear throughout this section.

For detailed information on seed data and for procedures for viewing and editing seed data, see [“Seed Data” on page 345](#).

Unregistered Users and Anonymous Browsing

Several Siebel applications allow anonymous browsing of views intended for public access as default functionality. Anonymous browsing typically applies to Siebel customer and partner applications, not employee applications. However, you can configure any Siebel application to either allow or disallow anonymous browsing.

Unregistered users gain access to application views and the database through the anonymous user. The anonymous user is a record in the Siebel database that also performs functions during user authentication and user self-registration. If you implement an external authentication system, the anonymous user has a corresponding record in the user directory.

The anonymous user is required even if your applications do not allow access by unregistered users. When the Object Manager first starts up, it uses the anonymous user account to connect to the database and retrieve information (such as a license key) before presenting the Login screen. For information about the anonymous user's role in user authentication, see [“User Authentication” on page 63](#).

Implementing Anonymous Browsing

To make views accessible to unregistered users, you must perform the following tasks:

- Modify the anonymous user record.
- Set configuration parameters.
- Modify views.

For Siebel applications for which anonymous browsing is implemented by default, you should confirm that these tasks are done.

Modifying the Anonymous User Record

The anonymous user is a record in the Siebel database and, if you implement external user authentication, a corresponding record in the external directory of users. The anonymous user is a component in user authentication, anonymous browsing, and self-registration. For applications that allow anonymous browsing, the anonymous user provides visibility of the pages for which you allow anonymous browsing.

You should set up your user authentication architecture before configuring an application for user access. Therefore, the anonymous user should already exist in your Siebel database and in your directory.

The responsibility that is assigned to a user record in the database contains a list of views to which the user has access. You must confirm that the anonymous user that you use for your Siebel application includes an appropriate responsibility so that unregistered users can see the views you intend them to see.

If you choose to use a seed anonymous user in your authentication setup, then you should verify that its seed responsibility includes the views you want to provide for anonymous browsing. For example, if you use the GUESTCST seed user for a Siebel customer application, then you should verify that its responsibility, Web Anonymous User, includes the required views. If the responsibility does not include your required views, then you can do one of the following:

- Create one or more additional responsibilities that include missing views, and then add the responsibilities to the existing seed responsibility in the anonymous user's multi-value Responsibility field. The user has access to all the views in all the assigned responsibilities.
- Copy the seed responsibility record, add missing views to the copy, and replace the responsibility in the anonymous user record with the modified responsibility.

NOTE: You cannot directly modify a seed responsibility.

For information about creating a responsibility or adding views to a responsibility, see [“Access Control” on page 247](#).

For information about assigning a responsibility to a user, see [“Internal Administration of Users” on page 224](#).

For information about seed data, see [“Seed Data” on page 345](#).

Setting Configuration Parameters

You must set the following configuration parameters to allow anonymous browsing.

- **AllowAnonUsers.** Set this parameter in the Siebel application's configuration file to TRUE.

For information about setting parameter values in application configuration files, see [“Siebel Application Configuration File Parameters” on page 164](#).

- **AnonUserName.** This parameter is the user name for an anonymous user that is stored in the directory and also in the Siebel database. This anonymous user provides binding between the directory and the application's object manager to allow a Siebel application home page to display to a user who has not logged in. Similarly, this anonymous user supplies a login so the user can see other pages for which you allow anonymous browsing.
- **AnonPassword.** This parameter is the authenticated password that is paired with AnonUserName.

Modifying Views to Allow or Disallow Anonymous Browsing

Even when a view is included in the responsibility for the anonymous user, the view is not accessible to unregistered users if the view is designated for "explicit login." A view that is designated for explicit login requires the viewer to be a registered user who has been authenticated.

The following procedure is intended to present the main steps in a Siebel Tools task. For detailed information about modifying view properties in Siebel Tools, see *Siebel Tools Reference, MidMarket Edition*.

To set or remove the explicit login requirement for a view

- 1** Open Siebel Tools.
- 2** In Object Explorer, select the View object.
The Views list appears.
- 3** Select a view.
- 4** Choose Tools > Lock Project.
- 5** Check the Explicit Login field to set the view for explicit login or remove the check to allow anonymous browsing.
- 6** Recompile the Siebel repository file, and unlock the project.

Self-Registration

Several Siebel applications allow users to self-register as a default functionality.

This section observes the following principles about self-registration functionality that is provided by default with your Siebel applications:

- Self-registration applies to Siebel customer applications.
- Self-registration can be implemented only in Siebel applications whose clients use standard interactively. It cannot be implemented for Siebel employee applications or for any other Siebel application that uses the high interactively client.
- You implement security adapter authentication with Siebel applications for which you allow self-registration.

To implement self-registration for applications that use Web SSO user authentication, you are responsible for configuring the self-registration functionality at the Web site level and for synchronizing the user data with the Siebel database. Configuration guidelines are not provided in Siebel applications documentation. Self-registration is not feasible when you implement database authentication.

NOTE: If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel applications, including user self-registration. For information about user authentication, see [“User Authentication” on page 63](#).

Self-registration functionality for Siebel customer applications is included in your Siebel eBusiness Applications installation.

The End User Experience for Self-Registration

The self-registration experience for end users varies, depending on the application. Some application-specific capabilities are:

- **Siebel eService.** A user self-registers to gain access to more services.
- **Siebel eSales.** A user self-registers to be allowed to make an online purchase.

To self-register

- 1 The user clicks New User on a Siebel application page.

The Personal Information form appears.

- 2 The user completes the form using the following guidelines, and then clicks Next.

Field	Entry
First Name	Required.
Last Name	Required.
User ID	Required. This contiguous character string is stored as the user ID in the User record. Depending on how you configure authentication, the user may or may not use this entry as a login name.
Password	Required. The user uses this password to log in. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. The user enters this password to log in. It must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form.
Verify Password	Required.
Challenge Question	Required. The user enters a phrase for which there is an "answer." If the user clicks Forgot Your Password?, this phrase is displayed, and the user must enter the correct answer to receive a new password.
Answer to Challenge Question	Required. The user provides a word or phrase that is considered the correct answer to the challenge question.

The Contact Information form appears. The fields on this form vary depending on the application.

- 3** The user completes the Contact Information form, and then clicks a button at the bottom of the form to continue. The names and number of buttons vary depending on the application.
- 4** If the application is Siebel eSales, then the user must complete forms that collect payment and address information.
- 5** On the Usage Terms form, the user must agree to the terms of the license agreement to be registered.

The Registration Confirmation message appears.

Implementing Self-Registration

Several components comprise the self-registration feature:

- Siebel seed workflow processes provide a sequence of interactive forms to the user for collecting the new user's data. These processes also validate data and write much of the data to the new User record in the Siebel database.
- Some fields in the new User record in the database are populated automatically from fields in the anonymous user record.
- A new record is created in the user directory. The security adapter authenticates the user against this record. Fields are populated automatically from the data the user enters to the forms.

You must perform one or more of the following tasks to implement self-registration:

- (Optional) Modify the anonymous user record.
- Set configuration parameters.
- Activate workflow processes for self-registration.

Modifying the Anonymous User Record

The anonymous user is a record in the Siebel database and a corresponding record in the user directory. The anonymous user is a component in user authentication, anonymous browsing, and self-registration.

Your user authentication architecture should be set up before configuring an application for user access. Therefore, the anonymous user should already exist in your Siebel database and in your user directory.

For information about user authentication, see [“User Authentication” on page 63](#).

Different Siebel applications in the same implementation may use different anonymous users. [“Seed Data” on page 345](#) describes seed data users, responsibilities, and the Siebel applications for which they are designed.

When a user self-registers, a new record is created in the User Registration business component. The User Registration business component is based on the same tables as the User business component, so a new User record is essentially created.

The following key fields are populated automatically from fields in the anonymous user’s record in the Siebel database:

- **Responsibility.** The new user’s responsibility is inherited from the anonymous user’s New Responsibility field. A user’s responsibility is the list of views to which the user has access.
- **New Responsibility.** The new user’s New Responsibility field value is also inherited from the anonymous user’s New Responsibility field. The New Responsibility field is not used by regular registered users. Several Siebel applications allow customer or partner users to be upgraded to delegated administrators. A delegated administrator can register other users, who inherit their responsibility from the delegated administrator’s New Responsibility field.

The New Responsibility field is a single-value field. Therefore, if the seed responsibility in the New Responsibility field of your anonymous user does not provide all the views you require for self-registering users, you must do one of the following tasks:

- Replace the New Responsibility with a responsibility you create.
- Copy the seed responsibility record, add missing views to the copy, and replace the New Responsibility with the modified responsibility.

NOTE: You cannot directly modify a seed responsibility.

For information about creating a responsibility or adding views to a responsibility, see [“Access Control” on page 247](#).

For information about seed data, see [“Seed Data” on page 184](#).

Setting Configuration Parameters

The user directory can be administered through Siebel applications if you implement security adapter authentication. Changes such as adding a user or changing a password by an internal administrator, a delegated administrator, or when a user self-registers are propagated to the user directory.

You must set the following parameter for user data, including user name and password, to propagate to the user directory when users self-register:

- **SecExternalUserAdministration.** Set this Siebel system preference to FALSE to allow administration of the user directory through the Siebel Web client.

For information about the functions of Siebel system preferences and the procedure for setting them, see [“System Preferences” on page 175](#).

NOTE: If you do not configure your security adapter authentication architecture to allow administration through the Siebel Web client as described here, then you must manually create a record in the user directory whenever a new user of this application is created in the Siebel database.

Activating Workflow Processes

When you install your Siebel eBusiness Applications, you are provided the following workflow processes that control self-registration for several Siebel applications. These workflow processes together present a sequence of forms for the user to complete, perform data validation, and invoke database operations.

- **User Registration Initial Process.** For purposes of self-registration, this process is invoked when a user clicks New User on the login form or clicks Check Out during the buying process in Siebel eSales. This process is also invoked by clicking Forgot Your Password? on the login form. The process branches to one of the following subprocesses:
 - User Registration Process
 - User Registration Forgot Password Process

- **User Registration Process.** This is the main self-registration process. It updates the database, including:
 - Creating a new User record
 - Checking for a duplicate User record
 - Updating the existing User record with new information if a duplicate record is found
- **User Registration SubProcess.** This process is a subprocess to User Registration Process. It performs all of the information gathering and validation. The validated information includes:
 - A duplicate user ID does not exist in the database.
 - The Password and Verify Password entries are identical.
 - All required fields are completed.

To view workflow processes

- 1** From a Siebel employee application such as Siebel Call Center, navigate to the Business Process Administration screen.
- 2** From the Show drop-down menu, choose Workflow Processes.
The Workflow Processes list appears.
- 3** In the Workflow Processes list, scroll or query to find and select a workflow process.
- 4** Do one of the following, depending on the information about the process you want to see:
 - Click the Process Designer view tab to see a flow chart of the process. You can double-click a step to see its properties.
 - Click the Process Properties view tab to see any property in this workflow process.

The registration workflow processes branch at various stages depending on these cases:

- The application is Siebel eSales.

- The application is either Siebel eService or Siebel eCustomer, MidMarket Edition, which make up the default case.

Table 15 lists the views specified in the workflow processes that provide interactive forms during self-registration.

Table 15. Self-Registration Workflow Views

View Name	Applications that Use this View	Description
User Registration Initial Form View User Registration Password Error Msg View User Registration Missing Info Msg View User Registration Login Error Msg View User Registration Legal Confirmation View User Registration Confirmation Msg View User Registration Declined View	All	These views, common to all applications that use the User Registration Process, comprise two groups: <ul style="list-style-type: none">■ Personal Information form and messages resulting from flawed entries or a duplicate user ID with an existing user record■ Usage Terms form and messages resulting from accepting or declining to agree
User Registration Contact Information View	Default	This view is the Contact Information form used by default.
User Registration Contact Information View (eSales)	eSales	This view is the Contact Information form used by eSales.

For the self-registration workflow processes to be invoked, they must have the Active status.

To activate a workflow process

- 1 From a Siebel employee application such as Siebel Call Center, choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.

- 2 In the Workflow Processes list, scroll or query to find and select a workflow process.

If the process has status Active, then you do not have activate it.

- 3 To activate a workflow process, it must have the In Progress status. If the status is not In Progress, click Revise.

A workflow process of the same name, but with an incremental version number, is created and selected. The original workflow process is given an Outdated status.

- 4 Click Activate.

The new process is given the Active status. It is the only version of this process that has the Active status, and it is the version that is invoked.

- 5 Click Save.

Modifying Self-Registration Views and Revising Workflow Processes

You can modify existing views in a self-registration workflow process or create new views as required by your business rules. You can modify the seed workflow processes that are used for self-registration.

You can modify the default self-registration functionality in several ways. You can do one or more of the following tasks:

- Replace the license agreement text
- Revise a workflow process, including creating custom business services
- Redefine the fields the user is required to complete
- Add or delete fields in a view
- Change the physical appearance of a view or applet, such as moving fields or changing colors
- Create a new view
- Modify user deduplication

Modifying self-registration views, applets, and workflow processes include standard processes common with modifying other views, applets, and workflow processes. However, you should understand the way that data is collected by the User Registration business component and is written to the database before you do any modifications.

The views used in the self-registration workflow processes are based on the User Registration business component. The User Registration business component and the User business component are both based on the S_PARTY, S_CONTACT, and S_USER database tables. Therefore, writing a record through the User Registration business component is equivalent to writing a record through the User business component. In either case, a new user is created.

The User Registration business component allows collecting data into virtual fields. For most applications that use the self-registration workflow processes, no data is written to the database until all stages of collecting user data are completed. This process provides the following benefits:

- If the self-registration process is terminated before completion, there is no need to perform the time-consuming process of undoing a new, partially written record in the database. This process requires searching several tables.
- User record duplication can be prevented before a record is written.

Replacing the License Agreement Text

You can replace the default license agreement that appears to the self-registering user in the User Registration Legal Confirmation View.

The DotCom Applet License Base 1 Column Web template includes the Web template file with the name DotCom Applet Form Base 1 Column which is the file of name dCCAppletLicenseBase1Col.swt. The license agreement is contained in the dCCAppletLicenseBase1Col.swt file following the phrasing <!--This is where we include the html license agreement-->. You can replace the license agreement text.

For information about working with Web templates, see *Siebel Tools Reference, MidMarket Edition*.

Revising a Workflow Process

The self-registration workflow processes for your business scenario may require that you do revisions to the seed self-registration workflow processes, such as:

- Replace or insert a view
- Insert or delete a step
- Modify a step

You cannot directly modify a seed workflow process, such as any of the self-registration processes. Instead, you must create a copy of the process, and then revise the copy.

By convention, to avoid renaming processes, you can use the Revise button to make a copy of the same name, but with an incremented version number. All other processes of the same name are assigned Outdated status, so that the new version can be the only active version. This convention is recommended for revising any workflow process, not just seed processes.

To create a revised copy of a workflow process

- 1** In a Siebel employee application, such as Siebel Call Center, log in as an administrator, and then from the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.

- 2** Select a workflow process.

NOTE: You cannot revise a workflow process whose status is In Progress. This status indicates that the workflow process is being modified.

- 3** Click Revise.

A new workflow process record appears with the same name as the original process and with a version number one greater than the highest existing version number for that process.

For information about Workflow, see *Siebel Business Process Designer Administration Guide, MidMarket Edition*.

Creating Custom Business Services

Siebel applications provides predefined business services that you can use in a step of a workflow process. You can also script your own custom business services and then run them in workflow process steps.

For information about predefined business services and creating business services, see *Siebel Tools Reference, MidMarket Edition*.

For information about running business services in workflow processes, see *Siebel Business Process Designer Administration Guide, MidMarket Edition*.

Redefining Required Fields

As default functionality, a user who is self-registering is required to provide entries in certain fields. These fields may differ depending on the application. Required fields are indicated by asterisks in the user interface.

You can change the “required” status of a field in a view used in the self-registration workflow processes.

You can use the Workflow Administration screen to determine the view that includes a self-registration field.

To determine the view in which a self-registration field appears

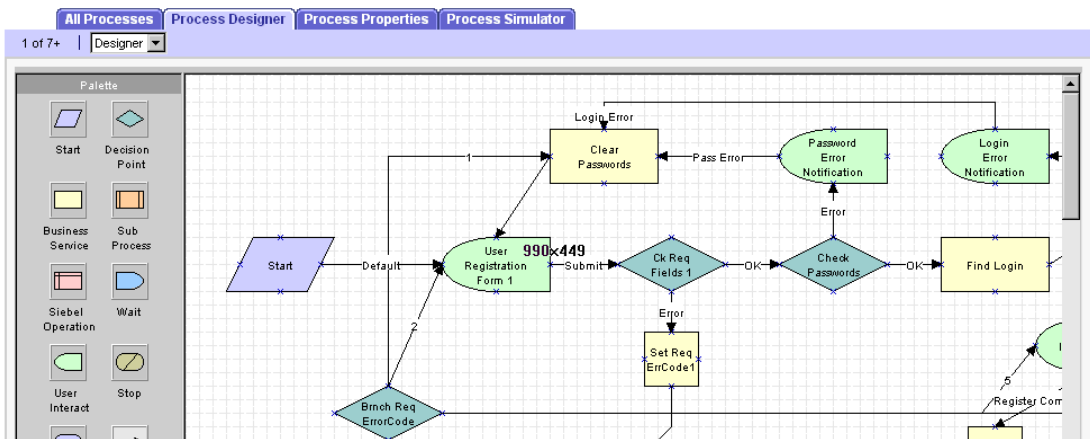
- 1 Log in as an administrator to a Siebel employee application, such as Siebel Call Center, and then choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.

- 2 Query or scroll to select User Registration SubProcess. All data collection from the self-registering user is performed in this workflow process.

- 3 Click the Process Designer view-level tab.

The Process Designer flow chart and palette appear. The following figure shows an example flow chart and palette.



- 4 Double-click the User Interact step, such as User Registration Form 1, which represents the stage of the self-registration process in which you want to require a field to be completed.

A User Interact form appears listing properties of this step.

The screenshot shows two windows from Siebel Tools. The top window, titled 'User Interact', displays the configuration for a step named 'User Registration Form 1'. It includes fields for Name, View, Workflow Process, Business Object, Type, Created By, and Created. The bottom window, titled 'Next Steps', shows a table with columns for Branch Name, Type, Next Step, Event Object Type, Event, Event Object, Sub Event, Comments, and Event Cancel Flag.

Branch Name	Type	Next Step	Event Object Type	Event	Event Object	Sub Event	Comments	Event Cancel Flag
Submit	Condition	Ck Req Fields 1	Applet	InvokeMethod	User Registration Ini	WriteRecord		

- 5 Record the entry in the View field.

The `CSSSWEFrameUserRegistration` class is applied to applets that are used in views that appear in the seed self-registration workflow processes. This class allows you to specify required self-registration fields.

To designate a required field in a self-registration form, you must use Siebel Tools to modify the applet that contains the form.

The following procedure is intended to present the main steps in a Siebel Tools task. For detailed information about working with applets and views in Siebel Tools, see *Siebel Tools Reference, MidMarket Edition*.

To designate a required field in a self-registration form

- 1 Open Siebel Tools.
- 2 Lock the User Registration project.
- 3 In Object Explorer, expand the View object.

The Views list appears.

- 4 Select the view you recorded in “[To determine the view in which a self-registration field appears.](#)”

- 5 In Object Explorer, expand the View Web Template child object, and then expand its child, View Web Template Item.

Self-registration views typically contain a single form applet. It is listed in the View Web Template Item list.

- 6 In the View Web Template Item list, drill down on the link in the Applet field for the single applet that is listed. If there is more than one applet listed, drill down on the one you think is most likely to contain the field you are looking for.

The Applets list appears with one record, the applet you drilled down on.

- 7 In the Object Explorer, expand the Applet object, and then expand the Control child object.

The Controls list appears below the Applets list.

- 8 In the Controls list, select the record whose Caption field is the name displayed in the user interface for the field you want to require users to complete. Record the value in the Name column; for example, MiddleName.

- 9 In Object Explorer, click the Applet User Prop object.

The Applet User Properties list displays the user properties for the applet in the Applets list.

- 10 With the Applet User Properties list active, choose Edit > New Record.

A new user property record appears.

- 11 Complete the new record using the following guidelines, and then save the record by stepping off of the record.

Field	Entry
Name	Required. Enter Show Required and a sequence number one greater than the largest existing sequence number. For example, if Show Required 6 is the greatest sequenced entry, enter Show Required 7. This entry is case-sensitive.
Value	Required. The value in the Name field that you recorded in Step 8 , such as MiddleName.

- 12 Recompile the Siebel repository file, and unlock the User Registration project.

When viewed in the self-registration interface, the new required field has an asterisk.

To remove the “required” property from a field in the user interface, follow the steps in [“To determine the view in which a self-registration field appears” on page 198](#) and [“To designate a required field in a self-registration form” on page 199](#) with the following exception: In the Applet User Properties list, either check the Inactive column for the record or delete the record.

Adding or Deleting Fields in an Existing View

All the data collected in views used in the seed self-registration workflow processes are written to fields in the User Registration business component. The following process describes how data is collected in the user interface and written to a user’s record in the database:

- The user enters data, such as the user’s height, into a text box on a form.
- The form field is mapped to a virtual field, for example Vheight, in the User Registration business component, so the data is written directly to that field.
- Self-registration data collection is done in the User Registration SubProcess. A process property, for example Vheight, of the User Registration SubProcess maps to the Vheight virtual field. Therefore the virtual field value populates the process property. The virtual field and the process property can have the same name, and this naming convention makes it easier to track the mapping.
- The Vheight process property serves as output from the User Registration SubProcess to its parent, the User Registration process. The posting happens only after the User Registration SubProcess is complete, that is, when the user has successfully completed the registration forms. The output is mapped to a process property in the User Registration Process, such as, again, Vheight by convention. Process properties from different workflow processes, even parent and child, can have the same name.

- The process property in User Registration Process, Vheight in this example, maps to a field in the database, such as Height. Because the User Registration business component writes to the same database tables as the User business component, each field is actually stored as part of a user record. Except for some Siebel partner-specific data, no data from the User Registration Process properties is written to the User Registration business component fields until the self-registration process is complete.

To add or delete fields in a view used in a self-registration workflow process, you must perform tasks in the following stages:

- Siebel Tools tasks
- Workflow tasks

Siebel Tools Tasks

To add a field to one of the views used in the self-registration workflow processes, you must use Siebel Tools to do one or more steps of the following procedure. This procedure is intended to list the major tasks required. For detailed information about modifying views and applets, see *Siebel Tools Reference, MidMarket Edition*.

To add a field to a view used in a self-registration workflow process

- 1** Open Siebel Tools.
- 2** Lock the User Registration project.
- 3** Determine the business component and the underlying database table on which the new field is based.
- 4** If the new field is not based on an existing database table column, define a column on an extension table of the appropriate table.
- 5** Create a new field, based on the new or existing table column, in the appropriate business component.
- 6** If the new field is based on the User Registration business component, create a new virtual field in the business component.
 - a** Create the field in the business component as you would any field. The naming convention used for existing virtual fields is to prefix the name with a “V”, such as “Vheight.”
 - b** Set the new field’s Calculated property to TRUE.

- 7 Configure the appropriate applet to expose the new virtual field.
- 8 If necessary, configure the new field so that a self-registering user is required to complete it.

For information about configuring a required field, see [“Redefining Required Fields” on page 198](#).

- 9 Recompile the Siebel repository file, and unlock the User Registration project.

To remove a field from the self-registration user interface, you do not have to delete the field from the applet in which it appears. Instead, configure the applet so that the field is not exposed.

For detailed information about configuring applets, see *Siebel Tools Reference, MidMarket Edition*.

Workflow Tasks

Adding a field to a view that is used in a self-registration workflow process requires that you associate process properties with the field so that information gathered through the workflow process is written to the appropriate field in the business component.

The following procedure is intended to list the major tasks you must perform in the Business Process Administration screen to allow an added field in the user interface to correctly populate a field in the User Registration business component. It applies the principle of writing user data to the database only after the registration process is complete. It assumes you have already completed the tasks described in [“Siebel Tools Tasks” on page 202](#). For detailed information about Workflow administration, see *Siebel Business Process Designer Administration Guide, MidMarket Edition*.

To modify self-registration workflow processes to handle an added field

- 1 In a Siebel employee application, such as Siebel Call Center, log in as an administrator, and then from the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.
- 2 Query or scroll to select User Registration SubProcess.
- 3 Create a revised copy of User Registration SubProcess as described in [“To create a revised copy of a workflow process” on page 197](#). Edit this revised copy.

- 4 Click the Process Properties view-level tab.

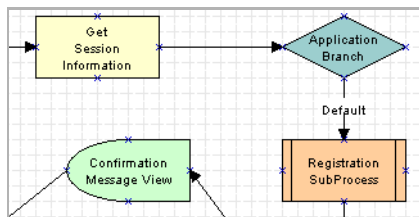
The Process Properties list appears.

- 5 In the Process Properties list, create a new record. Enter only the fields listed below by using the guidelines provided.

Field	Guideline
Name	Enter a process property name, such as Vheight. This can be a name of your choice.
Data Type	Pick the appropriate data type.
Business Component	Enter <code>User Registration</code> .
Virtual Field	Enter the name of the virtual field, such as <code>Vheight</code> , in the <code>User Registration</code> business component that corresponds to the new field.

- 6 Click the All Processes view-level tab, and then select `User Registration Process`.
- 7 Click the Process Designer view-level tab.

The Process Designer flow chart appears. One of its subprocess steps is `Registration SubProcess`. The following figure is an example of flow chart.



- 8 Double click the `Registration SubProcess` step.

The Sub Process form appears.

- 9** In the Sub Process Output Arguments list, create a new record. Enter only the fields listed below by using the guidelines provided.

Field	Guideline
Property Name	Enter a process property name, such as <code>Vheight</code> , for the User Registration Process. This can be a name of your choice.
Type	Enter <code>Output Argument</code> .
Sub Process Output	Enter the process property, such as <code>Vheight</code> , of the User Registration SubProcess that you created in Step 5 on page 204 .

- 10** Click the Process Designer view-level tab.

The Process Designer flow chart appears.

- 11** Perform the following steps for each Siebel Operation step that inserts a new user, for example Insert New User:

- a** Double click the step's flow chart icon.

The Siebel Operation form appears.

- b** In the Fields list, create a new record. Enter only the fields listed below by using the guidelines provided.

Field	Guideline
Field Name	Enter the new field name, such as <code>height</code> , that you created in the User Registration business component. This should be the field that writes to the database, not the corresponding virtual field.
Type	Enter <code>Process Property</code> .
Property Name	Enter the process property, such as <code>Vheight</code> , of the User Registration Process that you created in Step 9 on page 205 . This process property is the end of the chain that passes the virtual field value collected by the user interface.

12 In the Siebel Operation form, click Return to Designer.

The Process Designer flow chart and palette appear.

13 Click the All Process view-level tab.

The Workflow Processes list appears. The revised process is still selected.

14 On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

NOTE: If you remove a field from the self-registration user interface, you must also make sure that the User Registration SubProcess workflow process does not require the user to complete the field and that the field is not used to check for duplicate User records.

For information about removing the requirement that the user must complete a field, see [“Workflow Tasks” on page 203](#).

For information about removing a field from the deduplication check, see [“Modifying the Fields Used to Determine a Duplicate User” on page 209](#).

Changing the Physical Appearance of a View or Applet

For information about changing the physical appearance of a view or applet, such as moving fields or changing colors, see *Siebel Tools Reference, MidMarket Edition*.

Creating a New View

You create a new view for insertion into one of the self-registration workflow processes in the same way you create a view for any other purpose.

You can include new applets in a view that you create that you include in a self-registration workflow process. You create the new applet and include it in the view in the same way as you would for any other purpose, with the following consideration:

- If you base the applet on the User Registration business component, apply the `CSSSWEFrameUserRegistration` class to the applet. This allows you to define fields for which an asterisk displays in the user interface. By convention, fields that you require users to complete during the self-registration process have an asterisk.

For information about working with views, see *Siebel Tools Reference, MidMarket Edition*.

Modifying User Deduplication

When a user self-registers, the User Registration Process workflow process attempts to determine whether the user already exists in the database. User deduplication is a default feature, and it is configurable.

As default functionality, if all of the following non null field values entered by the self-registering user match those for an existing user, the users are considered to be the same person.

- First name
- Last name
- Email address

If the self-registering user is a match of an existing user, the existing User record is updated instead of a new User record being written. If the value in a field of the existing User record differs from the self-registering user's non-null entry, the existing field is updated with the new data. All other existing field values are left unchanged.

In the User Registration SubProcess workflow process, the duplication comparison is done by the `ValidateContact` method in the User Registration business service. The comparison is done in the Check User Key business service step.

Modifying Updated Fields

You can specify that certain fields in the User Registration business component are not updated when a duplicate user is determined.

The following procedure is intended to list the major steps you must do. For detailed information about doing any step, see *Siebel Tools Reference, MidMarket Edition*.

To exclude a field from being updated when a duplicate user is determined

- 1** Open Siebel Tools.
- 2** Lock the User Registration project.
- 3** Determine the field in the User Registration business component that you want to exclude from updating.
 - a** In the Object Explorer, expand Business Component, and then expand its Field child.
 - b** In the Business Component list, query or scroll to select the User Registration business component.
- 4** In the Object Explorer, expand Business Service, and then click on its Business Service User Properties child.

The Business Services list applet and the Business Service User Properties child list applet appear.

- 5** In the Business Services list applet, select User Registration.
- 6** In the Business Service User Properties, create a new record.
- 7** Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter <code>Exclude From Update number</code> , where <i>number</i> is the next number in the sequence for this particular user property. For example, enter <code>Exclude From Update 3</code> . This entry is case-sensitive.
Value	Enter the User Registration business component field name that you noted in Step 3 on page 208 .

- 8** Commit the record.
- 9** Recompile the Siebel repository file and unlock the User Registration project.

Modifying the Fields Used to Determine a Duplicate User

You can change the fields that are used to determine whether a duplicate user exists.

The following procedure is intended to list the major steps you must perform to modify the fields used to determine a duplicate user. For detailed information about performing any step, see *Siebel Tools Reference, MidMarket Edition*.

To modify the fields used to determine a duplicate user

- 1** Open Siebel Tools.
- 2** Lock the User Registration project.
- 3** Determine the fields in the User Registration business component that you want to add or delete from the duplication comparison.
 - a** In the Object Explorer, expand Business Component, and then expand its Field child.
 - b** In the Business Component list, query or scroll to select the User Registration business component.
- 4** In the Object Explorer, expand Business Service, and then click on its Business Service User Properties child.

The Business Services list applet and the Business Service User Properties child list applet appear.

- 5** In the Business Services list applet, select User Registration.
- 6** Delete a field from the duplication comparison.
 - a** In the Business Service User Properties list applet, select the record with name `App User Key: Default number` whose value is the User Registration business component field you want to delete from the comparison.
 - b** Click to put a check in the Inactive field, and then commit the record.

- 7** Add a field to the duplication comparison.
 - a** In the Business Service User Properties, create a new record.
 - b** Enter only the fields listed below by using the guidelines provided, and then commit the record.

Field	Guideline
Name	Enter App User Key: Default <i>number</i> or App User Key: <i>application number</i> , where <i>application</i> is the name of the Siebel application, and <i>number</i> is the next number in the sequence for this particular user property. For example, enter App User Key: Default 2 to add a field for Siebel eService. This entry is case-sensitive.
Value	Enter the name of the User Registration business component field that you want to add to the duplication check.

- 8** Recompile the Siebel repository file and unlock the User Registration project.

Deactivating the Duplication Check

You can deactivate the duplication check.

The following procedure is intended to show the main steps in deactivating the duplication check. For more detailed information on working with workflow processes, see *Siebel Business Process Designer Administration Guide, MidMarket Edition*.

To deactivate the self-registration deduplication check

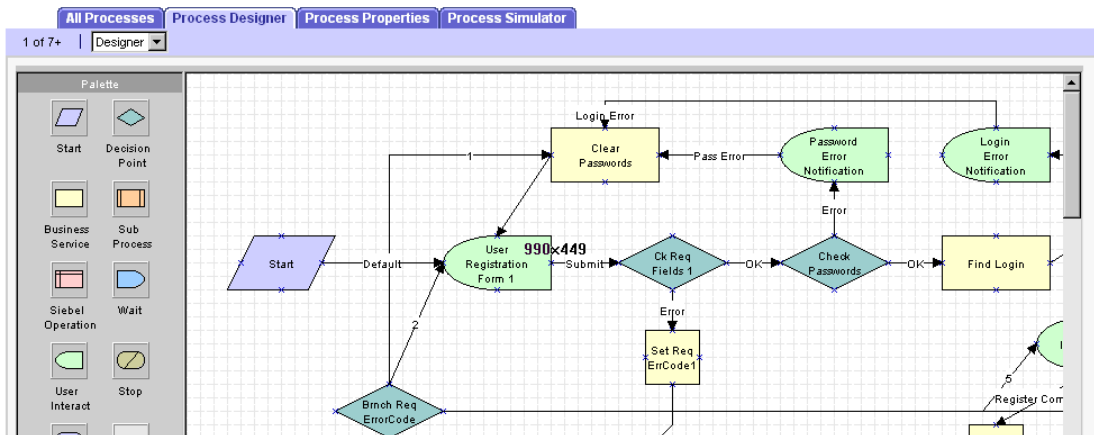
- 1** From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.

- 2** Query or scroll to select User Registration SubProcess.
- 3** Create a revised copy of User Registration SubProcess as described in [“To create a revised copy of a workflow process” on page 197](#). Edit this revised copy.

- 4 Click the Process Designer view-level tab.

The Process Designer flow chart and palette appear. This following figure is an example flow chart.



- 5 Record the sources of all connectors to the Check User Key step and the destination of the single connector from the step. Reroute the connectors to bypass the step.
- 6 Delete the bypassed process step, which should now not be the source or destination of any connector.
- 7 Click the All Processes view-level tab.

The Workflow Processes list appears. The revised process is still selected.

- 8 On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

Forgot Your Password?

If a user who has previously self-registered on a Siebel customer application forgets his or her password, the user can get a new password by clicking the Forgot Your Password? link in the login dialog box.

NOTE: Forgot Your Password? is a default functionality of Siebel customer applications, but it is available only if you implement ADSI or LDAP security adapter authentication or database authentication. If you want to implement a similar functionality in a Web SSO authentication environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, and in your security adapter. Configuration guidelines are not provided in Siebel applications documentation.

The User Experience

A user who has previously self-registered can retrieve a new password. The user can change the new password in the Profile view on a future login.

To retrieve a new password

- 1 In the login dialog box, the user clicks Forgot Your Password?.

The User Information form appears.

- 2 The user completes all fields of the form, and then clicks Submit.

- The database comparisons done with the Last Name field and First Name field entries are case sensitive.
- The Work Phone # entry numbers are compared with the database. The comparison disregards any separators.

If a matching record is found, the Challenge Question form appears.

- 3 The user enters the answer to the challenge question.

If the challenge question is answered correctly, the New Password Confirmation dialog box appears with a new password for the user.

- 4 Click Continue.

Forgot Your Password? Architecture

Forgot Your Password? is implemented in the User Registration Forgot Password Process workflow process. This process is a subprocess in User Registration Initial Process.

As described in [“To retrieve a new password” on page 212](#), to receive a new system-generated password, the user must provide identification data that is compared with database user records. If all four fields return a case-sensitive match with an existing record, the user must answer the challenge question associated with that record. The challenge answer must also return a case-sensitive match.

When a user enters values to the comparison fields in the user interface, the values are written to virtual fields in the User Registration business component. The User Registration business component is based on the same tables as the User business component. The virtual field values are not written to the database, but are compared with field values in those underlying tables. The user entries in the following fields in the user interface are compared with field values in the tables indicated:

- The Last Name, First Name, Email, and Work Phone # fields are compared with S_CONTACT field values.
- The Challenge Answer field is compared with an S_USER field value.

The User Registration Forgot Password Process workflow process uses the following views:

- User Registration Forget Pwd Info View
- User Registration Forget Pwd Challenge Ques View
- User Registration Forget Pwd Confirm View
- User Registration Forget Pwd Challenge Answer Error View
- User Registration Forget Pwd Decline View

Modifying Forgot Your Password?

You can modify the User Registration Forgot Password Process workflow process in the following ways:

- Make a comparison of null fields as well as fields for which the user has provided a value.
- Request different identification data from the user.

In the User Registration Forgot Password Process workflow process, the Query User step invokes the FindContact method of the User Registration business service. This method queries the database for user records whose data matches the identification data provided by the user. If the query returns a unique record, the user can then prove he or she owns the record by answering the challenge question.

The parameters of the Query User step in User Registration Forgot Password Process are shown in [Figure 13](#). These parameters include input arguments (such as EmailAddress, FirstName, and LastName) and output arguments (such as LoginName and RegError).

Business Service

Save | Return To Designer 2 of 4

Name: Query User
Business Object: User Registration
Business Service: User Registration
Created By: SADMIN
Workflow Process: User Registration Forgot Password
Type: Business Service
Method: FindContact
Created: 7/16/2001 5:54:26 PM

Input Arguments

Save | 1 - 6 of 6

Input Argument	Type	Value	Property Name	Property Data Type	Business Compo	Business Compo	Comments
EmailAddress	Process Property		VEmailAddress	String			
FirstName	Process Property		VFirstName	String			
LastName	Process Property		VLastName	String			
Output Field: Id	Literal	Id					
Output Field: Login Name	Literal	Login Name					
WorkPhoneNum	Process Property		VWorkPhoneNum	String			

Output Arguments

Save | 1 - 3 of 3

Property Name	Type	Value	Output Argument	Business Compo	Business Compo	Comments
Login Name	Output Argument		Login Name			
RegError	Output Argument		RegError			
Siebel Operation Ob	Output Argument		Id			

Figure 13. Query User Step Parameters

Table 16 describes the functions of parameters in the Query User step.

Table 16. Query User Step Parameters

List	Records	Comments About Values
Input Arguments	EmailAddress FirstName LastName WorkPhoneNum	The Input Argument field values are the field names in the User Registration business component that the FindContact business service queries for a match. The comparison is made with the process property values given in the Property Name field. These process properties collect the entries made by the user.
	Output Field: Id Output Field: Login Name	As given by the Input Argument field values, the FindContact method is requested to return the Id and Login Name field values for each user record whose field values match the entries by the user. A temporary table of values is defined in which the rows are the records returned and the columns are given by the Value field values. One row of the temporary table contains the ID for a returned record in the Id column and the record's Login Name in the Login Name column.
Output Arguments	Login Name Siebel Operation Object Id RegError	<ul style="list-style-type: none"> ■ Each Property Name field value is a process property name. The Login Name and Siebel Operation Object Id process properties receive values if FindContact returns a unique matching record. If a unique record is not determined that matches the criteria, RegError receives an error value. ■ Siebel Operation Object Id is used to identify the user record for subsequent operations in the workflow process, and it receives its value from the temporary table's Id column, that is, the ID of the user record. The Login Name process property receives its value from the temporary table's Login Name column, that is, the Login Name of the user record.

Modifying the Workflow Process to Make a Comparison of Null Fields

By default, if a user completes fewer than all four fields on the User Information form, only the fields that a user completes are used in the query to find a unique matching record in the database. For example, if the user enters first and last name only, the query does not do any comparisons on the Email or Work Phone # fields.

You can specify that the FindContact method in the User Registration business service must also check that fields left empty by the user are confirmed to be NULL in the database record to conclude that a record is a match. To do so, you must add the QueryAllFields input argument with a value of Y to the Query User process step. By default, the value of this input argument is N, so it is not listed.

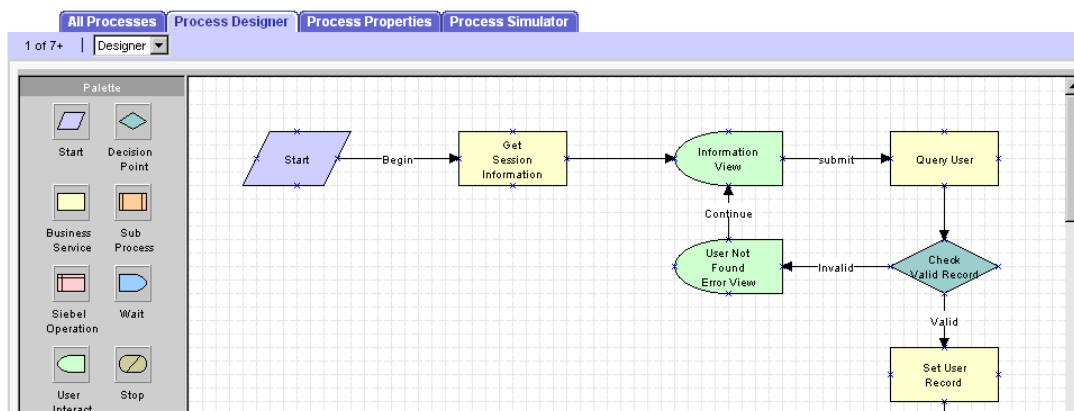
To specify that null fields be used in the query for a matching user record

- 1 From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.

- 2 Query or scroll to select User Registration Forgot Password Process.
- 3 Create a revised copy of User Registration Forgot Password Process as described in [“To create a revised copy of a workflow process” on page 197](#). Edit this revised copy.
- 4 Click the Process Designer view-level tab.

The Process Designer flow chart and palette appear.



- 5 Drill down on the Query User step.

A page that includes the Input Arguments list appears, as shown in [Figure 13 on page 214](#).

- 6** In the Input Arguments list, click the menu button and choose New Record.

A new input argument record appears.

- 7** Complete the new record, and then click Save. Enter only the following fields and values.

Field	Value
Input Argument	QueryAllFields
Type	Literal
Value	Y
Region	Siebel Financial Services only. This value specifies the user's geographic region. If you associate products with specific regions and set this field's value, Siebel eAdvisor users see only products associated with their regions.
RegionSetFlag	Siebel Financial Services only. Enter a check to indicate that this user's region is set. If this field is unchecked, a new Siebel eAdvisor user is asked to select a region.

- 8** In the Business Service form, click Return to Designer.

The Process Designer flow chart and palette appear.

- 9** Click the All Process view-level tab.

The Workflow Processes list appears. The revised process is still selected.

- 10** On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

Modifying the Workflow Process to Request Different Identification Data

The data requested from the user in the User Information form is compared with data in existing user records to locate a unique database record. If you want to compare different data than those compared in the seed User Registration Forgot Password Process workflow process, then you must do the following tasks:

- Modify the user interface.
- Modify User Registration Forgot Password Process.

Modifying the User Interface

To add or delete a field in the User Information form, you must use Siebel Tools to modify its underlying applet. The following procedure is intended to list the major steps you must perform to add or delete a field in the User Information form. For detailed information about performing any step, see *Siebel Tools Reference, MidMarket Edition*.

To add or delete a field in the User Information form

- 1** Open Siebel Tools.
- 2** Lock the User Registration project.
- 3** If you are adding a field, determine both the virtual field in the User Registration business component that corresponds to the field you want to add and the actual field that is used to write to the underlying table. For example, if you want to add a comparison to City, note the VCity virtual field and the City field.
 - a** In the Object Explorer, expand Business Component, and then expand its Field child.
 - b** In the Business Component list, select the User Registration business component.
- 4** Configure the User Registration Forget Pwd Info Applet to expose or hide the field.
 - a** In the Object Explorer, expand Applet, and then expand its Control child.
 - b** In the Applets list, query or scroll to select User Registration Forget Pwd Info Applet.
 - c** If you want to hide a field, select its record in the Controls list and check its Inactive field.

- d** If you want to add a field, add a new record in the Controls list, and then click Save. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter a name for this field, such as City
Caption	Enter the caption you want for this field in the user interface, such as City
Field	Enter the virtual field for this field that you determined in Step 3 on page 218 , such as VCity
HTML Display Mode	Delete the default value, so the field is empty
HTML Row Sensitive	Check
HTML Type	Pick Text
Sort	Check
Text Alignment	Pick an alignment
Visible	Check
Visible - Language Override	Enter Y

- 5** Configure the appropriate applet Web template for the User Registration Forget Pwd Info Applet to display or hide the field.

For information about adding or deleting a control in an applet Web template, see *Siebel Tools Reference, MidMarket Edition*.

- 6** Recompile the Siebel repository file and unlock the User Registration project.

To remove a field from the self-registration user interface, you do not have to delete the field from the applet in which it appears. Instead, configure the applet so that the field is not exposed.

For detailed information about configuring applets, see *Siebel Tools Reference, MidMarket Edition*.

If you are adding a field to the comparison, there must be a process property present to collect that field entry from the user and write it to a virtual field of the User Registration business component. If a process property is not present for collecting the entry, you must create a new process property.

To create a process property to collect and write data to a virtual field

- 1 From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

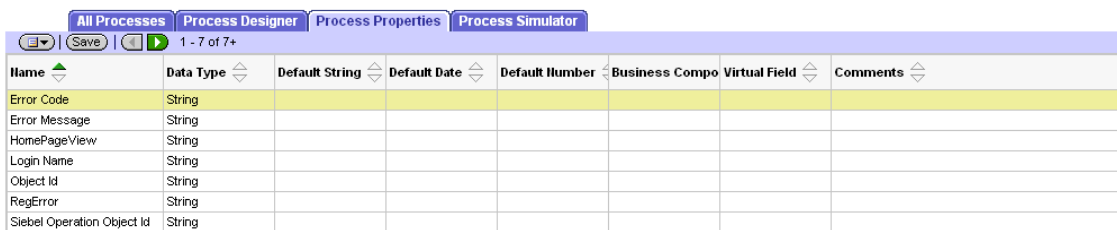
The Workflow Processes list appears.

- 2 Query or scroll to select User Registration Forgot Password Process.
- 3 Create a revised copy of User Registration Forgot Password Process as described in [“To create a revised copy of a workflow process” on page 197](#). Edit this revised copy.

A copy of the record appears with an incremented version number and a status of In Progress.

- 4 Click the Process Properties view-level tab.

The following figure shows a list of process properties for a workflow process.



The screenshot shows the Siebel Process Designer interface with the 'Process Properties' tab selected. The table below lists the properties for a workflow process.

Name	Data Type	Default String	Default Date	Default Number	Business Comp	Virtual Field	Comments
Error Code	String						
Error Message	String						
HomePageView	String						
Login Name	String						
Object Id	String						
RegError	String						
Siebel Operation Object Id	String						

- 5 In the Process Properties list, click the menu button and choose New Record.

A new record appears.

- 6** Complete the new record, and then click Save. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	By convention, provide the same name as the virtual field in the User Registration business component to which this process property writes. This is the virtual field that you noted in Step 3 of “To add or delete a field in the User Information form” on page 218 , such as <code>VCity</code> .
Data Type	Enter <code>String</code> .
Business Component	Pick <code>User Registration</code> .
Virtual Field	Enter the virtual field name that you noted in Step 3 of “To add or delete a field in the User Information form” on page 218 , such as <code>VCity</code> .
Region	This value specifies the user’s geographic region. If you associate products with specific regions and set this field’s value, Siebel eAdvisor users see only products associated with their regions.
RegionSetFlag	Enter a check to indicate that this user’s region is set. If this field is unchecked, a new Siebel eAdvisor user is asked to select a region.

- 7** Click the All Process view-level tab.

The Workflow Processes list appears. User Registration Forgot Password Process is still selected.

- 8** Do one of the following:

- If you are pausing the process of adding a field to the FindContact method input arguments, click Activate on the Workflow Processes list.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

- If you are continuing the process of adding a field to the FindContact method input arguments, leave the status as In Progress and exit this procedure.

In the Query User step of User Registration Forgot Password Process, you specify the input fields to the FindContact method in the User Registration business service that are used to find a matching user record. You must modify this step to add or delete an input field.

To add or delete input fields provided to the FindContact method

- 1 From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

The Workflow Processes list appears.

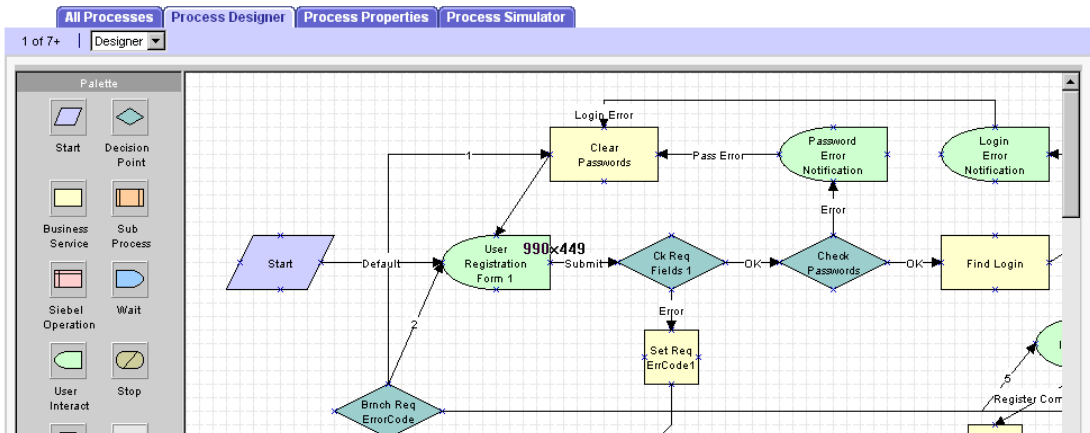
- 2 Query or scroll to select User Registration Forgot Password Process.

- 3 If you are not already working on a version of the process with an In Progress status, create a revised copy of User Registration Forgot Password Process as described in [“To create a revised copy of a workflow process” on page 197](#). Edit this revised copy.

A copy of the record appears with an incremented version number and a status of In Progress.

- 4 Click the Process Designer view-level tab.

The Process Designer flow chart and palette appear.



- 5** Drill down on the Query User step.

A page that includes the Input Arguments list appears, as shown in [Figure 13 on page 214](#).

- 6** If you are deleting an input field, select the appropriate record in the Input Arguments, and then click the menu button and choose Delete Record.

The record is deleted.

- 7** If you are adding an input field, click the menu button in the Input Arguments list and choose New Record.

A new input argument record appears.

- 8** Complete the new record, and then click Save. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Input Argument	Enter the name of the field in the User Registration business component that you noted in Step 3 of “To add or delete a field in the User Information form” on page 218 , such as <code>City</code> . This is the field in the existing user records with which the comparison is made.
Type	Pick <code>Process Property</code> .
Property Name	Pick the process property that corresponds to the virtual field in the User Registration business component that you noted in Step 3 of “To add or delete a field in the User Information form” on page 218 , such as <code>VCITY</code> . The process property has the same name as the virtual field, by convention.
Property Data Type	This field automatically populates with the data type of the process property.
Region	This value specifies the user’s geographic region. If you associate products with specific regions and set this field’s value, Siebel eAdvisor users see only products associated with their regions.
RegionSetFlag	Enter a check to indicate that this user’s region is set. If this field is unchecked, a new Siebel eAdvisor user is asked to select a region.

- 9 In the Business Service form, click Return to Designer.

The Process Designer flow chart and palette appear.

- 10 Click the All Process view-level tab.

The Workflow Processes list appears. User Registration Forgot Password Process is still selected.

- 11 On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

Internal Administration of Users

You can provide an employee, a customer, or a partner user with access to one or more Siebel applications by performing the following tasks:

- Provide the user with a method to be authenticated and thus to connect to a database account.
- An internal administrator uses a Siebel employee application, such as Siebel Call Center, to add the user to the Siebel database.

User Authentication Requirements

Your authentication architecture should be implemented before adding new users. As an ongoing task, you must arrange that each new user can be authenticated at login. The setup and administration that you must perform for each new user depends on the authentication architecture you implement.

For information about user authentication concepts mentioned in the following descriptions, see [“User Authentication” on page 63](#).

- **Database authentication.** You must enter the user name for a valid database account in the user’s user ID field. You must provide the user ID and the password to the database account to the new user.

- **Security adapter authentication.** You can configure your application so that when you create or modify user records in the Siebel database, the security adapter propagates those changes to the user directory. Therefore, no separate administration of the user directory is required.

NOTE: For a Siebel security adapter to propagate new or modified user data from the Siebel database to the user directory, the administrator who modifies the database records must log in through the same security adapter.

If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel applications. This includes internal administration of users that provides propagation of a user's Siebel user ID to the directory.

For information about user authentication, see [“User Authentication” on page 63](#).

CAUTION: Make sure the application user has write privileges to the user directory. If you do not implement an application user, make sure all users who create or modify users have write privileges to the directory.

- **Web SSO authentication.** You must maintain corresponding records in the external authentication system, the user directory, and the Siebel database for each user. If you want to implement a mechanism for synchronizing these records, you must develop the utility independently, and implement it at the Web site level. Configuration guidelines are not provided in Siebel applications documentation. You must provide authentication credentials to the new user.

Adding a User to the Siebel Database

A user of a Siebel application is a record in the User business component. The S_PARTY, S_CONTACT, and S_USER tables in the Siebel database underlie the User business component. Each user is assigned a responsibility, a user ID, and, depending on the authentication architecture being used, a password.

An employee or a partner user is a user who has a position within a division, either internal or external, in the Siebel database. Other users, such as those who use Siebel customer applications such as Siebel eSales, do not have a position or a division. The S_EMP_PER table underlies the Employee business component, to which employees and partner users belong, in addition to the tables that underlie the User business component.

For more information about the functions of responsibilities, positions, divisions, and organizations, see [“Access Control” on page 247](#).

An administrator uses different views to add employees, partner users, and other users, although each of these users has a record in the User business component.

Adding a New Employee

At a minimum, an employee must have a position, a responsibility, and a Siebel user ID.

You can also associate attributes with employee records such as skills and availability. By doing so, you can use the employee record and its attributes with features such as Siebel Territory Assignment Manager, MidMarket Edition and Siebel Professional Services Automation, MidMarket Edition.

For information about assigning attributes to employees, see *Applications Administration Guide, MidMarket Edition*.

The following procedure creates a User record for the employee only as a stage in allowing the employee to access the database.

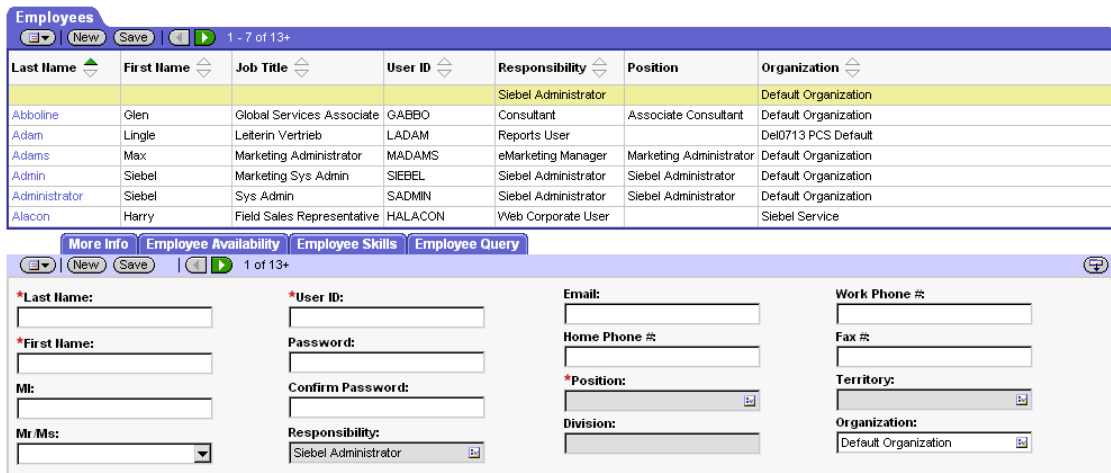
To add a new employee

- 1 Log in as an administrator to a employee application, such as Siebel Call Center, and then choose View > Site Map > User Administration > Employees.

The Employees list appears.

- 2 Click the menu button, and then choose New Record.

A new record appears in the Employees list and a corresponding form appears under the More Info view tab.



- 3 In the More Info form, click the show more button.

Additional fields appear in the More Info form, including the New Responsibility field.

- 4 Complete the form. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.

Field	Guideline
User ID	Required. This field must be unique for each user. Depending on your authentication architecture, the user may or may not log in with this identifier. If you implement database authentication, this field must be the login name for a database account.
Password	<ul style="list-style-type: none">■ This field is editable only if you implement database or security adapter authentication. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. The password is propagated to the user directory. The user uses this password to log in.■ This field is not editable if you implement Web SSO authentication. For Web SSO, you maintain the user's login password independently in the external authentication system.■ For information about user authentication architectures, see "User Authentication" on page 63.
Responsibility	Required. Pick one or more responsibilities which include appropriate views for the employee. If the administrator who creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "The New Responsibility Field" on page 234 .
New Responsibility	If the administrator who creates this user has a value in his or her New Responsibility field, then that responsibility is assigned to this field by default. For information about the New Responsibility field, see "The New Responsibility Field" on page 234 .
Position	Required. To be an employee, a user must have a position. If you assign multiple positions, the position you specify as Primary is the position the user assumes when he or she logs in.
Division	This field is populated automatically with the division to which the Primary position belongs.
Territory	This field is a read-only multi-value group. You are not able to enter a value manually. When you complete the Position field, the Territory field is populated automatically with territories with which the position is associated.

Field	Guideline
Organization	This field value is inherited from the user who creates this user, but the field is editable. Users whose positions are in this organization have access to this employee record. For information about organization access control, see “Access Control Mechanisms” on page 265 .
Region	This value specifies the user’s geographic region.
RegionSetFlag	Enter a check to indicate that this user’s region is set.

5 Click Save.

Completing Employee Setup

You can set up employees either before or after you assign them a responsibility. You can include additional information about the employee, including the following:

- **Territory Assignment Rules.** Allows you to see and administer all the assignment rules for an employee. For more information on assignment rules, see *Siebel Territory Assignment Manager Administration Guide, MidMarket Edition*.
- **Availability.** Used for Siebel Professional Services Automation. Lists the projects for which an employee is on staff. For more information on projects, see *Siebel Professional Services Automation Guide, MidMarket Edition*.
- **Utilization.** Displays a chart with the monthly and quarterly utilization of the currently selected employee. Managers use this chart for monitoring professional services projects and employees. For more information about professional services, see *Siebel Professional Services Automation Guide, MidMarket Edition*.

Deactivating an Employee

You can deactivate an employee by dissociating the employee record from its responsibilities, altering the user ID, and removing the employee’s access to the database.

To deactivate an employee

- 1** From the application-level menu, choose View > Site Map > User Administration > Employees.

The Employees view appears.

- 2** In the Employees list, select the employee you want to deactivate.
- 3** In the More Info view tab, delete all records from the Responsibility field.
- 4** Change the user ID slightly, to indicate that the employee is no longer current.

You may want to establish a convention for renaming user IDs when you deactivate employees. One possible convention is to append some text such as “expired” to the user ID. For example, you might change CARD to CARD-expired. That way you can continue to see the person’s name associated with previous activity in history records.

- 5** Remove the employee’s access to the database.

If you implemented database user authentication, you should remove the user’s database account. If you implemented external authentication, then delete the user from the directory from which the user’s database credentials are retrieved.

NOTE: In the case of external authentication, if the external user repository is shared by many applications—as in the case of an LDAP directory or Microsoft Active Directory—do not delete the user from the directory. In such a case, make sure that the user’s database access user name and password are different from that user’s directory user name and password. Otherwise the user would be able to access the database directly using some database connection tools.

Adding a New Partner User

A partner user is typically an employee in a partner company or a consultant to your company.

A partner user must have a position in a partner organization to be associated with that organization or to belong to position-based teams, such as opportunity or account teams.

You can assign a position to a new partner user from the following sources:

- Positions that you create internally and associate with the delegated administrator's partner organization
- Positions created by delegated administrators in the partner organization

You can register and administer partner users in the Partner Administration screen in Siebel Partner Manager or another Siebel employee application for which you have licensed this screen.

For information about using the Partner Administration screen, see *Siebel Partner Relationship Management Administration Guide, MidMarket Edition*.

Adding a New Contact User

Users who are not employees or partner users do not have positions. These users include, for example, customers who use Siebel eSales or eService. They are called customer or contact users to distinguish them from employee and partner users.

Contacts, such as contacts at a customer account, can exist in the database without having login capability. You create such contacts as Persons in the User Administration screen. The procedure in this section applies to contact users to whom you are providing a login to the Siebel database.

User Administration

Internal Administration of Users

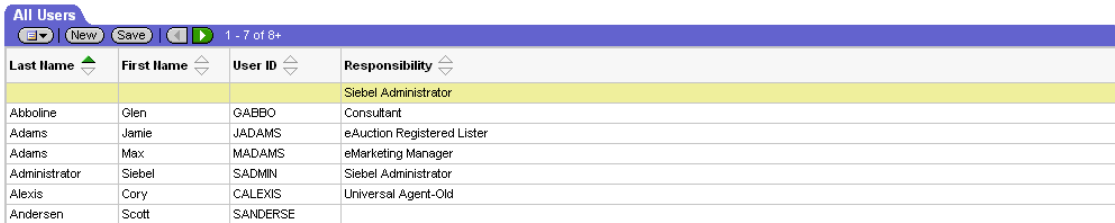
To add a new contact user

- 1 Log in as an administrator to a Siebel employee application, and then choose View > Site Map > User Administration > Users.

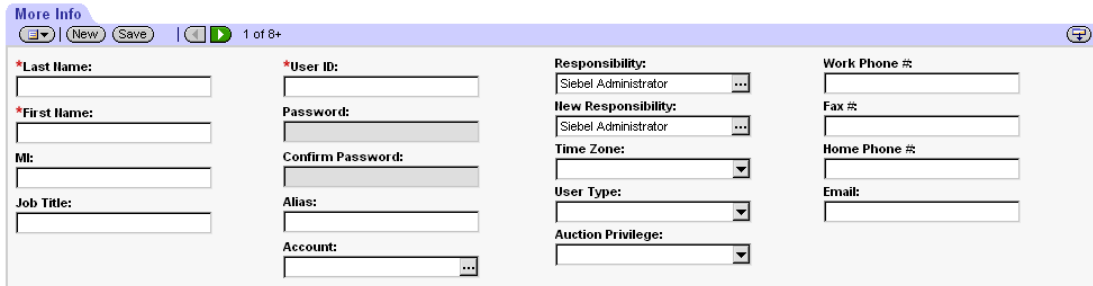
The All Users list appears.

- 2 Click the menu button, and then choose New Record.

A new record appears in the All Users list and a corresponding form appears under the More Info view tab.



Last Name	First Name	User ID	Responsibility
			Siebel Administrator
Abboline	Glen	GABBO	Consultant
Adams	Jamie	JADAMS	eAuction Registered Lister
Adams	Max	MADAMS	eMarketing Manager
Administrator	Siebel	SADMIN	Siebel Administrator
Alexis	Cory	CALEXIS	Universal Agent-Old
Andersen	Scott	SANDERSE	



*Last Name:

*First Name:

MI:

Job Title:

*User ID:

Password:

Confirm Password:

Alias:

Account:

Responsibility:

New Responsibility:

Time Zone:

User Type:

Auction Privilege:

Work Phone #:

Fax #:

Home Phone #:

Email:

- 3** Complete the fields in the More Info form, and then click Save. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.
User ID	Required. The user logs in with this ID.
Password	<ul style="list-style-type: none"> ■ For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. The user uses this password to log in. ■ This field is not editable if you implement Web SSO authentication. For Web SSO, you maintain the user's login password independently in the external authentication system. ■ For information about user authentication architectures, see "User Authentication" on page 63.
Account	Pick one or more accounts to associate to the user. Specify one as the primary account. For information about the function of the account in delegated administration, see "External Administration of Users" on page 236 .
Responsibility	Pick one or more responsibilities which include appropriate views in the customer application, such as Siebel eService, for this user. If the administrator who creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "The New Responsibility Field" on page 234 .
New Responsibility	If the administrator who creates this user has a value in the New Responsibility field, then that responsibility is assigned to this field by default. For information about the New Responsibility field, see "The New Responsibility Field" on page 234 .
Time Zone	Choose a time zone so that times for events can be expressed in terms of this zone.
User Type	This field serves as a filter so that different applications can query for contact users only applicable to each particular application.

Field	Guideline
Work Phone # Fax # Home Phone #	The application interprets only the digits the user provides. Any separators are disregarded.
Region	This value specifies the user's geographic region.
RegionSetFlag	Enter a check to indicate that this user's region is set.

The new user appears in the All Users list.

You can promote an existing contact to a contact user by assigning user credentials and a responsibility to a Person record.

To promote an existing contact to a contact user

- 1 Log in as an administrator to a Siebel employee application, and then choose View > Site Map > User Administration > Persons.

The All Persons list appears.

- 2 Select the record of the contact to promote.
- 3 Enter the user ID, Password, Responsibility, and New Responsibility fields as described in [“To add a new contact user” on page 232](#).

The New Responsibility Field

A user record may or may not have a value in the New Responsibility field. If a value does exist, then whenever the user creates a new user, the new user's Responsibility field is assigned the value in the creating user's New Responsibility field by default. This principle applies for any type of user (employee, partner user, contact user) creating any type of user that their application allows them to create.

A user's own New Responsibility field is populated in one of the following ways:

- The New Responsibility field value is inherited from the New Responsibility field of the user who creates this new user.
- The New Responsibility field value is manually assigned to the user.

A user's New Responsibility field can only be modified by an internal administrator.

Delegated administrators of Siebel customer and partner applications can upgrade a user's Responsibility, but they cannot edit the New Responsibility field. Therefore, your internal administrators control the default responsibility that any customer or partner user inherits from a delegated administrator. It is important to make sure delegated administrators have New Responsibility values that you intend your new customer and partner users to have, such as the seed responsibilities provided for such users.

You may or may not want to use the New Responsibility field functionality when administrators create new employee records. If there are a variety of responsibilities assigned new employees, then it may make sense to leave employee's New Responsibility field empty. If most of your new employees are assigned the same responsibility or you want to create a batch of new employee records that all have the same responsibility, then it is probably more efficient to assign a New Responsibility value to the administrator who adds the employees.

An internal administrator can modify New Responsibility values for employees, partner users, and contact users in the same administration screen.

To modify a user's New Responsibility field value

- 1** Log in as an administrator to a Siebel employee application, and then choose View > Site Map > User Administration > Users.

The All Users list appears, containing all the employees, partner users, and contact users in the database.

- 2** In the All Users list, select the user record to modify.
- 3** In the More Info form, pick a new value in the New Responsibility field, and then click Save.

The user must log out and log in for the New Responsibility value to become active.

External Administration of Users

A delegated administrator is a user of a Siebel customer or partner application whose responsibility provides views that allow the delegated administrator to register and administer other users of that application. Delegated administration is typically implemented in business-to-business relationships.

Delegated administration of users minimizes your internal administrative overhead by moving some of the administrative load to administrators in your customer or partner companies.

User Authentication Requirements

Delegated administration is a default functionality of most Siebel customer and partner applications, but it is available only if you implement ADSI or LDAP security adapter authentication.

Delegated administration cannot be implemented if you use database authentication. If you want to implement delegated administration in a Web SSO authentication environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, and in your security adapter. Configuration guidelines are not provided in Siebel applications documentation.

Delegated administration requires you configure the ADSI or LDAP security adapter to propagate new and modified user data from the Siebel database to the user directory.

If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow Siebel user IDs stored in the directory to be managed from within Siebel applications, including delegated administration of users. For information about user authentication, see [“User Authentication” on page 63](#).

CAUTION: Make sure the application user for your Siebel customer or partner application has write privileges to the user directory. If you do not implement an application user, make sure delegated administrator users of the application have write privileges to the directory. Typically, you do this by assigning write privileges to all users to avoid administering privileges for individual users.

For information about setting up ADSI and LDAP security adapter authentication, see [“LDAP and ADSI Security Adapter Authentication” on page 81](#).

Access Considerations

A delegated administrator has restricted access to user data.

- **Customer applications.** A delegated administrator can only see users that are associated with accounts with which the delegated administrator is associated. The My Account User Administration View is based on the Account (Delegated Admin) business component. This business component essentially restricts a delegated administrator's access to data that is associated with the accounts with which the delegated administrator is also associated.
- **Partner applications.** A delegated administrator can only see partner users whose positions are in the same partner organization to which the delegated administrator's position belongs.

A delegated administrator can add regular registered users or other delegated administrators. However, an administrator at your host company must add the first delegated administrator in:

- Each account for a Siebel customer application
- Each partner organization for a Siebel partner application

Creating a delegated administrator internally requires that you provide a user with a responsibility that includes the views needed for delegated administration. Your Siebel application provides seed responsibilities for delegated administrators of customer and partner applications.

For information about seed responsibilities, see [“Seed Data” on page 345](#).

Registering Users

Delegated user administration screens, navigation, and procedures vary somewhat among Siebel applications. This section describes delegated administration that is representative of customer and partner applications.

Registering Contact Users

A delegated administrator who uses a Siebel customer application must belong to at least one account. The delegated administrator registers a user in the currently active account. The new user inherits membership in that account.

A delegated administrator must assign at least one responsibility to a new user. A delegated administrator only has responsibilities, including seed responsibilities, available for assigning to users that your host company associates with the organization with which the delegated administrator is associated. The delegated administrator is associated with the organization to which the proxy employee for the application belongs. A responsibility is associated with an organization by an administrator at your company using an employee application such as Siebel Call Center.

For information about associating organizations with a responsibility, see *Applications Administration Guide, MidMarket Edition*.

To register a new customer user (by a delegated administrator)

- 1** Log in to a Siebel customer application that implements delegated administration and do one of the following to navigate to the Administration screen.
 - a** Click My Account, and then click User Administration under the My Company tab.

The following figure shows the location of My Account on the Administration screen.



- b** Choose View > Site Map > Administration.

A list of Delegated Accounts and Users appears. This list's appearance may vary somewhat by application.

The image shows two screenshots from a Siebel application interface. The first screenshot is titled 'Delegated Accounts' and shows a table with one row of data. The second screenshot is titled 'Users' and shows a table with four rows of data.

Name	Location	Home Page	Email	Phone Number	City	State
Marriott International	HQ	www.marriott.com		(800) 234-5000	Bethesda	MD

Last Name	First Name	Middle Initial	User ID	Email	Responsibility	User Type	Edit
McGrath	Sam		SMCGRATH	smcgrath@marriott.com	Web Corporate User	Web Corporate User	
Metz	Curtis		CMETZ	cmetz@marriott.com	Web Registered User		
Miller	Sam		SAMILLER	SMiller@marriott.de	Web Registered User		
Miller	Sam		SMILLER	smiller@marriott.com	Web Corporate User	Web Corporate User	

- 2** In the Delegated Accounts list, select the account with which you want to associate the new user.

The users in this account appear in the Users list.

- 3** In the Users list, click New.

A Users form appears, similar to the one shown below for Siebel eService.

The image shows a 'Users' form with various input fields for user information. The form is titled 'Users' and has 'Save' and 'Cancel' buttons at the top left.

Fields include:

- *Last Name: [Text Field]
- *First Name: [Text Field]
- Middle Initial: [Text Field]
- Job Title: [Text Field]
- Home Phone #: [Text Field]
- Work Phone #: [Text Field]
- Work Fax #: [Text Field]
- Email: [Text Field]
- User ID: [Text Field]
- Password: [Text Field]
- Confirm Password: [Text Field]
- Responsibility: [Icon]
- User Type: [Dropdown Menu]
- Time Zone: [Dropdown Menu]

- 4 Complete the fields in the Users form, and then click Save. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.
User ID	Required to allow the user to log in. The security adapter identifies the user in the database with this field value. Depending on how you configure your security adapter, the user may log in with this ID.
Password	Required to allow the user to log in. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Responsibility	Pick one or more responsibilities, such as a seed responsibility provided for contact users. If the delegated administrator who creates this user has a value in the New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see “The New Responsibility Field” on page 234 .
Home Phone # Work Phone # Work Fax #	The application interprets digits only in these telephone number entries. Any separators are disregarded.
Region	This value specifies the user’s geographic region.
RegionSetFlag	Enter a check to indicate that this user’s region is set.

The new user record appears in the Users list.

Registering Partner Users

A delegated administrator using a partner application, such as Siebel PRM, has a position in a partner division. The delegated administrator can only assign to a new partner user a position from those included in the partner organization to which the partner division belongs.

A partner user must have a position in a partner organization to be associated with that organization or to belong to position-based teams, such as opportunity or account teams. A delegated administrator in a partner company can assign a position to a new partner user from the following sources:

- Positions that you create internally and associate with the delegated administrator's partner organization
- Positions created by delegated administrators in the partner organization

A delegated administrator only has responsibilities available for assigning to partner users that your host company associates with the delegated administrator's partner organization. An administrator at your company associates partner organizations with responsibilities using an employee application such as Siebel Call Center.

For information about associating organizations with a responsibility, see *Applications Administration Guide, MidMarket Edition*.

A delegated administrator must do two tasks to provide a new partner user with access to the database:

- Register the partner user
- Assign a responsibility to the partner user

To register a new partner user (by a delegated administrator)

- 1** Log in to a partner application, such as Siebel PRM, that implements delegated administration, and then choose Site Map > Administration > User Administration.

The Users list appears, displaying partner users in the delegated administrator's organization.

User Administration

External Administration of Users

- In the Users list, click New.

A More Info form appears, similar to the one shown in the following figure.

The screenshot shows a web form titled "Users" with a "Menu" dropdown, "Save", and "Cancel" buttons. The form is organized into four columns of fields:

- Column 1:** *Last Name, *First Name, Middle Initial, Mr Ms (dropdown), Alias.
- Column 2:** Job Title, *User ID, Password, Verify Password, *Position (with a help icon).
- Column 3:** Work Phone #, Home Phone #, Work Fax #, Email.
- Column 4:** Pager #, Pager PII#, Pager Type (dropdown).

- Complete the fields in the Users form, and then click Save. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.
User ID	Required to allow the user to log in. The security adapter identifies the user in the database with this field value. Depending on how you configure your security adapter, the user may log in with this ID.
Password	Required to allow the user to log in. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Position	If you assign multiple positions, the position you specify as Primary is the position the partner user assumes when he or she logs in.
Work Phone # Home Phone # Fax # Pager #	The application interprets digits only in these telephone number entries. The user can enter any separators.

Field	Guideline
Region	This value specifies the user's geographic region.
RegionSetFlag	Enter a check to indicate that this user's region is set.

4 Click Save.

The new partner user record appears in the Users list.

The delegated administrator separately assigns a responsibility to a new registered partner user.

To assign a responsibility to a partner user (by a delegated administrator)

1 Log in to a Siebel partner application that implements delegated administration, and then choose Site Map > Administration > User Administration.

2 Click the Responsibility view tab.

The Responsibility list appears. If the delegated administrator who creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default.

3 On the Responsibility list, click the menu button, and then choose New Record.

The Add Responsibilities list appears.

4 Pick one or more responsibilities, and then click OK. For information about seed responsibilities provided for assigning to partner users, see [“Seed Data” on page 345](#).

The new responsibility appears in the Responsibility list.

5 In the Users list, click Save.

For information about the New Responsibility field, see [“The New Responsibility Field” on page 234](#).

Maintaining a User Profile

Each employee, partner user, and customer user is provided a profile screen in which to update identification and authentication data. Depending on the application and on the authentication architecture you implement, a user can perform tasks such as:

- Edit personal information, such as the address or time zone.
- Edit company information in a partner application.
- Change the login password.
- Change the active position in an employee application.
- Change the primary position in a partner application.

Profile forms, names, and navigation paths differ somewhat across Siebel applications. The procedures in this section are representative of those in Siebel employee, partner, and customer applications. Procedures in individual applications may differ.

Editing Personal Information

Users can change a variety of personal information in their profile form. In this context, authentication and access control data, such as passwords and positions, are not included.

To edit personal information

- 1 Depending on the application, the user does one of the following:
 - In a Siebel customer application, the user clicks My Account, and then clicks User Profile under the My Settings tab.

The following figure shows the location of My Account in a Siebel customer application.



The User Profile form appears.

- In a Siebel partner application, the user clicks Profile. The Personal Profile form appears.
 - In a Siebel employee application, the user chooses View > Site Map > User Profile Preferences > Profile. The Contact Information form appears.
- 2 The user clicks Edit to make the form fields editable, if necessary.
 - 3 The user enters or changes data in editable fields, and then clicks Save.

Changing a Password

If you implement database or security adapter authentication, then a user can change the login password.

NOTE: If you want to implement a similar functionality in a Web SSO authentication environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, in your security adapter, and in the Siebel application views. Configuration guidelines are not provided in Siebel applications documentation.

To change a password, a user accesses the profile form as described in [“Editing Personal Information” on page 244](#), and then completes the appropriate fields. The password-related fields are not editable if the password cannot be changed in the current authentication architecture.

Changing the Active Position

An employee or partner user of a Siebel application can have one or more positions, of which one is the primary position. When the user logs in, the user assumes the primary position only and the data access that the position determines.

An employee can assume a position other than the primary position, which immediately makes it the active position. The employee then accesses only the data determined by the new active position.

Changing the active position does not change the employee's primary position. When the employee subsequently logs in, the primary position becomes active.

To change the active position in a Siebel employee application

- 1** Choose View > Site Map > User Profile Preferences > Change Position.

The Change Position list appears.

- 2** Click on a position record to select it, and then click OK.

A check appears in the Active Position field for the selected position.

A partner user can change the primary position. The user assumes the primary position when the user next logs in.

To change the primary position in a Siebel partner application

- 1** The partner user clicks Profile.

The Personal Profile form appears.

- 2** The partner user clicks the Active Position select button.

The Positions Occupied list appears.

- 3** The partner user checks a position to make it the new primary position, and then clicks the Save button for the record.

- 4** The partner user clicks OK.

The new primary position displays in the Personal Profile form.

- 5** The partner user logs out, and then logs in again to make the new primary position active.

Access Control **10**

Access control is the means to control visibility of data records to each individual user. This section discusses fundamental access control mechanisms you can use to control data access.

Access Control Overview

In Siebel application terms, a screen is a collection of views. The screen represents a broad area of functionality, such as working with accounts. To the user, a view is simply one Web page. Within a view, the user may see lists of data records or forms presenting individual records. These lists and forms are also referred to as applets in a configuration context.

In [Figure 14](#), the My Accounts view of the Accounts screen is shown, as indicated by the selected Accounts screen tab and the display of My Accounts in the Show drop-down list. This view includes an Accounts list and an accompanying form with detail for the selected account.

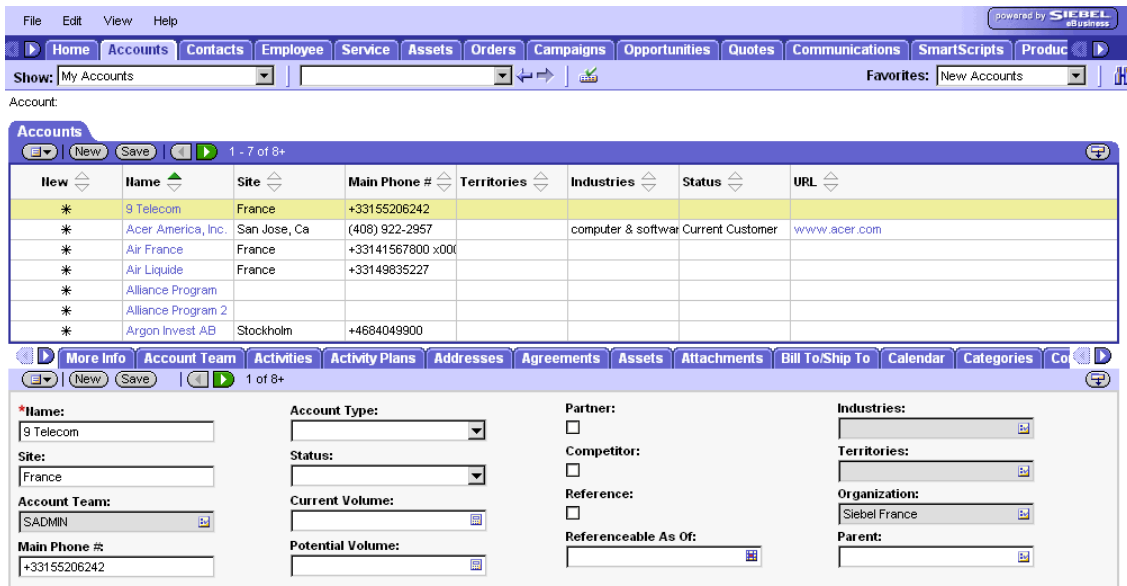


Figure 14. My Accounts View

Basic access control consists of the following:

- **View level access control.** You allow a user to see only the views that you want the user to see.
- **Record level access control.** You allow a user to see only the data records that you want the user to see.

View level access control mechanisms include filtering of available views at the application level, and through a user's responsibilities, or sets of views, assigned to the user.

Implementation of view level access control is direct and is not discussed in this section. For more information about implementing view access control, see ["Implementing Basic Access Control" on page 289](#).

You can use several different access control mechanisms to associate data with users. Access control mechanisms include persons, positions, organizations, and access groups—each provides a slightly different set of functions. You can also create hierarchical organizations of users and hierarchical categories of data to provide access control that is flexible, efficient, and simple to maintain.

The following sections provide understanding of access control mechanisms. The sections discuss:

- **Data.** The type of data and whether the data is categorized determines which access control mechanisms can be applied.
- **Parties.** People, entities representing people, and collections of people are unified as parties. Different party types have different access control mechanisms available.
- **Access control mechanisms.** Access control mechanisms you apply to parties and data determines what data a user sees.

Data

The following groupings are necessary for purposes of discussing access control:

- Master data
 - This data includes the following referential data: products, literature, solutions, resolution items, and competitors.
 - Master data can be organized into catalogs, which are hierarchies of categories. By categorizing master data, access can be controlled at the catalog and category levels through access groups. This is the recommended strategy for controlling access to master data.
 - Master data can be associated with organizations. By associating master data with organizations, access can be controlled at data item level. This strategy requires more administration than the access group strategy.

- Customer data
 - This data includes contacts and transactional data such as opportunities, orders, quotes, service requests, and accounts.
 - Access is controlled at the data item level.
- Other data
 - This data includes referential data that is not master data, such as price lists,, rate lists, and Smartscripts.
 - Access is controlled at the data item level.

Data Categorization

Master data can be organized into catalogs made up of hierarchical categories for two purposes:

- **Ease of navigation.** Categorized data is easier to navigate and search. For example, it is easy to find products of interest in a product catalog organized by product lines and subgroups of related products.
- **Access control.** Access to catalogs and categories of master data can be granted to collections of users. This is an efficient means to control data access in given business scenarios. For example, you can control partner users' access to your internal literature.

You can categorize master data to represent hierarchical structures, such as product catalogs, geographical categories, service entitlement levels, or channel partners.

A catalog is a single hierarchy of categories, as illustrated in [Figure 15](#).

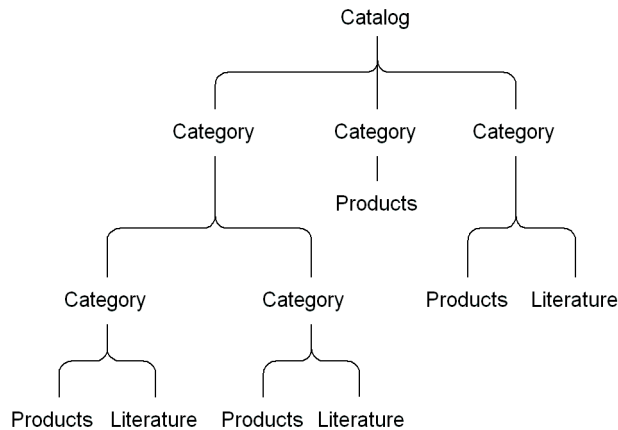


Figure 15. Catalog

The following properties apply to catalogs and categories:

- A catalog can be thought of as the name for an entire hierarchy of categories.
- Individual data items are contained in categories.
- A category can contain one or more types of master data.
- A category can be a node in only one catalog.
- A data item can exist in one or more categories, in one or more catalogs.
- A catalog can be public or private. If it is private, some access control is applied at the catalog level. If it is public, then all users can see this catalog, but not necessarily categories within this catalog, depending on whether the categories are private or public.

Parties

Individual people, groupings of people, and entities that represent individual or groupings of people are unified in the common notion of *parties*.

Parties are categorized into the following party types: Person, Organization, Position, User List, and Access Group. [Table 17](#) describes the qualitative differences among different parties.

Table 17. Parties

Party Type	Party	Examples	Distinguishing Features
Person	Person (or Contact)	<ul style="list-style-type: none"> ■ An employee at a customer company ■ An employee at a competitor's company 	<ul style="list-style-type: none"> ■ A Person is an individual who is represented by a Person record in the database. ■ Without additional attributes, a Person has no access to your database.
	User	<ul style="list-style-type: none"> ■ A registered customer on your Web site ■ A self-registered partner user, that is, one who has no position 	<ul style="list-style-type: none"> ■ A User is a Person who can log in to your database and has a responsibility that defines what views of data are accessible. ■ A self-registered partner on a Siebel partner application has a responsibility, but does not have a position like full partner users have.
	Employee	<ul style="list-style-type: none"> ■ An employee at your company 	<ul style="list-style-type: none"> ■ An Employee is a user who is associated with a position in a division within your company.
	Partner User	<ul style="list-style-type: none"> ■ An employee at a partner company 	<ul style="list-style-type: none"> ■ A Partner User is a user who is associated with a position in a division within an external organization. Therefore, a Partner User is also an Employee, but not an internal one.

Table 17. Parties

Party Type	Party	Examples	Distinguishing Features
	Position	<ul style="list-style-type: none"> ■ A job title within your company ■ A job title within a partner company 	<ul style="list-style-type: none"> ■ Positions exist for the purpose of representing reporting relationships. ■ A position within your company is associated with a division and is associated with the organization to which that division belongs. ■ A position within a partner company is associated with a division and is associated with the partner organization to which that division belongs. ■ A position can be associated with one division only. ■ A position may have a parent position. It may also have child positions. ■ One or more employees can be associated with an internal position, and one or more partner users can be associated with an external position. ■ An employee or partner user can be associated with more than one position, but only one position is active at any time.

Table 17. Parties

Party Type	Party	Examples	Distinguishing Features
Organization	Division	<ul style="list-style-type: none"> An organizational unit within your company such as Manufacturing or Corporate 	<ul style="list-style-type: none"> A division exists for the purposes of mapping a company's physical structure into the Siebel database and for providing a container for position hierarchies. A division may have a parent division. It may also have child divisions. Data cannot be associated directly with a division.
	Organization	<ul style="list-style-type: none"> An organizational unit within your company, such as your European organization A partner company 	<ul style="list-style-type: none"> An organization exists for the purpose of providing a container in which positions can be associated with data. An organization can be internal or it can be a partner organization. A division can also be designated as an organization. A division is associated with one organization, itself or an ancestor division that is also an organization.
	Account	<ul style="list-style-type: none"> A company or individuals with whom you do business 	<ul style="list-style-type: none"> An account is typically made up of contacts. An account is not a division, an internal organization, or an external organization. An account may have a parent account. It may also have child accounts. An account can be promoted to a partner organization.

Table 17. Parties

Party Type	Party	Examples	Distinguishing Features
User List	User List	<ul style="list-style-type: none"> ■ A support team made up of some internal employees and some partner users 	<ul style="list-style-type: none"> ■ A user list is an ad hoc group of people. It may have any combination of contacts, users, employees, and partner users as members. ■ A user list cannot have a parent or children.
Access Group	Access Group	<ul style="list-style-type: none"> ■ Your partner IT service providers and business-to-business customer companies that buy networking equipment ■ A partner community, such as the resellers of a particular sector of your product line 	<ul style="list-style-type: none"> ■ An access group is a group of any combination of parties of type Position, Organization, and User List. That is, it is a group of groups. ■ An access group may have a parent access group. It may also have child access groups.

Party Data Model

The S_PARTY table is the base table for all of the following single parties: Person (Contact), User, Employee, Position, Account, Division, Organization, and Partner Organization. Previously existing and new extension tables provide the differentiation between parties.

In [Figure 16 on page 256](#), the base table and extension tables that make up the party data model are shown within the Party boundary. The tables shown outside of the Party boundary are used to define relationships among parties.

In the Party schema, the previously-existing S_ORG_INT table is eliminated.

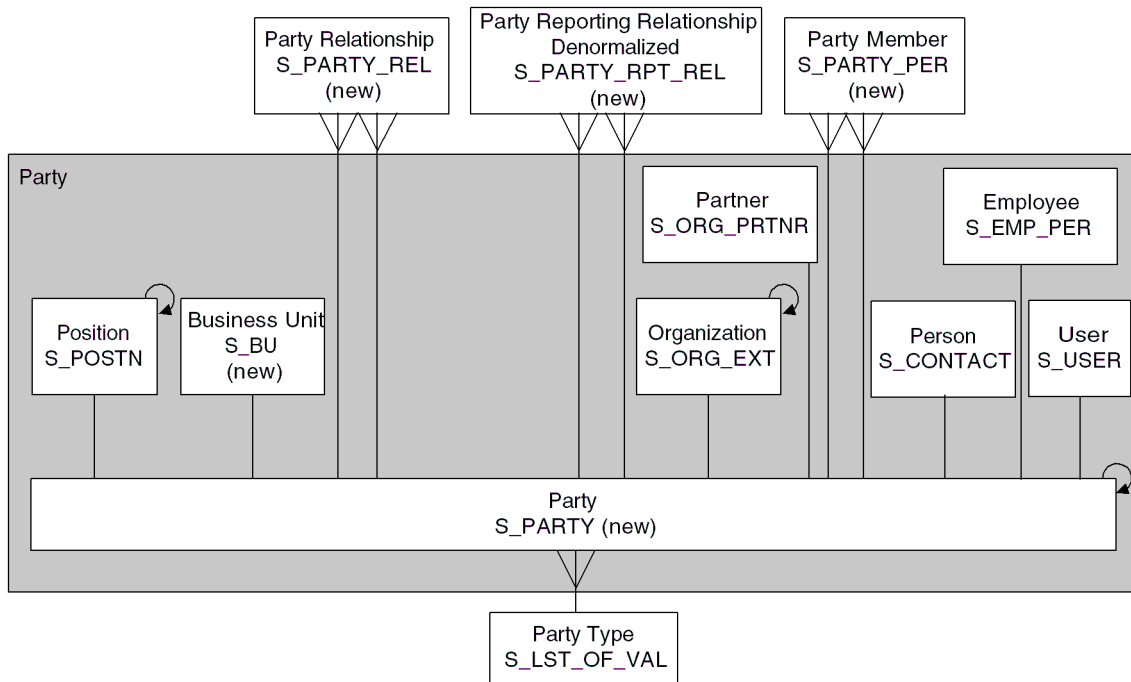


Figure 16. Party Data Model

In [Figure 17](#), the base table and extension table that define a Person, or Contact are shaded in the figure. A Person is the simplest representation of an individual in the database.

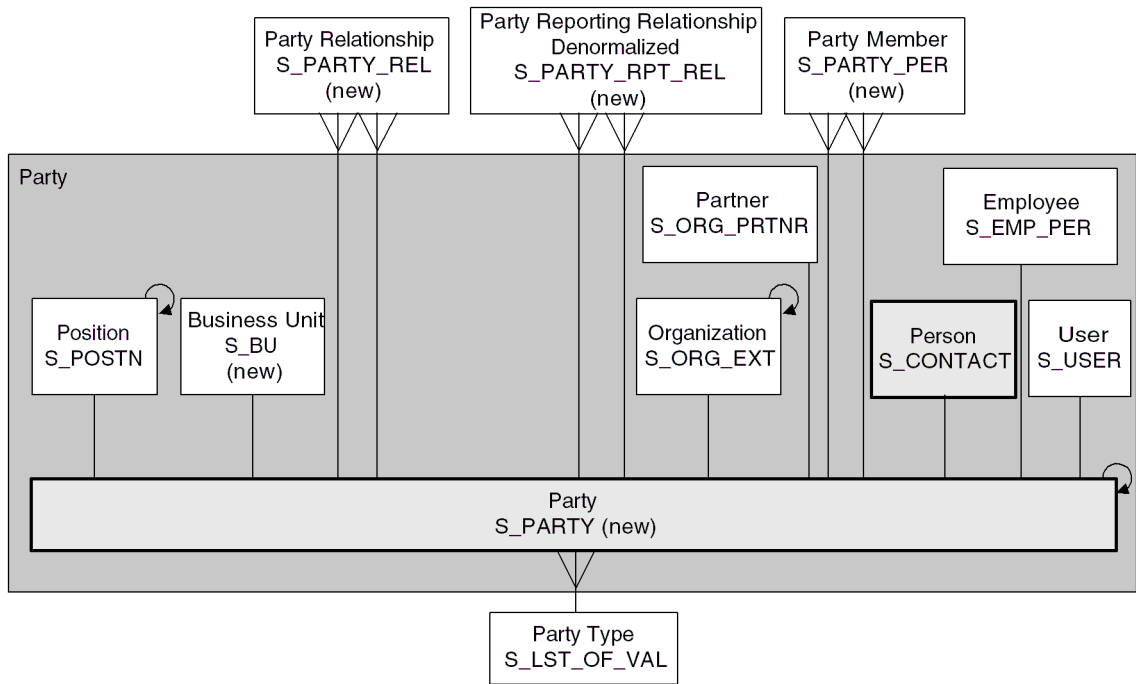


Figure 17. Person (Contact) Data Model

In [Figure 18](#), the base table and extension tables that define a User are shaded in the figure. A User is a Person with the following added qualities:

- S_USER contains a login for this user.
- The S_PER_RESP intersection table (not shown) specifies a responsibility for this user.

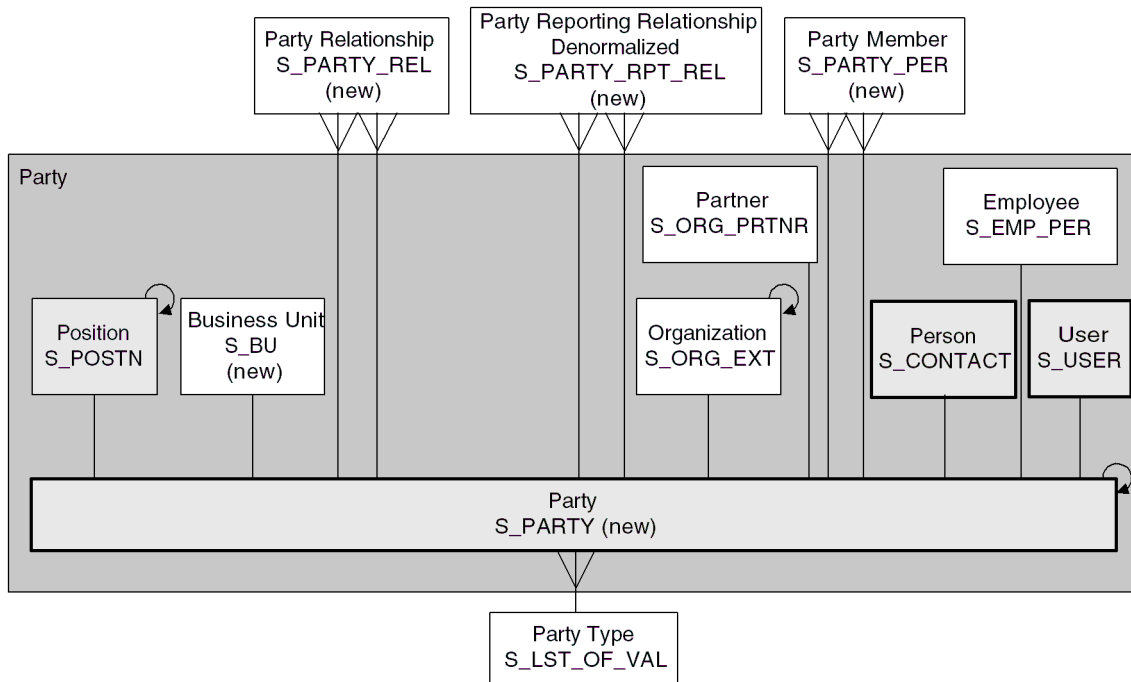


Figure 18. User Data Model

In [Figure 20](#), the base table and extension table that define a Position are shaded in the figure.

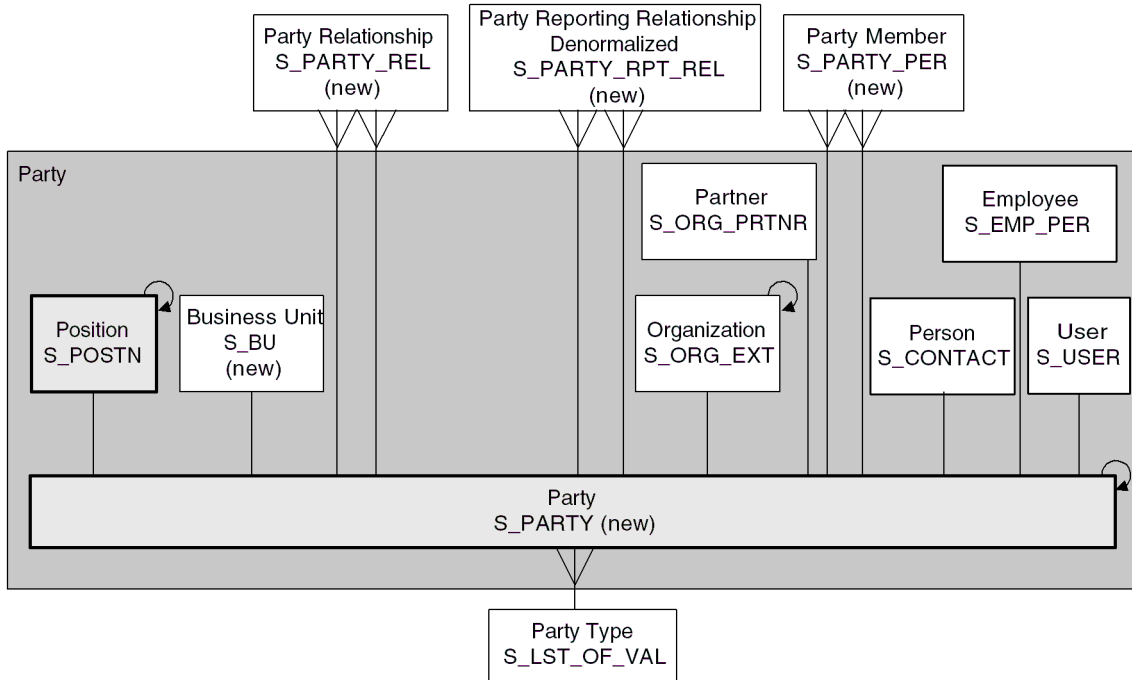


Figure 20. Position Data Model

In [Figure 21](#), the base table and extension table that define an Account are shaded in the figure.

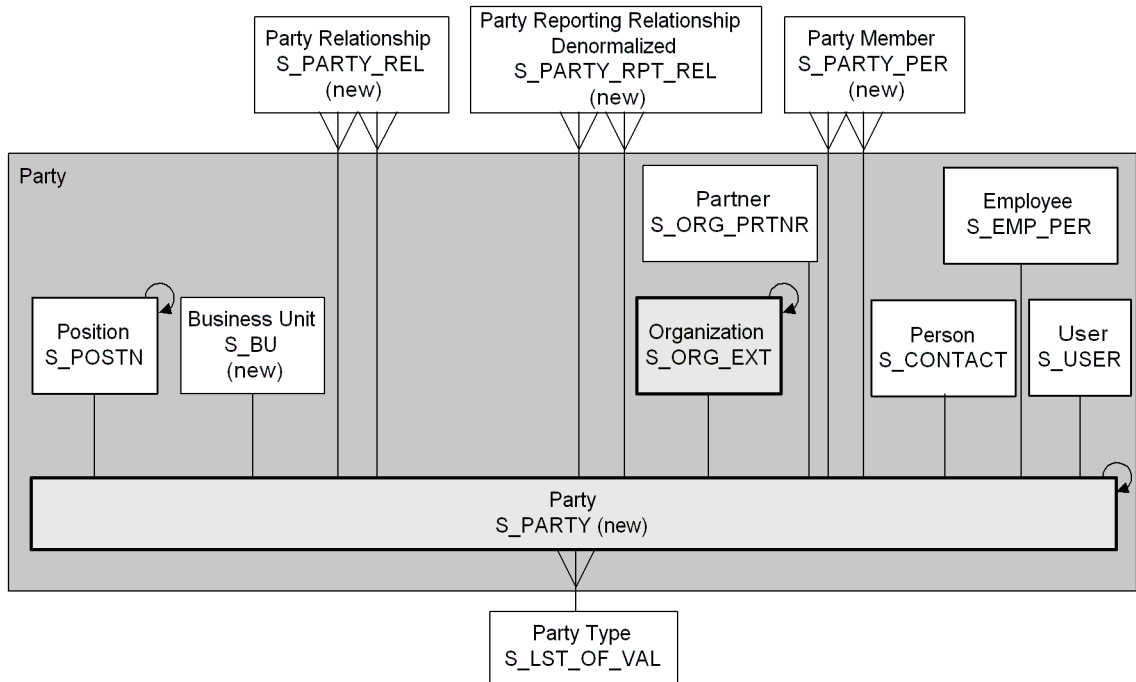


Figure 21. Account Data Model

In [Figure 22](#), the base table and extension tables that define a Division are shaded in the figure. In S_ORG_EXT, INT_ORG_FLG specifies that a division is an internal organization.

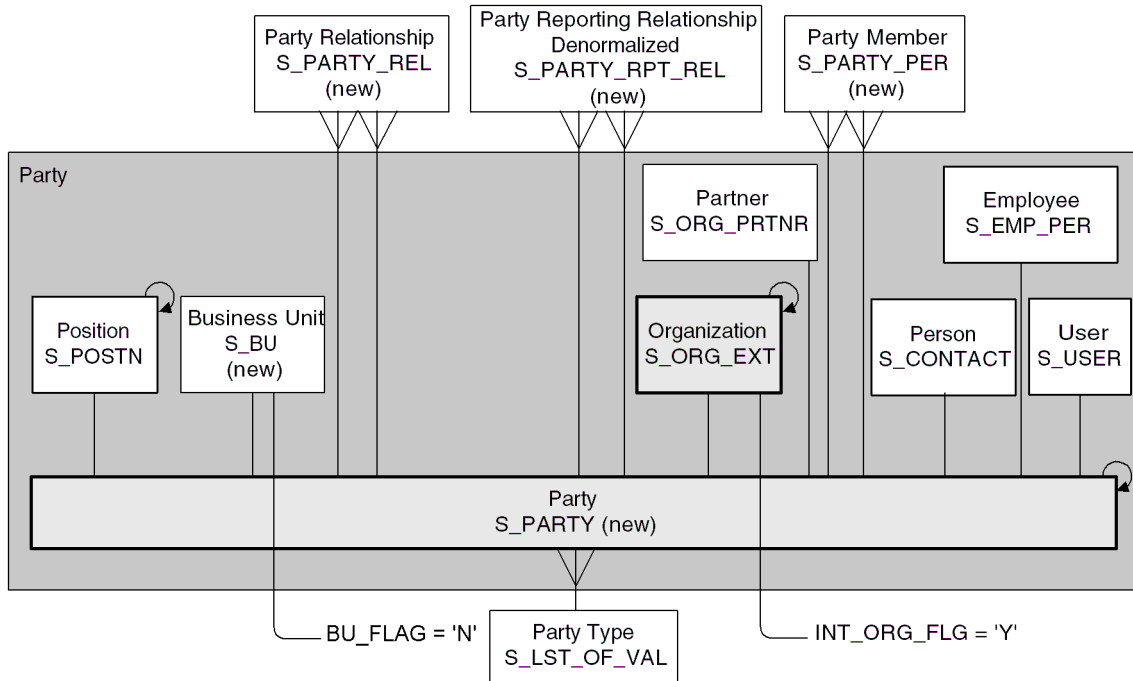


Figure 22. Division Data Model

In [Figure 23](#), the base table and extension tables that define an Organization are shaded in the figure. An Organization is a Division that is also a business unit.

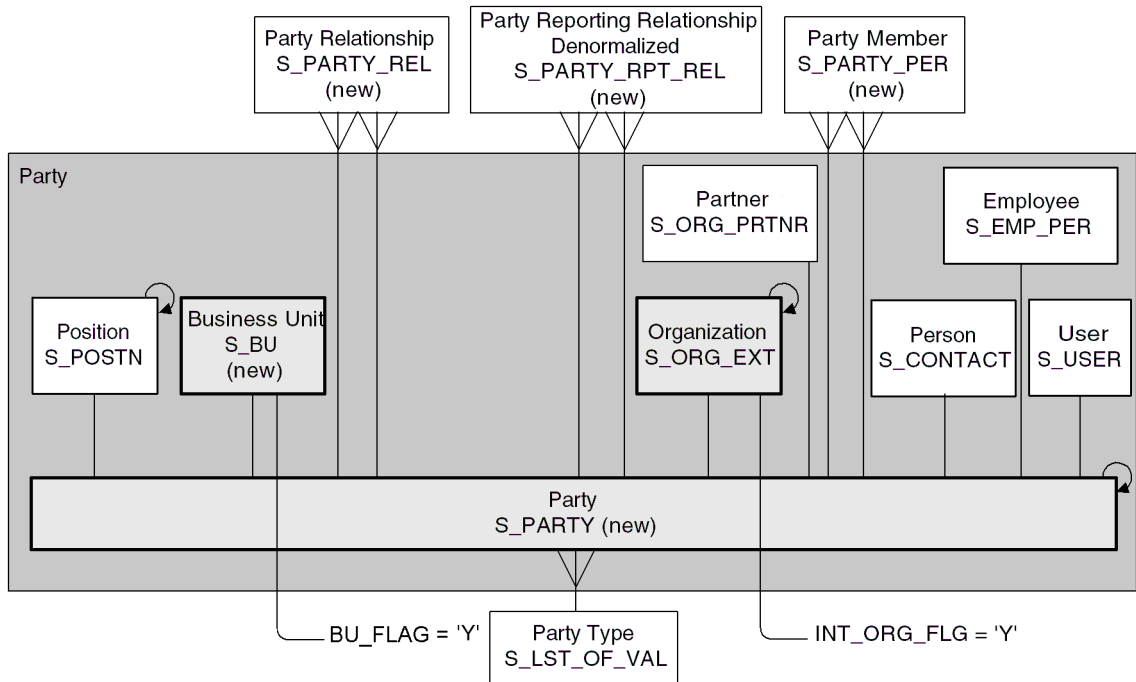


Figure 23. Organization Data Model

In [Figure 24](#), the base table and extension tables that define a Partner Organization are shaded in the figure.

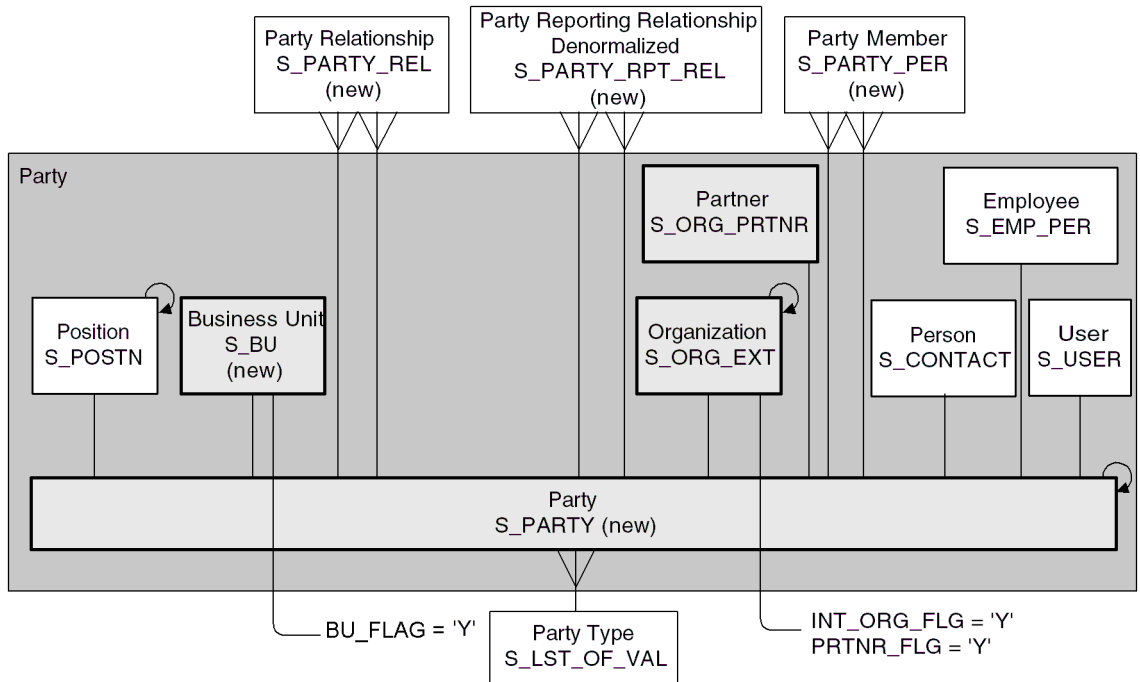


Figure 24. Partner Organization Data Model

How Parties Relate to Each Other

Parties have some required relationships, as described in the following list. References to “organization” in the following list are not to the party type, but to instances of that party type. Divisions, organizations, and accounts are instances of the Organization party type.

- A division, internal or partner, is also an organization if its internal organization flag is TRUE.
- Every division is associated with one organization, either itself or the closest ancestor division that is also an organization.
- Every position is associated with a division. The position is then also automatically associated with one organization, the organization with which the division is associated.
- Typically, you associate each employee and partner user with one or more positions. The employee or partner user can only log in one position at any time, so the employee or partner user is automatically associated with one division and one organization at a time—the division and organization associated with the position.

Access Control Mechanisms

The basic access control mechanisms include:

- Personal access control
- Position-based access control
- Organization-based access control
- *All* access control
- Access Group access control

Personal Access Control

If individual data can be associated with a user's Person record in the database, then you can restrict access to the data to that person.

Typically, you can implement personal access control when data has a creator or a person is assigned to the data, usually as the owner. The following are some examples:

- In the My Service Requests view, a Web site visitor can only see the service requests he or she has created.
- In the My Expense Reports view, an employee can see only the expense reports the employee has submitted for reimbursement.
- In the My Activities view, a user can see only the activities the user owns.

Some views that apply Personal access control are My Activities, My Personal Contacts, My Product Defects, My Service Requests, and Personal Address Book.

The words "My" and "My Personal" are frequently in the titles of views that apply Personal access control. However, "My" does not always imply Personal access control. Some "My" views apply position- or organization-based access control. For example, the My Opportunities view applies position-based access control.

Frequently different views have the same name because they are used in similar, but different, contexts. Some views under a given name may apply Personal access control, while others with the same name may apply position- or organization-based access control.

For information about business component view modes, see "[Business Component View Modes](#)" on page 295.

For information about implementing access control in a view, see "[View Access Control Properties](#)" on page 302.

Position-Based Access Control

A position is a job title in a division of an internal or partner organization. A position hierarchy represents reporting relationships among positions. Positions provide an appropriate basis for access control in many scenarios because a position in an organization is typically more stable than the individual's assignment to the position.

Customer data and some types of referential data can be associated with one or more positions. If individual data can be associated with a position, then you can apply position-based access control to the data by one or more of the following means:

- **Single position.** You can associate a single position to individual data.
- **Sales Team.** You can associate multiple positions, in the form of a team, to individual data.
- **Manager.** You can grant access concurrently to data associated with a position and data associated with subordinate positions in a reporting hierarchy.

An employee or partner user can be associated with one or more positions, of which one can be the active position at a given time. All position-based access control for an employee or partner user is determined by the active position.

One of the user's positions is designated as the primary position. When a user logs in, the primary position is the active position. To make a different position the active position, one of the following must happen:

- An employee must designate another position as the active position.
- A partner user must designate another position as the primary position, and then log in again.
- You can configure an agent who uses Siebel Call Center or Siebel Service, MidMarket Edition to automatically change positions based on the data provided for an incoming service call.

For information about administering positions, see *Applications Administration Guide, MidMarket Edition*.

For information about agent setup, see *Siebel Communications Server Administration Guide, MidMarket Edition*.

Single Position Access Control

You can associate a single position to individual data. For example, in the My Quotes view, an employee logged on in a particular position can see only the Quotes associated with that position. The My Quotes view applies single position access control.

The word “My” is frequently in the titles of views applying single position access control. However, “My” does not always imply single position access control. Some “My” views apply personal, organization-based, or position-based sales team access control. For example, the My Activities view applies personal access control.

A business component’s view modes determine whether single position access control can be applied in a view that is based on the business component. To have single position access control available, a business component must have a view mode (usually Sales Rep) of owner type “Position” with an entry in the Visibility Field column (instead of the Visibility MVField column).

For information about business component view modes, see [“Business Component View Modes” on page 295](#).

For information about implementing access control in a view, see [“View Access Control Properties” on page 302](#).

Sales Team Access Control

You can associate multiple positions, in the form of a team, to individual data. For example, in the My Opportunities view, an internal employee or partner with a particular active position can see all the opportunities for which that position is included in the opportunity’s Sales Team.

A team may include internal and partner positions.

The display names for fields representing position teams vary with the view in which they appear. Some common views that apply sales team access control follow, with the display names for their teams:

- The My Opportunities view has a Sales Team field.
- The My Accounts view has an Account Team field.
- The My Contacts view has an Access List field.
- The My Projects view has an Access field.

Although the field for the sales team can contain multiple positions, only one name is displayed without drilling down. In a view that uses sales team access control, for example My Projects, the name of the active login is displayed. Other views, such as those using organization access control, may also have a field for the sales team. In these other views, the name of the login that occupies the primary position is displayed.

The word *My* is frequently in the titles of views applying sales team access control. However, *My* does not always imply sales team access control. Some *My* views apply personal, organization-based, or single position access control. For example, the My Activities view applies personal access control.

A business component's view modes determine whether Sales Team access control can be applied in a view that is based on the business component. To have Sales Team access control available, a business component must have a view mode (usually Sales Rep) of owner type "Position" with entries in the Visibility MVField and Visibility MVLink columns (instead of the Visibility Field column).

One of a sales team's members is designated as the primary member. The primary member is a factor in Manager access control, but not in Sales Team access control.

For information about business component view modes, see "[Business Component View Modes](#)" on page 295.

For information about Manager access control, see "[Manager Access Control](#)" on page 269.

For information about implementing access control in a view, see "[View Access Control Properties](#)" on page 302.

Manager Access Control

You can indirectly associate a position with data associated with subordinate positions in a reporting hierarchy. For example, in the My Team's Opportunities view, an employee with a particular active position can see opportunities associated with that position and opportunities associated with subordinate positions.

NOTE: If an employee's position has no subordinate positions, the employee sees no data in views that use Manager access control, not even the employee's own data.

Manager-subordinate relationships are determined from a position hierarchy. One position hierarchy is included as seed data when you install your Siebel application.

You can specify one parent position for a position, which represents that the position is a direct report to the parent. The parent of an internal position may be in the same division or a different division. For example, a sales manager in the Sales division may report to a sales vice-president in the Corporate division.

In a view using Manager access control, the employee or partner has access to the following data:

- If the business component on which the view is based uses single position access control, the user sees data associated directly with the user's active position or with subordinate positions.
- If the business component on which the view is based uses sales team access control, then the user sees data for which the user's active position is on the team or a subordinate position is the primary member on the team.

Views that apply Manager access control generally contain the phrase "My Team's" in the title, such as My Team's Accounts. The word "My" is sometimes omitted, as in Team's Activities.

There are no business component view modes specific to Manager access control. Manager access control is set at the view level. It requires that the business component on which the view is based has a view mode with Owner Type Position.

For information about business component view modes, see ["Business Component View Modes" on page 295](#).

For information about administering positions, see *Applications Administration Guide, MidMarket Edition*.

For information about implementing access control in a view, see ["View Access Control Properties" on page 302](#).

Organization-Based Access Control

When individual data can be associated with an organization, you can apply organization-based access control to the data by one or more of the following means:

- **Single Organization.** You can associate a single organization with individual data.

- **Multiple Organization.** You can associate multiple organizations with individual data.
- **Sub-Organization.** You can grant access concurrently to data associated with an organization and data associated with subordinate organizations in the organizational hierarchy.

Siebel Territory Assignment Manager is also organization-enabled; that is, assignment rules can use organization as a criterion.

A user is associated with one organization at any given time, the organization to which the user's active position belongs. For information about changing the active position of an employee or a partner user, see [“Position-Based Access Control” on page 267](#).

A contact user is indirectly associated with an organization through the proxy employee specified for a Siebel customer application.

For information about proxy employees, see [“User Authentication” on page 63](#) and [“Seed Data” on page 345](#).

For information about administering organizations and divisions, see *Applications Administration Guide, MidMarket Edition*.

Single Organization and Multiple Organization Access Control

Depending on the type of data, you can associate one or more organizations to individual data. The user can see data that is associated with the user's active organization. For example, in the All Service Requests view, a user can see all the service requests associated with the user's active organization.

For data that can be associated with multiple organizations, one of the organizations is designated as the primary organization. The primary organization is a factor in sub-organization access control, but not in multiple organization access control.

[Table 18](#) lists data on which you can apply organization-based access control and whether a single or multiple organizations can be associated with the data.

Table 18. Organization-Enabled Data

Object Type	Object	Relationship
Customer data	Account	Multiple
	Competitor	Multiple
	Contact	Multiple
	Opportunity	Multiple
	Order	Multiple
	Partner	Multiple
	Quote	Multiple
	Service Request	Multiple
Referential data	SmartScript	Multiple
	Literature	Multiple
	Price List	Multiple
	Product	Multiple
	Catalog	Multiple
Administrative data	Employee	Single
	Division	Single
	Position	Single
	Responsibility	Multiple
Other	Rate list	Multiple
Assignment Manager	Assignment Manager	Enabled

All (but not *All across*) is frequently in the titles of views applying single or multiple organization access control. For example, the All Contacts view applies single organization access control, and the All Product Defects view applies multiple organization access control. However, *All* does not always imply single or multiple organization access control. Some *All* views apply *All* access control. For example, the All Service Requests view applies *All* access control.

A business component's view modes determine whether single organization or multiple organization access control can be applied in a view that is based on the business component. To have single organization access control available, a business component must have a view mode (typically Organization) of Owner Type Organization with an entry in the Visibility Field column (instead of the Visibility MVField column). To have multiple organization access control available, a business component must have a view mode (typically Organization) of Owner Type Organization with entries in the Visibility MVField and Visibility MVLink columns (instead of the Visibility Field column).

For information about *All* access control, see [“All Access Control” on page 274](#).

For information about business component view modes, see [“Business Component View Modes” on page 295](#).

For information about implementing access control in a view, see [“View Access Control Properties” on page 302](#).

Sub-Organization Access Control

Sub-organization access control, based on hierarchical organizations, is analogous to Manager access control, based on hierarchical positions.

For any organization in the organizational hierarchy, you can grant access to data associated with subordinate organizations. This access control mechanism is designed to provide roll up views of data. For example, a director of a continental sales organization can see the data rolled up from subordinate regional sales organizations. A vice president in the corporate sales organization can then see roll ups of the continental sales organizations and the regional sales organizations.

Subordinate relationships are determined from the organizational hierarchy, as an administrator can view by choosing View > Site Map > Group Administration > Organizations. The organizational hierarchy is included as seed data when you install your Siebel application. Within the organizational hierarchy, you can create branches for both internal and partner organizational structures.

You can specify one parent organization for an organization.

In a view using sub-organization access control, the user has access to the following data:

- If the business component on which the view is based uses single organization access control, the user sees data associated directly with the user's active organization or with a descendent organization.
- If the business component on which the view is based uses multiple organization access control, then the user sees data for which the user's active organization or a descendent organization is the primary organization.

The titles of default views applying sub-organization access control are structured as *All business component name across My Organizations*, such as All Opportunities across My Organizations.

There are no business component view modes specific to sub-organization access control. Sub-organization access control is set at the view level. It requires that the business component on which the view is based has a view mode with Owner Type Organization.

For information about business component view modes, see [“Business Component View Modes” on page 295](#).

For information about implementing access control in a view, see [“View Access Control Properties” on page 302](#).

For information about administering organizations and divisions, see *Applications Administration Guide, MidMarket Edition*.

All Access Control

All access control provides access to all records that have a valid owner, as defined in any of the business component's view modes. The owner may be a person, a position, a valid primary sales team position, or an organization, depending on the view modes that are available for the business component.

All users with a view in their responsibilities that applies *All* access control see the same data in the view. A user's person or position need not be associated with the data.

All visibility essentially provides a view of data across all organizations. For example, in the All Quotes across Organizations view, a user sees all the quotes that are associated with any internal or external organization in the enterprise, for which there is a valid person, position or organization owner.

The phrases *All across* and *All* are frequently in the titles of views applying *All* access control. For example, the All Opportunities across Organizations and the All Service Requests views apply *All* access control. However, *All* does not always imply *All* access control. Some *All* views apply Single or multiple organization access control. For example, the All Contacts view applies single organization access control.

A separate property (Admin Mode) provides the means to see all records in a view using Sales Team access control, including those without a valid owner. Admin mode allows the administrator to modify records that otherwise no one could see. You specify Admin mode for a view in the Admin Mode Flag property.

There are no business component view modes specific to *All* access control. *All* access control is set at the view level.

For information about business component view modes, see [“Business Component View Modes” on page 295](#).

For information about implementing access control in a view, see [“View Access Control Properties” on page 302](#).

For information about Admin mode, see [“View Access Control Properties” on page 302](#).

Access Group Access Control

Access group access control is a means to control access by groups of diverse party types to categorized master data.

An access group is a collection of any combination of positions, organizations, divisions, accounts, and user lists. Its members are instances of party types other than Person, that is, its members cannot be individual people. For example, an access group could consist of several partner organizations and user lists to which you want to grant access to a particular set of your sales tools.

A user is associated with an access group if, during the current session, the user is associated with a position, organization, division, account, or user list that is a member of the access group.

You can create hierarchies of access groups. An access group can belong to only one access group hierarchy. That is, an access group can have only one parent access group. For example, the access group mentioned above might belong to a hierarchy of access groups for the purpose of granting differing levels of access to sales tools.

You can grant access groups access to catalogs and categories of master data: products, literature, solutions, resolution items, and competitors. For example, branches in the access group hierarchy above could be granted access to categories in a hierarchical catalog in which each category contains sales literature and competitive briefs.

A category of master data can contain any combination of master data items. You can only control access to catalogs and categories of master data. You cannot control access to individual master data using access group access control.

When access groups are associated with a catalog or with categories in the catalog, you can apply access group access control. You can control access to the data in one of the following ways:

- **Group.** While in a given category, the user sees either a list of the category's first-level subcategories (child categories) to which he or she has access or all the data records in the current category, depending on the applet being used. If the user is at the catalog level, the user sees the first level categories.
- **Catalog.** The user sees a flat list of all the data in categories across all catalogs to which the user has access. This visibility type is typically used in product pick lists and other lists of products, such as a recommended product list.

For more information about data and data categorization, see [“Data” on page 249](#).

For more information about parties, see [“Parties” on page 252](#).

For information about administering access group access control, see [“Administering Access Group Access Control” on page 308](#).

Planning for Access Control

Two main strategies are available for controlling access to data in Siebel applications:

- **Access group access to catalogued data.** This strategy can be implemented with all party types. It is designed to reduce access control administration by associating hierarchical groups of users with similarly organized data. It is limited to master data.
- **Multiple-organization access control.** This strategy limits data access to only those organizations that have a need to see the information. Organizational access control can be implemented across internal or external organizations. This strategy can be applied to transaction data, master data, and other referential data.

For analysis and recommendations for choosing and implementing access control strategies, see *Access Control Upgrade and Migration Guide for Siebel 7* on the Siebel SupportWeb site.

Business Environment Structure

As part of implementing an access control strategy for your application, you must define your company's structure, outside partner relationships, and so on. How you define the structure of your business environment will impact the records and views users will be able to access.

This section provides some background information about business environment structure. If your business enterprise is complex, you can accurately reflect its structure in your Siebel application's setup. You can build multilevel hierarchies of organizations, divisions, and positions. You build a hierarchy by associating positions, for example, with other positions through parent-child relationships.

Defining your business environment structure involves setting up the categories shown in [Table 19](#).

Table 19. Elements of Business Environment Structure

Element	Parent-Child	Description
Organizations	Y	The major parts or entities that make up your company (or your partner companies). Used to control visibility of data.
Divisions	Y	Subunits of your company's (or partner company's) organizations. Used to set default currencies. Can be used in Actuate reports.
Positions	Y	Control the data set (records) to which a user has access.
Responsibilities	N	Control the views to which a user has access.
Employees	N	Individual users in your company and in channel partners who have access to your company's data.

For more information about how your Siebel application uses business environment structure, see *Siebel Territory Assignment Manager Administration Guide, MidMarket Edition*.

You can set up organizations, divisions, positions, responsibilities, and employees in any order. You can also associate these types of records with one another in a variety of ways. For example, to link a responsibility and an employee, you can associate the employee with the responsibility in the responsibility record, or you can associate the responsibility with the employee in the employee record.

CAUTION: Changing your company structure—such as positions and divisions—can cause routers to reevaluate visibility for all objects related to the objects that have changed. This can result in diminished performance. For more information, see *Siebel Remote Administration Guide, MidMarket Edition*.

Benefits of Organizations

Using organizations provides the following benefits:

- It allows your company to partition itself into logical groups, and then display information appropriate to each of those groups.
- It provides the ability to limit visibility (access) to data based on the organization to which positions are assigned.
- It affects both customer data (accounts, opportunities, service requests, and so on) and master data (price lists, literature, and so on).
- It allows you to set up multitenancy for call centers. For more information, see *Siebel Communications Server Administration Guide, MidMarket Edition*.

Deciding Whether to Set Up Multiple Organizations

If your Siebel application is already deployed and you do not need to change your users' visibility, your company may not need more organizations. Some circumstances where your company could benefit from multiple organizations are as follows:

- **Internal business units.** If you have a small number of distinct internal business units, you may want to use organizations to support specific versions of a limited number of data entities such as products and price lists.
- **Complex multi-region enterprise.** If you have an enterprise that encompasses multiple internal and external businesses in different regions, each of which is made up of multiple business units, your company will benefit from implementing organizations. In this circumstance, some data should be available only to some units, while other information must be shared at the corporate level.
- **Internal and external units.** If your company shares data with external partner companies, you can set up each of these companies as an organization. You may make fewer views available to these external organizations than to your internal organizations. You may also configure the employee drop-down list so that it shows only employees who belong to the user's organization.

- **Different rules for business units.** If you would like to make different Territory Assignment Manager Workflow rules apply to different parts of your company, then your company will benefit from implementing organizations. For example, a company might want some Territory Assignment Manager rules to apply to a telesales organization and other rules to apply to partners through the Siebel Partner Portal.
- **Web-enabled enterprise.** If you have customers that log in through a Web site, you can set up a customer organization to control their access to views and data. If you have channel partners who log in through a Web site, you must set up channel partner organizations to control their access. For more information on using organizations with Siebel customer and partner applications, see *Siebel Partner Relationship Management Administration Guide, MidMarket Edition*.

Defining a Company Structure

The following sections explain the common tasks for defining a company structure in your Siebel application. These include tasks for defining the following entities:

- Organizations
- Divisions
- Responsibilities
- Positions

Organizations

Organizations are designed to represent the broadest divisions of your company. An organization controls the data access of the employees that are assigned to it. Organizations can be internal, or they can be external (in the case of Siebel PRM).

NOTE: Technically, internal organizations are divisions, because at the data model level they are divisions with a business unit flag (BU_FLG) selected.

Setting up organizations is an optional step in your implementation. If you are upgrading from a previous version of your Siebel application, all the data is automatically assigned to one default organization. With one organization, there is no impact on visibility and data access. However, if you wish to divide your company into multiple structural units, you can create multiple organizations.

NOTE: You cannot delete organization records. Business components throughout your Siebel application refer to organization records. Deleting an organization could cause invalid references on transaction records. This could lead to unexpected negative results, such as valid data not appearing in the user interface.

You may want to delegate administration of users to organizations that access only their users. To do this, you must configure the appropriate views using Siebel Tools. For more information on configuring views, see *Siebel Tools Reference, MidMarket Edition*.

Setting Up Organizations

This section describes procedures for setting up organizations.

To set up an organization

- 1 From the application-level menu, choose View > Site Map > Group Administration > Organizations.

The Organizations view appears.

- 2 In the More Info form, add a new record and complete the necessary fields.

Some fields are described in the following table.

Field	Comments
Parent Organization	If this organization is a suborganization, select the parent organization. This allows an organization to be associated with another organization.
Partner Manager Position	Used for partner relationship management. Person in the organization who manages the relationship of that particular channel partner. Used in fund requests as the default value in the "Assign to" column. For more information, see <i>Siebel Partner Relationship Management Administration Guide, MidMarket Edition</i> .
Partner Flag	When selected, indicates that the organization represents an external enterprise that is a partner of your company.

CAUTION: It is recommended that you do not change the name of the default organization. It is seed data and is referenced in many places. If your company decides to change the default organization name, you must be aware that the default organization must have a name that is unique from any other organization or division name. If you are using Workflow, you need to rename references in Assignment Objects to the new name for Default Organization. For more information about these procedures, see *Siebel Tools Reference, MidMarket Edition*.

Setting Up Divisions

Divisions belong to organizations and have no direct effect on visibility. Divisions help you to group positions, to record addresses, and to maintain default currencies. User reporting structures are defined by their parent positions, but their country of operation and currency are defined by their division. Divisions can also be used by Actuate reports. For more information on reports, see *Siebel Reports Administration Guide, MidMarket Edition*. To implement Siebel eBusiness Applications, you must set up at least one division.

You can assign divisions to organizations. You can also promote a division to an organization. Multiple divisions can be arranged in a multilevel hierarchy by assigning some divisions as the parents of others.

You can assign positions to a division. When you associate employees with those positions, the employees become associated with the division.

NOTE: You cannot delete division records because business components throughout your Siebel application refer to organization records. Deleting a division would cause invalid references on transaction records. This would lead to unexpected negative results such as valid data not appearing in the user interface.

To set up a division

- 1 From the application-level menu, choose View > Site Map > Group Administration > Divisions.

The Divisions view appears.

- 2 In the More Info form, add a new record and complete the necessary fields.

Some fields are described in the following table.

Field	Comments
Parent Division	If this division is a subdivision, select the parent division. This allows a division to be associated with another division.
Organization Type	Read-only. Name of the organization the division belongs to.

Field	Comments
Organization Flag	When selected, indicates that the division is also an organization. The system copies that division into the Organization view.
Partner Manager Position	Used for partner relationship management. Person in the organization who manages the relationship of that particular channel partner. Used in fund requests as the default value in the "Assign to" column. For more information, see <i>Siebel Partner Relationship Management Administration Guide, MidMarket Edition</i> .

Setting Up Positions

A position represents a specific job slot within your company. As you define your company structure, define specific positions with each level in the hierarchy of divisions. Positions determine which records users have access to. You must be logged on to a server database to add positions.

NOTE: An employee should have a position in order to create and use accounts, opportunities, contacts, and other customer data objects in your Siebel application.

Each position typically has only one associated employee. In some circumstances such as job-sharing situations, a position may have multiple associated employees. One employee can be associated with multiple positions. There can be only one primary employee for a position, but an employee can be primary for more than one position.

There is a drawback to having multiple employees associated with a position. Because a position can have only one primary employee, only the primary employee is visible in the Employee field. If you search for an employee in a positions list, you may not find relevant position records in which the employee is not primary for the position.

Only the primary employee for a position appears in the Account Team, Opportunity Sales Team, and Contact Access lists. However, all the employees in that position can access the My Accounts, My Opportunities, and My Contacts views.

A position can be associated with only one organization. If you want an employee to have visibility to multiple organizations, you must create a position for each organization and assign that employee to each position. The employee can then see one organization's data at a time by changing positions.

Positions can be set up in a multilevel hierarchy. In this case, the parent position gains visibility to all the sets of data visible to the child positions individually.

Your Siebel application allows users to change their position to any other position in the organization. A user can change positions while logged in by choosing View > Site Map > User Preferences > Change Position and selecting a different position in the list. For instance, a sales representative could change position to a sales executive and have access to the same views as the previous position, but gain visibility to another organization's data.

NOTE: You cannot make a position obsolete by setting the End Date. This field records only the end date for the current employee associated with the position. It does not make the position obsolete after that date has passed.

CAUTION: Do not delete a position. This can cause unexpected and negative results. For example, if you delete a position that is primary for an account, and you do not select a new primary position for that account, Territory Assignment Manager may not be able to assign resources to activities for that account.

If you rename a position, check these areas in your Siebel application to make sure the name change is reflected correctly:

- Territory Assignment rules, if you have used these positions in assignment rules. For more information, see *Siebel Territory Assignment Manager Administration Guide, MidMarket Edition*.
- Workflow processes, if you have used these positions in workflow processes. For more information, see *Siebel Business Process Designer Administration Guide, MidMarket Edition*.
- Enterprise Integration Manager (EIM), if you are referring to these positions in EIM import SQL scripts. For more information, see *Siebel Enterprise Integration Manager Administration Guide, MidMarket Edition*.
- The Position field of the Employees view.

In positions, as in other areas of your Siebel application, seven foreign key references are implemented with the ROW_ID column in the base tables. The ROW_ID column is not visible in the user interface and cannot be changed manually. This is because the integrity between the various base tables would be lost if users were allowed to change this value. Changing a position name does not affect the foreign keys (the ROW_ID in the underlying base table).

A special consideration for mobile users is as follows: If you change a mobile user's position, that user's visibility rules change. In this case, it is recommended that the user reextract his or her local database. However, if you change only the position name (for example, from Sales Representative to Sales Associate), then the reextraction is not required. This is because position names are stored in the S_POSTN table, and this column has enterprise-wide visibility. In other words, changes to this column will be distributed to all users.

To set up a position

- 1 From the application-level menu, choose View > Site Map > Group Administration > Positions.

The Positions view appears.

- 2 In the More Info form, add a new record and complete the necessary fields.

Some fields are described in the following table.

NOTE: Most fields in the More Info form are filled in automatically from the Employee record of the active employee. If you have not set up employees, you can associate them with positions later.

Field	Comments
Billing Product	Used by Siebel Professional Services Automation.
End Date	Last day for the currently associated employee to be associated with this position.
Last Name	Select one or more employees to occupy the position. In the Assigned Employees dialog box, select the Primary field for the employee whom you want to make primary for this position.
Parent Position	If this position is a subposition, select the parent position. This allows a position to be associated with another position.

Field	Comments
Position Type	Type of position. This field is informational and has no impact on visibility.
Territory	Allows a position to be associated with a territory. For use by Territory Assignment Manager.

Defining Responsibilities

Responsibilities determine which views users have access to. For example, the System Administrator responsibility allows access to all views. Defining responsibilities lets you limit user access to views, and therefore to your Siebel application's information and functions. You must assign responsibilities to all users. Without a responsibility, a user cannot use the Siebel application, because that user cannot access any views.

Define responsibilities that correspond to the major job functions in your organization. For example, you might create responsibilities for the marketing administrator, the sales manager, and sales representatives. The sales representative responsibility might have access to all views except those reserved for sales management, marketing administration, and applications administration. The sales manager responsibility might have access to the same views as the sales representative, plus the Sales Manager views, and so on.

To define a responsibility, you must specify which views are available to that responsibility. You can use the seed responsibilities that come with your Siebel application. These can be copied and then customized.

NOTE: You cannot modify or delete the seed responsibilities. For instance, you cannot change the SADMIN responsibility. You can copy the seed responsibilities and modify the copies.

When you are defining responsibilities, consider the following issues:

- You should grant access to the System Preferences view to only a selected group of administrators. End users should not be given access to the System Preferences view. System preferences control many things throughout the system, for example server logic and processing for Siebel Remote and Territory Assignment.

- You should not add Administration views to responsibilities associated with end users. Likewise, you should limit access to the Mobile Clients, Responsibilities, Views, and Territories views. The work performed with these views has far-reaching implications for the entire application.
- You may want to hide access to license keys by deleting the license key-related views from a user's responsibility. For more information, see *Applications Administration Guide, MidMarket Edition*.
- If you add the Internal Division View to a user's responsibility, all organizations in the Organizational picklist are displayed. By default, only the organization the user belongs to appears in this list.

To define a responsibility

- 1** From the application-level menu, choose View > Site Map > Application Administration > Responsibilities.

The Responsibilities view appears.

NOTE: By default, the Responsibilities view shows all responsibilities, regardless of organization. However, you may want to configure new views in Siebel Tools that restrict the visibility to responsibilities. For more information on configuring views, see *Siebel Tools Reference, MidMarket Edition*.

- 2** In the Responsibility list, add a new record and enter a name and description for the responsibility.
- 3** In the Organization field, select an organization for the responsibility.
- 4** To add views, do the following:
 - a** In the Views list, add a new record.
 - b** Select the appropriate views in the Add Views dialog box and click OK.

NOTE: You can also delete views from the Views list.

- 5 To add users, do the following:
 - a In the Users list, add a new record.
 - b Select the appropriate users in the Add Users dialog box and click OK.

NOTE: You can also delete employees from the Users list.

Implementing Basic Access Control

The particular data exposed in a view and whether a view is exposed at all are determined by settings made for related components.

You configure most of these settings in Siebel Tools. This section specifies where to find these settings within Tools, but in most cases does not provide procedures to implement them. Changing any settings in Siebel Tools requires recompiling the Siebel repository file.

For more information about required practices when using Siebel Tools, see *Siebel Tools Reference, MidMarket Edition*.

The following components determine what views a user sees.

- **Application.** Each Siebel application includes a licensed set of views. When a user is in an application, the user has no access to views that are not included in the application.
- **Responsibilities.** Every user has one or more responsibilities, which define the collection of views to which the user has access. If a particular view is not in a user's responsibilities, then the user does not see that view. A wide-ranging view such as All Opportunities Across Organizations is not typically included in the responsibility for an employee such as a district sales rep.

The following components determine the data within a view to which a user has access.

- **Business component view mode.** A view can have several applets— lists, forms, or trees. Each applet is based on a business component. The business component’s view mode determines the allowable parties on which access control can be based for that business component. The business component’s view modes also determine how the association with the party will be determined, for example “owned by” or “created by.”
- **Applet visibility properties.** A view can specify one of its applets as the visibility applet. The visibility applet connects the business component to the view. The visibility applet specifies which business component to use and the display names for the business component’s fields.
- **View visibility properties.** A view’s visibility properties determines the access control mechanism that is applied to the business component on which the view is based. For example, the business component may have personal or position-based access control available. The view specifies which of these to use, and in which form to use it.

In short, the application and a user’s responsibility restrict the views presented to the user. Within a view, view visibility properties determine the applet that drives visibility in the view and specifies the access control mechanism to apply to the business component. The view’s visibility applet specifies the business component used in the view. The business component specifies how a user can be associated with data to provide access.

Application Level Access Control

Each Siebel application is associated with a set of screens. Each screen is in turn made up of a set of views.

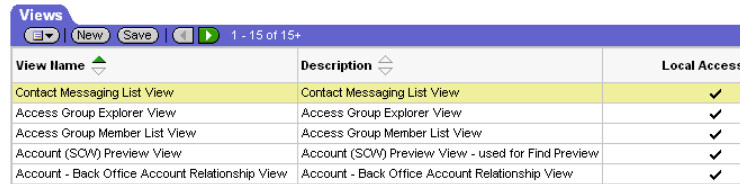
In a particular application, all users are limited to the views that are licensed to your company and that are defined for the application. The licensed views are specified in the license key, which is determined by the features you purchase for your Siebel eBusiness application.

To see an application’s views

- 1 Log in as an administrator, and then click the Application Administration screen tab.

- 2 In the Show drop-down list, select Views.

This figure shows a sample list of views defined for an application.



View Name	Description	Local Access
Contact Messaging List View	Contact Messaging List View	✓
Access Group Explorer View	Access Group Explorer View	✓
Access Group Member List View	Access Group Member List View	✓
Account (SCW) Preview View	Account (SCW) Preview View - used for Find Preview	✓
Account - Back Office Account Relationship View	Account - Back Office Account Relationship View	✓

For information about adding screens and views to an application, see *Siebel Tools Reference, MidMarket Edition*.

Responsibilities

A responsibility is a set of views. Each user must be assigned at least one responsibility. When you assign responsibilities to a user, the user has access to all the views contained in all of the responsibilities assigned to the user that are also included in the user's current application.

If a view in an application is not included in a user's responsibilities, the user will not see the view or a listing of the view in the Site Map, in the Show drop-down list, or in any other pick list. If the user does not have access to any of the views in a screen, then that screen's listing in the Site Map and its screen tab are not displayed.

For example, the responsibility assigned to an administrator might include the views in the Server Administration screen. The administrator sees the Server Administration screen listed in the Site Map and the appropriate views in the Show drop-down list. A customer care agent typically does not have administrative views in a responsibility, so the agent would not see the Server Administration screen or its views listed in any context.

A user can have one or more responsibilities. The user has access to all the views in the union of all the responsibilities assigned. For example, you could assign a sales manager both the sales manager responsibility and the field sales responsibility.

Associating a Responsibility With Organizations

You can associate a responsibility with one or more organizations.

A user can see responsibilities that are associated with the organization with which the user is associated for the session.

- An employee or partner user is associated with the organization with which his or her primary position is associated.
- A contact user is associated with the organization of the proxy employee defined for the particular Siebel customer application.

For information about proxy employees, see [“User Authentication” on page 63](#) and [“Seed Data” on page 345](#).

A user can be assigned responsibilities across organizations for the purpose of providing the user access to views. However, the user can only see the responsibilities that are associated with the user’s active organization.

For example, you could decide that delegated administrator responsibility should only be assigned to users by internal administrators, and not by other delegated administrators. A user can then have a delegated administrator responsibility, but would not be able to see it in a list of responsibilities. Therefore, the delegated administrator could not assign it to other users. You can accomplish this scenario by associating the delegated administrator responsibility with an organization other than that with which the delegated administrator is associated.

NOTE: You should associate each responsibility with at least one organization if you include position- or organization-based views in the responsibility.

Local Access

Each view has a Local Access flag. If set to TRUE (checked), all users with the view in their responsibilities can access the view from either the local or server database. When set to FALSE (unchecked), users can only access the view when they are connected to the server database.

The Local Access field can be set for a view through either of the following paths:

- View > Site Map > Application Administration > Views

- View > Site Map > Application Administration > Responsibilities

Figure 25 shows the Local Access field for views associated with a responsibility.

Responsibilities	
Description	Responsibility
Agreement Administrator	Agreement Administrator
Siebel Service Administrator - SSV only	Call Center Administrator
Call Center Representative requiring Webphone Access	Call Center Representative - Wkr
Channel Executive (eChannel)	Channel Executive
Channel Manager (eChannel)	Channel Manager
Channel Marketing Manager (eChannel)	Channel Marketing Manager
Channel Operations Manager (eChannel)	Channel Operations Manager

Views					
View Name	Description	Local Access	Edit	Delete	Save
Account Duplicates Detail View	Account Duplicates Detail View	✓			
Account Duplicates View	Account Duplicates View	✓			
Action Plan View	Action Plan View	✓			
Activity Attachment View	Activity Attachment View	✓			
Activity Chart View - Activity Analysis	Activity Chart View - Activity Analysis	✓			
Activity Chart View - Contact Analysis	Activity Chart View - Contact Analysis	✓			
Activity Chart View - Status Analysis	Activity Chart View - Status Analysis	✓			

Figure 25. Responsibility Views List

NOTE: In the Responsibilities Views list, shown in Figure 25, you cannot edit the Local Access field for a view in a seed responsibility. Use the Views Administration view instead.

The Local Access column is primarily a mechanism for controlling which views mobile users can work in offline. In addition to enabling or disabling local access to views based on responsibility, administrators can turn off one set of views for one mobile user and a different set for another mobile user. For more information, see *Siebel Remote Administration Guide, MidMarket Edition*.

NOTE: You should disable access to views applying *All* access control by setting the Local Access field to FALSE. A view with *All* access control will have unpredictable and possibly undesirable results for a mobile user.

For information about creating and modifying responsibilities and views, see *Applications Administration Guide, MidMarket Edition*.

For information about *All* access control, see [“All Access Control” on page 274](#).

Assigning a Responsibility to an Individual

You can add a responsibility to a Person, to a User, to an Employee, or to a Partner record. The following procedure describes how to add a responsibility to a Person record. Alternatively, you can assign a responsibility in the All Users list, the All Employees list, or in the All Partners list of the User Administration screen.

If the individual does not have a current responsibility, this procedure upgrades the Person to a User. If the individual already has at least one responsibility, then the individual is already a User, an Employee, or a Partner. As such, the individual’s record appears in the Persons list also, so this procedure works for any scenario.

To assign a responsibility to a Person

- 1** Log in to a Siebel employee application as an administrator and choose View > Site Map > User Administration > Persons.

The All Persons list appears.

- 2** Select a Person record.
- 3** In the More Info form, click the browse button on the Responsibility field.

A list of the responsibilities assigned to this Person appears.

- 4** In the Responsibilities list, click New.

A list of responsibilities available for assigning appears.

- 5** Select one or more responsibilities, and then click OK.

The selected responsibilities appear in the list of responsibilities for this Person.

- 6** Click OK.

- 7** In the More Info form, click Save.

If you want to assign the same responsibility to multiple users, you can alternatively add the users to the responsibility through the Application Administration screen.

Business Component View Modes

A business component's view modes determine the allowable access control mechanisms that can be applied to the business component in any view. When a view is based on a particular business component, the view must use one of the view modes specified for the business component. For example, the Account business component can only be used in Organization view mode or Sales Rep view mode.

Each view mode also determines how data is associated with a user to determine whether the user gets access. For example, a business component that allows personal access control may connect the data to the person by comparing the data's Owner Id field to the person's Login ID. Another business component may apply personal access control through the data's Created by field.

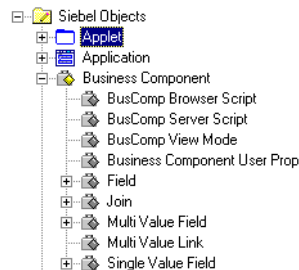
You use Siebel Tools to work with properties of business components.

NOTE: If a business component has no listed view modes, then there is no access control based on the business component in views that are based on that business component.

To view a business component's view mode and visibility fields

- 1 Launch Siebel Tools.
- 2 In the Object Explorer, click + to expand the Business Component object type.

The Business Component sub-tree appears.



- 3 Click the BusComp View Mode icon.

The Business Components list applet and its BusComp View Modes detail applet appear as shown in the following figure.

The screenshot shows two applets. The top applet, titled 'Business Components', contains a table with columns: W, Name, Changed, Project, Cache Data, and Class. The bottom applet, titled 'BusComp View Modes', contains a table with columns: W, Name, Changed, Owner Type, and Private Field.

W	Name	Changed	Project	Cache Data	Class
	Access Group		Access Group		CSSBCGroup
	Access Group Member		Access Group		CSSBCBase
>	Account		Account		CSSBCBase
	Account (Delegated Admin)		Admin		CSSBCUser
	Account Attachment		Account		CSSBCFile

W	Name	Changed	Owner Type	Private Field
>	Organization		Organization	
	Sales Rep		Position	

- 4 In the Business Components list applet, select a business component for which there are records in the BusComp View Modes list applet.

A record in the BusComp View Modes list applet represents one view mode the business component can assume.

The following fields in the BusComp View Modes applet in Siebel Tools determine allowable visibility for a business component.

- **Owner Type.** This is the party type, with one exception (described in the following list) that is used to determine whether a user is associated with a record. The allowable owner types are:
 - **Person.** Access control can be based on the user's Person record.
 - **Position.** Access control can be based on the position of the user.
 - **Organization.** Access control can be based on the organization of the user, as determined by the organization to which the user's current position belongs.
 - **Group.** Access control can be based on membership in access groups that have access to particular catalogs and categories.

- **Catalog Category.** Catalog Category is not a party type. Access can be restricted to all of the data in all of the categories across catalogs to which the user has access. This data includes data in public categories and data in private categories to which the user's access groups have access. The user sees a flat (uncategorized) list of data.

For example, the Account business component's Sales Rep view mode determines the association of the user to the record by the user's position. The Service Request business component's Personal view mode determines the association of the user to the record by the user's Person record.

- **Private Field.** This flag determines whether the record is private or public. If it is not private, then the record is shown, independent of its view mode. If it is set as private, then access control is applied as specified by the business component's Visibility Field or VisibilityMV Field. This is applicable to all view modes.
- **Visibility Field.** A value in either Visibility Field or Visibility MVField is required. The value in this field is compared with the corresponding value for the user, as specified in Owner Type, to determine whether the user is associated with a record. If they are associated, the user gets access to the record.
- A value in this field indicates that there is only one party associated with this business component when using this view mode.

For example, the Service Request business component's Personal view mode determines whether the user is associated with the record by comparing the user's Login ID with the value in the Contact Id field. When this view mode is used, only one user qualifies as being associated with this record. Typically, this user would be the creator of the service request.

- **Visibility MVField (or multi-value field).** This field has the same purpose as Visibility Field, except a value in this field indicates that there can be more than one party associated with this business component when using this view mode.
- For example, the Account business component's Sales Rep view mode determines whether the user is associated with the record by comparing the user's position with the value in the Sales Rep field. When this view mode is used, more than one position can be associated with a record. In some applets, the Sales Rep field has a display name like "Account Team," indicating that more than one position is associated with the record.

- **Visibility MVLink (or multi-value link).** An entry in this field is required if there is a value in Visibility MVField.

- This field specifies which of the business component's multi-value links should be used to determine the value in the MVField for this record. Links establish a parent/child relationship between business components, often by specifying an intersection table (in the case of a many-to-many relationship). This multi-value link's Destination Link property indicates which link ultimately defines this relationship.

To see a business component's multi-value links and their properties in Siebel Tools, expand the Business Component object in the Object Explorer, and then click Multi Value Link. The Destination Link property is a field in each record.

For example, the Account business component's Sales Rep view mode has "Position" as its MVLink. The Destination Link property for this multi-value link specifies that this relationship uses the Account/Position link. As seen in Tools' Link object type listing, this link uses the S_ACCNT_POSTN intersection table to look up the positions associated with an account.

- **Name.** The name typically suggests the view mode. For example, a view mode named Organization typically has an Owner type of Organization. However, the only requirement is that view mode records for a buscomp must have unique names. A business component cannot, for example, have two view modes named Personal.
 - **Personal.** This name is typically used when Owner type is Person.
 - **Sales Rep.** This name is typically used when Owner type is Position.
 - **Organization.** This name is typically used when Owner type is Organization.
 - **Group.** This name is typically used when Owner type is Group.

- **Catalog.** This name is typically used when Owner type is Catalog.

For example, the Account business component’s Sales Rep view mode determines the association of the user to the record by the user’s position. An example of an exception to the typical naming convention is the Service Request business component. Both the Personal and Sales Rep view modes have an Owner type of Person, one interpreting owner by Contact Id and the other by Owned By Id. These two Person-based view modes are needed because the creator and the customer care agent both need access to the data based on their person.

For information about working with business components, see *Siebel Tools Reference, MidMarket Edition*.

Applet Access Control Properties

A view presents a collection of lists, forms, and trees at once, as shown in [Figure 26](#). These lists and forms are referred to as applets in a configuration context.

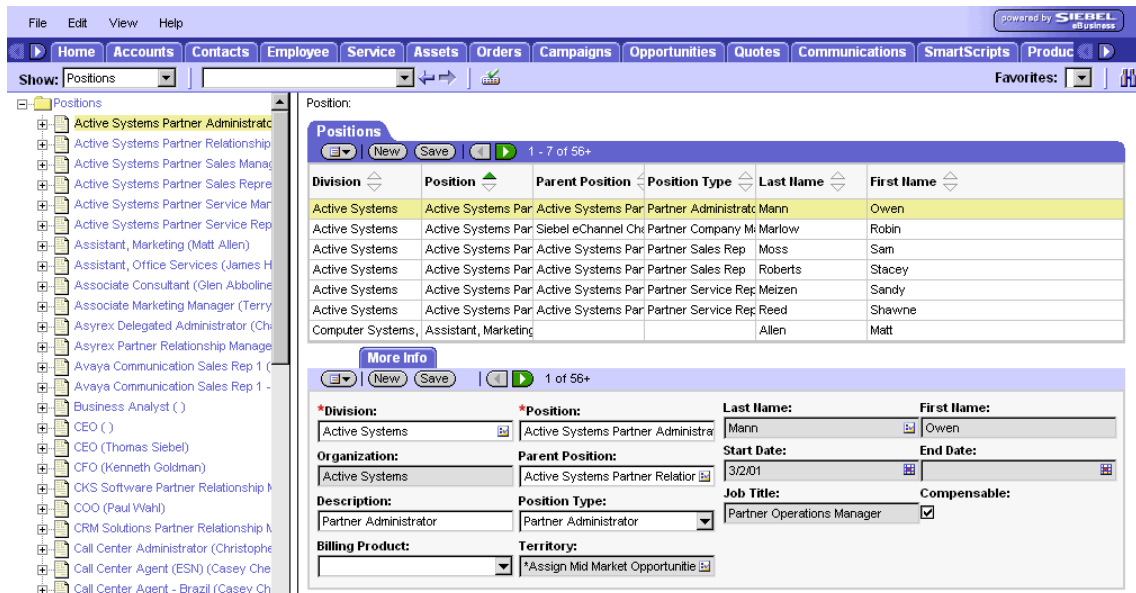


Figure 26. Applets

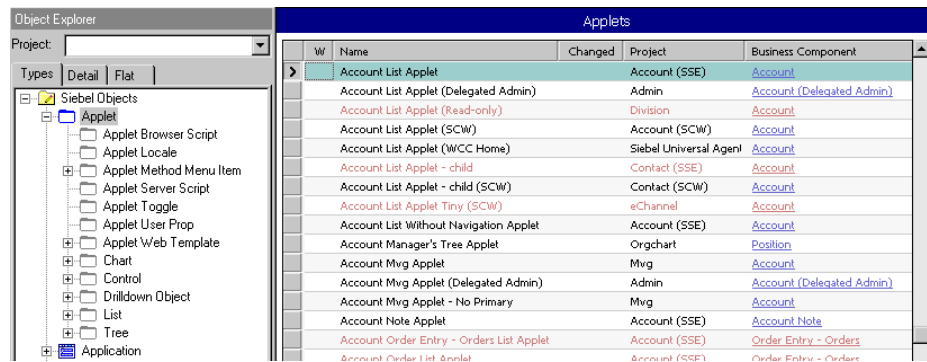
Applets are reused in different views and can have different access control properties applied in different views. If visibility is defined specifically for a view, then one of the applets in the view is specified as the visibility applet. Several properties of the visibility applet drive the access control of data in the view.

You use Siebel Tools to work with properties of applets.

To view an applet's properties

- 1 Launch Siebel Tools.
- 2 In the Object Explorer, click + to expand the Applet object type.

The Applet sub-tree appears. The Applets list applet also appears as shown in the following figure.



- 3 To see a particular applet property, click the icon for its sub-component or click + to expand the sub-tree for a sub-component, and then click its subcomponent.

A detail applet for the sub-component appears below the Applets list applet.

Two applet properties in particular contribute to data visibility.

- Business Component.** As shown in [Figure 27](#), this field in the Applets list applet specifies the business component on which the applet is based. For example, Account List Applet uses the Account business component.

Applets				
W	Name	Changed	Project	Business Component
	Account Form Applet - Short		Account (SSE)	Account
	Account Form ReadOnly Applet		Account (SSE)	Account
	Account List Applet		Account (SSE)	Account
	Account List Applet (Delegated Admin)		Admin	Account (Delegated Admin)

Figure 27. Business Component Field for an Applet

- Display Name.** In the Tools Object Explorer, choose Applets > List > List Columns. As shown in [Figure 28](#), the List Columns list applet shows the fields of the business component that this applet will display. For each business component field, the Display Name entry in the accompanying Properties applet shows how that field is labeled in the applet. For example, the Accounts business component can use either the Sales Rep or Organization field to determine user association with a record. It is useful to know how these fields display in the Account List Applet. The Organization field has display name “Organization” in the applet, but the Sales Rep field has display name “Account Team.”

The screenshot shows the Siebel Tools interface with four main windows:

- Object Explorer:** Shows a tree view of Siebel Objects, with 'List Column' selected under the 'List' folder.
- Lists:** A table showing a single entry: 'List'.
- List Columns:** A table listing various fields from the 'Account' business component. The 'Sales Rep' field is highlighted in blue.
- Properties:** A table of properties for the selected 'List Column'. The 'Display Name' property is set to 'Account Team'.

W	Field	Changed	Available	Available - Lan
	PO Approved Flag			
	PO Auto Approval Limit			
	Parent Account Location			
	Parent Account Name			
	Parent HQ DUNS			
	Partner Flag			
	Postal Code		✓	
	Price List			
	Primary Employee Login			
	Primary Fulfillment Inventory Locator			
	Row Status		✓	
	S-S Instance		✓	
	Sales Rep		✓	

Property	Value
List Column [Sales Rep]	
Alphabetic	
Categorized	
Available	TRUE
Available - Language C	
Comments	
Content Fixup Name	
Detail Applet	
Display Format	
Display Name	Account Team
Field	Sales Rep
Field Retrieval Type	
HTML Attribute	
HTML Display Mode	
HTML Height	
HTML Height - Language	
HTML Icon Map	
HTML List Edit	FALSE
HTML Max Chars Disp	
HTML Max Chars Disp	
HTML Only	FALSE
HTML Row Sensitive	TRUE
HTML Sequence	
HTML Sequence - Lar	
HTML Type	Field

Figure 28. List Columns List Applet

For information about working with applets, see *Siebel Tools Reference, MidMarket Edition*.

View Access Control Properties

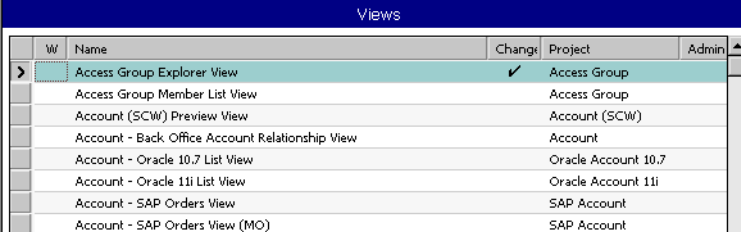
A view's access control properties determine what applet is used to drive visibility and what access control mechanism is applied to the business component on which the view is based.

You use Siebel Tools to work with properties of views.

To see a view's access control properties

- 1 Launch Siebel Tools.
- 2 In the Object Explorer, click the Views object type.

The Views list applet appears as shown in the figure below. Its fields include those that influence visibility.



Wf	Name	Change	Project	Admin
>	Access Group Explorer View	✓	Access Group	
	Access Group Member List View		Access Group	
	Account (SCW) Preview View		Account (SCW)	
	Account - Back Office Account Relationship View		Account	
	Account - Oracle 10.7 List View		Oracle Account 10.7	
	Account - Oracle 11i List View		Oracle Account 11i	
	Account - SAP Orders View		SAP Account	
	Account - SAP Orders View (MO)		SAP Account	

The following fields in the Views list applet help determine data visibility.

- **Title.** The title is the name given to a view in the user interface. It should suggest the level of access control on the view's data. For example, My Accounts suggests more restricted visibility than My Team's Accounts.
- **Visibility applet.** Typically, this is the master in a master-detail applet relationship. This applet defines the business component on which the view is based and how fields of the business component are displayed.
 - A view has an entry in this field if the view is not derived from another view. For example, a view that is listed in the Show drop-down list for any screen has a visibility applet, but a view that results from drilling down from another view does not. A view with no visibility applet typically inherits access control properties from the view from which it is derived.
 - Multiple views can have the same visibility applet. For example, both All Account List View and Manager's Account List View have Account List Applet as their visibility applet.

- **Visibility Applet Type.** This field determines the access control mechanism that is applied to that view. It specifies which of the business component's view modes are applied and how they are applied. Following are the choices available in the pick list for this field:
 - **All.** This view applies *All* access control. The user can access all records, except for those with a missing or invalid owner.
 - **Personal.** This view applies Personal access control. The user can access records with which the user's Person record is associated, as determined by the business component's Visibility Field. To use this visibility applet type, the business component must have a view mode with Owner Type Person.
 - **Sales Rep.** This view applies Single Position or Sales Team access control. The user can access records owned by the user's position or records whose sales team contains the user's position, as determined by the business component's Visibility Field or Visibility MVField. To use this visibility applet type, the business component must have a view mode with Owner Type Position.
 - **Manager.** This view applies Manager access control. The user can access records associated with the user's own position, positions that report directly to the user's position, and positions subordinate to those direct reports. Specifically, the user has access to the following data:
 - If the business component on which the view is based uses single position access control, the user sees data associated directly with the user's active position or with subordinate positions.
 - If the business component on which the view is based uses sales team access control, then the user sees data for which the user's active position is the primary position on the team or a subordinate position is the primary member on the team.

NOTE: If a user's position has no subordinate positions, the user sees no data in views that use Manager Visibility Applet Type, not even the user's own data.

To use this visibility applet type, the business component can also have a view mode with Owner Type Position.

- **Organization.** This view applies single organization or multiple organization access control, as determined by the business component's Visibility Field or Visibility MVField. The user can access records associated with the organization to which the user's position is associated. To use this visibility applet type, the business component must have a view mode with Owner Type Organization.
- **Sub-Organization.** This view applies sub-organization access control. The user has access to the following data:
 - If the business component on which the view is based uses single organization access control, the user sees data associated directly with the user's active organization or with a descendent organization.
 - If the business component on which the view is based uses multiple organization access control, then the user sees data for which the user's active organization or a descendent organization is the primary organization.

Descendent organizations are defined by the organization hierarchy. To use this visibility applet type, the business component must have a view mode with Owner Type Organization.

- **Group.** This view applies Group access control, which is one mechanism of access group access control. The user is associated with an access group if, during the current session, the user is associated with a position, organization, account, or user list that is a member of the access group. The user can access categories of master data that are associated with any of the access groups with which the user is associated. In a view that provides a navigable tree, the user sees accessible first-level subcategories (child categories) in the current category. In a view that provides a list of master data records, the user sees all the records in the current (already accessed) category. To use this visibility applet type, the business component must have a view mode with an Owner Type of Group.

- **Catalog.** This view applies Catalog access control, which is one mechanism of access group access control. The user is associated with an access group if, during the current session, the user is associated with a position, organization, division, account, or user list that is a member of the access group. The user sees a flat (uncategorized) list of all the data in all of the categories across catalogs to which all of the user's access groups have access. This visibility type is typically used in product pick lists and other lists of products. To use this visibility applet type, the business component must have a view mode with an Owner Type of Catalog Category.
- **Admin Mode.** This property requires a TRUE or FALSE value. When TRUE, the view operates in Admin mode. When the view is in Admin mode, all inset, delete, merge, and update restrictions for the business component used by applets of the view are ignored (including those restrictions specified by business component user properties). Examples of Admin mode views include Account Administration view, Opportunity Administration view, and Product Administration view.

Admin mode does not override pop-up visibility. It does not override Read Only restrictions on fields in a business component.

In Admin mode, every record in a view that uses Sales Team access control is visible, even those with no primary position designated. (This mode is distinct from *All* visibility, which shows all records that have a primary team member designated.)

CAUTION: Views using Admin mode are intended for access by administrators and are typically included in a grouping of like views in an administration screen, such as Application Administration. Do not include views in Admin mode in a screen with views not set for Admin mode. When a user transitions from a view that is in Admin mode to one that is not, the target view remains in Admin view, thereby exposing data that is not intended to be seen.

An Example of Flexible View Construction

The following example shows how several existing views were constructed, based on the same visibility applet and business component. It suggests how similar view “families” can be constructed in Siebel Tools, but does not give procedures for constructing views. Changing any settings in Siebel Tools requires recompiling the Siebel repository file.

For more information about required practices when using Siebel Tools, see *Siebel Tools Reference, MidMarket Edition*.

Figure 29 shows the Siebel Tools BusComp View Modes applet for the Accounts business component.

BusComp View Modes						
Name	Changed	Owner Type	Private Field	Visibility Field	Visibility MVField	Visibility MVLink
> Organization		Organization		Organization	Organization	Organization
Sales Rep		Position		Sales Rep		Position

Figure 29. Account Business Component View Modes

As indicated by the Owner Type field, organization-based and position-based view modes are allowed. As indicated in the Visibility MVField, accounts can be associated with multiple organizations and multiple positions (for example, sales teams).

Figure 30 shows five views in the Siebel Tools Views applet.

Views			
Name	Title	Visibility Applet	Visibility Applet Type
Account List View	My Accounts	Account List Applet	Sales Rep
Manager's Account List View	Team's Accounts	Account List Applet	Manager
All Account List View	All Accounts	Account List Applet	Organization
All Accounts across My Organizations	All Accounts across My Organizations	Account List Applet	Sub-Organization
All Accounts across Organizations	All Accounts across Organizations	Account List Applet	All

Figure 30. Some Views Based on the Account Business Component

The Title field shows the display name for the view. All five views have the Account List Applet as their visibility applet. The Account List Applet is based on the Accounts business component.

These five views provide different lists of data by specifying different visibility applet types, as shown in the following table.

View	Visibility Applet Type	Data Access
Account List View (displayed as My Accounts)	Sales Rep	Sales Rep is a position-based access control mechanism. It is applied to a business component for which multiple positions can be associated. Access is granted to a user whose position is on the account team.
Manager's Account List View (displayed as Team's Accounts)	Manager	Manager is a position-based access control mechanism. Here it is applied to a business component for which multiple positions can be associated. Access is granted to data for which the user's active position or a subordinate position is the primary position on the account team.
All Account List View (displayed as All Accounts)	Organization	Organization is an organization-based access control mechanism. It is applied to a business component for which multiple organizations can be associated. Access is granted to a user whose primary organization is one of the organizations with which the account is associated.
All Accounts across My Organizations	Sub-Organization	Sub-organization is an organization-based access control mechanism. In this view it is applied to a business component for which multiple organizations can be associated. Access is granted to data for which the user's active organization or a descendent organization is the primary organization.
All Accounts across Organizations	All	The Account business component has only position-based and organization-based view modes. Any user with this view in the user's responsibilities sees every account for which there is a primary position on the account team or an organization associated with the account.

Administering Access Group Access Control

You associate an access group to a catalog or category of master data. When an access group is associated with a catalog or a category, the users associated with the access group have visibility of the data in the catalog or the category.

- The following principles apply to access group access control. An access group in the following context is an individual node in an access group hierarchy:
- **Private catalogs and categories.** A catalog is a hierarchy of categories. A catalog cannot itself contain data. To apply access group access control on all of a catalog's categories, you must designate the catalog as private, and then associate access groups to the catalog. If a catalog is not private, then any user can see data in its categories. You can designate individual categories private within a public catalog.
- **Access group access is inherited.** If an access group is associated with a category, then the group's descendent groups (child, grandchild, and so on) are automatically associated with the category. Conversely, if an access group is disassociated with a category, then its descendent groups are also disassociated. The inheritance association is enforced at run time.
- **Cascading category visibility is optional.**
 - If an access group is associated with a category, the Cascade flag provides that the access group is automatically associated with that category's descendent categories (child, grandchild, and so on). Therefore, users associated with the access group have access to the data in those descendent categories.
 - If the access group is disassociated with the category, then the access group is automatically disassociated with that category's descendent categories. If the access group is disassociated with one of the descendent categories, then the access group's cascading visibility is granted only down to, but not including, that descendent category.
 - Once the Cascade flag is set, cascading access can only be disabled by disassociating the access group from a category. The flag itself cannot be unset.
 - If the Cascade flag is not set, access is limited to the individual category to which the access group is associated.

A Scenario That Applies Access Group Access Control

Assume you want the status of your resellers to determine which of your “knowledge” resources they have access to. Your resellers include partner organizations and some individual consultants that are not associated with a partner organization.

Your solution must meet the following requirements:

- It must provide your base resellers access to basic product information resources— service FAQs and product documentation.
- In addition to basic product information, it must provide your “premier” resellers access to more sales- and service-specific resources—marketing FAQs and documents that describe internal service resolutions.
- In addition to product and sales resources, it must provide your alliance resellers access to competitive briefs.
- As the status of a reseller changes, the administration required to change the reseller’s access to data must be minimal.

Figure 31 illustrates one access control structure that solves this business problem.

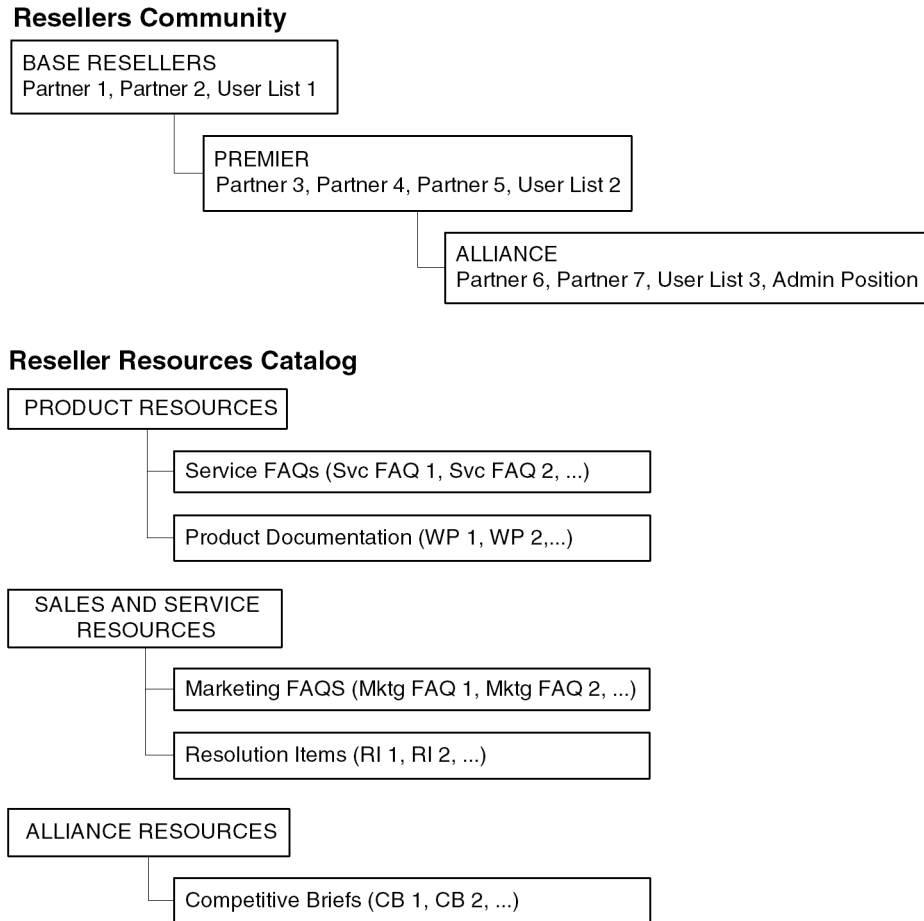


Figure 31. Reseller Resources Access Control

This solution assumes that your partners are stored as organizations, in which partner users are associated with positions. The consultants exist as users; they have responsibilities, but not positions, and are not associated with an organization.

The Resellers Community is an access group hierarchy. Each node is an access group whose members are partner organizations and a single user list. The user list in each node contains all consultants of the appropriate status. For internal administrators to have visibility of the catalog, include their positions in the ALLIANCE access group.

The Reseller Resources catalog is constructed of categories containing data and nodes that are empty categories to define access levels.

Apply the following principles to construct this structure:

- Construct the Resellers Community such that the upper levels have the narrowest access to resources. Therefore, the BASE RESELLER access group is the parent of the PREMIER access group, which is in turn the parent of the ALLIANCE access group.
- Construct the Reseller Resources Catalog such that the PRODUCT RESOURCES, SALES AND SERVICE RESOURCES, and ALLIANCE RESOURCES nodes are all first level categories in the catalog.
- The child nodes to the PRODUCT RESOURCES node include categories of product resources. The child nodes to the SALES AND SERVICE RESOURCES and ALLIANCE RESOURCES nodes are determined similarly.

The following implementation procedure restricts the base resellers' access to product resources only, premier resellers' access to product resources and sales resources, and alliance resellers' access to all resources.

To implement the structure shown in [Figure 31 on page 310](#)

- 1** Construct the Reseller Resources Catalog, and specify it as private, with access provided to the BASE RESELLERS access group.

Access to the catalog is also granted to the PREMIER and ALLIANCE access groups because access group access is inherited.

- 2** Associate the BASE RESELLERS access group with the PRODUCT RESOURCES category, and set the cascade flag.

Access is inherited by the PREMIER and ALLIANCE access groups from the BASE RESELLERS group, and access cascades from the PRODUCT RESOURCES category to its subcategories containing data. The resulting behavior is that all the nodes in the Resellers Community have access to all the subcategories in the PRODUCT RESOURCES category.

- 3 Associate the PREMIER access group with the SALES AND SERVICE RESOURCES category, and set the cascade flag.

Access is inherited by the ALLIANCE access group from the PREMIER group, and access cascades from the SALES AND SERVICE RESOURCES category to its subcategories containing data. The resulting behavior is that the PREMIER and ALLIANCE groups have access to all the subcategories in the SALES AND SERVICE RESOURCES category.

- 4 Associate the ALLIANCE access group with the SALES AND SERVICE RESOURCES category, and set the cascade flag.

No group inherits access from the ALLIANCE group. Access cascades from the ALLIANCE RESOURCES category to its subcategory containing data. The resulting behavior is that only the ALLIANCE group has access to the subcategory in the ALLIANCE RESOURCES category.

- 5 Set the catalog to type Partner to make it visible to partners and consultants on partner applications such as Siebel PRM, and to internal administrators on Siebel employee applications in the Info Center screen.

This structure meets the minimal maintenance requirement. If the status of a partner organization changes, add the partner organization to the appropriate access group and delete the partner organization from the old access group. If the status of a consultant changes, add the user to the appropriate user list, and delete the user from the old user list. Recategorized consultants and partner users are granted appropriate new access as defined by the structure.

Sales tools of the same type, for example FAQs or product documentation, are in separate categories.

For information about:

- Creating and administering catalogs, see *Siebel eSales Administration Guide, MidMarket Edition*.
- Creating and administering user lists and access groups, see [“Administering Access Group Access Control” on page 308](#).

The User's Experience

You can configure a catalog to display in Siebel employee applications and in selected customer and partner applications, such as Siebel eSales and Siebel PRM, as a default functionality.

In an employee application, such as Siebel Call Center, a user can see categorized data controlled by access group membership in the Info Center Explorer screen.

As shown in [Figure 32](#), Info Center Explorer provides a tree interface for navigating all the catalogs to which the user has access, down to the data item level.

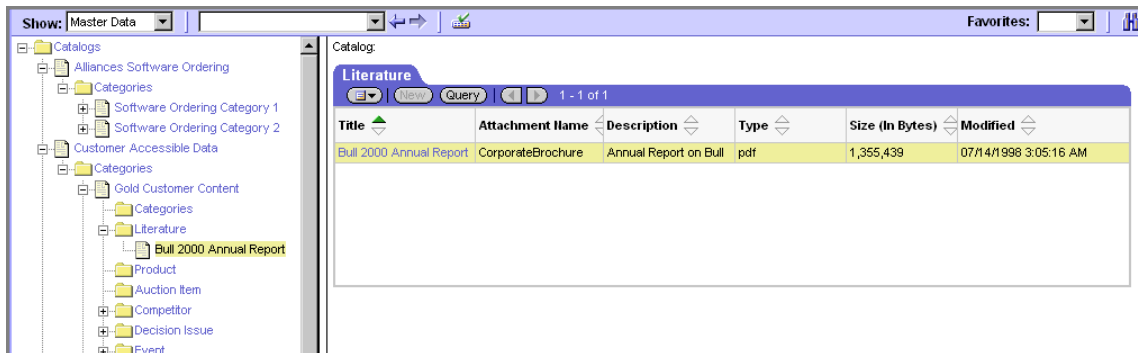


Figure 32. Info Center Explorer

Administrative Tasks

Access group access control requires that you do the following tasks:

- Administer catalogs of master data—build the catalogs and categories, associate data, and modify catalog structures as needed.
- Administer the party types that are members of access groups—positions, organizations, and user lists.
- Administer access groups—build the access groups and modify their structures as needed.
- Associate access groups with catalogs and categories of data.

Administering Catalogs of Data

You can do the following catalog and category administration tasks in the Catalog Administration screen:

- Create and delete catalogs and categories of master data.
- Associate data with categories.
- Modify the hierarchical position of a category within a catalog.

Key principles for setting up a catalog include, but are not limited to:

- Set the Catalog Type field to allow display of the catalog in certain Siebel customer or partner applications, in addition to Info Center and Info Center Explorer in Siebel employee applications. For example, set the Catalog Type to Partner to display the catalog in Siebel PRM, as well as in Info Center Explorer.
- Make sure the Active flag is set and the Effective Start Date and Effective End Date fields provide visibility of the catalog during your intended time interval.

For information about creating and administering catalogs, see *Siebel eSales Administration Guide, MidMarket Edition* and *Siebel Partner Relationship Management Administration Guide, MidMarket Edition*.

Administering Positions, Organizations, and User Lists

Access groups are made up of positions, organizations, and user lists.

Administering Positions

You must do the following administrative tasks with positions:

- Create positions.
- Associate positions with employees and partner users.
- Maintain position hierarchies.

For information about administering positions, see *Applications Administration Guide, MidMarket Edition*.

Administering Organizations

The Organization group type includes organizations, divisions, and accounts. You must do the following administrative tasks with organizations:

- Create divisions and accounts
- Promote divisions to organizations
- Maintain division hierarchies
- Associate positions with divisions and with partner organizations

For information about administering accounts, divisions, and organizations, see *Applications Administration Guide, MidMarket Edition*.

Administering User Lists

You can group arbitrary users into user lists for the purpose of granting them access to data through access groups. Users in this context include contact users, employees, and partner users.

For information about user lists, see [“Parties” on page 252](#).

Creating a User List

You can create a user list in the Group Administration screen.

To create a user list

- 1** Choose View > Site Map > Group Administration > User Lists.
The User Lists list appears.
- 2** In the User Lists list, add a new record.
A new user list record appears.
- 3** Enter a name for the user list. Optionally, change the default entry for Group Type.
- 4** Click Save.

Modifying a User List

You can modify a user list by adding or deleting users.

To add users to a user list

- 1 Choose View > Site Map > Group Administration > User Lists.

The User Lists list appears.

- 2 In the User Lists list, select a user list.
- 3 In the Users list at the bottom of the view, add a new record.
- 4 Select one or more users, and then click OK.

The selected users appear in the Users list. If a user, such as a customer user, belongs to an account, the Account field populates automatically.

You can delete users from a user list similarly.

Administering Access Groups

You can group parties of types Position, Organization, and User List into access groups for the purpose of controlling their individual members' access to data.

You administer access groups in the Group Administration screen by choosing View > Site Map > Group Administration > Access Groups. This screen contains the Access Groups tree and the Access Groups list.

The Access Groups tree lists all access groups on the second level of the tree. Each access group can be expanded to show its descendents. Therefore, an access group may appear at different levels in multiple branches of the tree.

An access group that has no parent access group is the top node of an access group hierarchy.

For information about access groups, see [“Parties” on page 252](#) and [“Access Group Access Control” on page 275](#).

Creating an Access Group

You can create an access group in the Group Administration screen.

To create an access group

- 1 Choose View > Site Map > Group Administration > Access Groups.

The Access Groups tree and the Access Groups list appear.

- 2 In the Access Groups list, add a new record.

A new access group record.

- 3 Complete the following fields, using the guidelines provided in the following table, and then click Save.

Field	Guideline
Name	Required. Provide a name for the access group.
Group Type	Pick Access Group or Partner Community. These labels denote conceptual differences. Functionally, they are the same.
Parent Access Group	Specify a parent access group from which this new group inherits access to data that the parent group has access to.

The new access group also appears in the Access Groups tree.

Modifying an Access Group

You can modify an access group by adding or deleting members.

To add members to an access group

- 1 Choose View > Site Map > Group Administration > Access Groups.

The Access Groups list appears.

- 2 In the Access Groups list, select an access group.

- 3 In the Members list, add a new record.

A pop-up list appears that contains positions, organizations, accounts, and user lists.

- 4 Select one or more members, and then click OK.

The selected members appear in the Members list.

- 5 In the Access Groups list, click Save.

You can delete members from an access group similarly.

Modifying an Access Group Hierarchy

You can modify the hierarchy of an access group by changing an access group's parent.

To modify a hierarchy of access groups

- 1 Choose View > Site Map > Group Administration > Access Groups.

The Access Groups list appears.

- 2 In the Access Groups list, select an access group.

- 3 Click on the Parent Access Group field.

The text box becomes editable and its entry is highlighted.



- 4 Do one of the following to modify the hierarchy:
 - To make the access group the top node of its own hierarchy, delete the entry in the Parent Access Group field, and then click Save.
 - Click the ellipsis button on the Parent Access Group field, and then pick a new parent and click OK. Click Save.

The Access Group tree is updated to reflect the access group's new position in a hierarchy.

Associating Access Groups With Data

The individual users in an access group are provided access to data by associating the access group with catalogs or categories of data.

Be aware of the following user interface behaviors related to associating an access group with a catalog or category:

- **Access inheritance.** When you associate an access group with a category, its descendent groups are also associated with the category. However, this inheritance is implemented at run time, and is not represented in the database. As such, the descendent access groups associated with the category are not displayed in the list of groups associated with the category.
- **Cascade flag.** When you set the Cascade flag for the relationship of an access group with a catalog or category, the check appears in the field. When you save or step off of the record, the check displays briefly, indicating that the group is being associated with descendent categories, and then it disappears. You cannot disable cascading visibility unless you disassociate an access group with a category, so this flag cannot be unset as other flags can.
- **Private catalog.** If you specify a catalog to be private, its categories are all set as private. If you remove privacy at the catalog level, the categories retain privacy. You must then set or remove category privacy individually.

Associating an Access Group With a Catalog

By associating an access group with a catalog of master data, you grant access to the data in the catalog to individual users in the access group.

NOTE: For a catalog and all of its categories to be visible only to the access groups associated with it, the catalog's Private flag must be set.

To associate an access group with a catalog

- 1 Choose View > Site Map > Catalog Administration > Access Groups.
The Catalogs list appears.
- 2 Select a catalog.

- 3** In the Access Groups list, add a new record.
A pop-up list appears that contains access groups.
- 4** Select an access group, and then click Add.
The access group appears in the Access Groups list.
- 5** In the Access Groups list, click Save.
- 6** Select an access group, and then click Add.
The access group appears under the Access Group tab.
- 7** Complete the following fields, using the guidelines provided in the following table, and then click Save.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer the catalog.
Cascade	Set this flag to automatically associate this access group with the catalog's descendent categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendent categories.

You can disassociate an access group from a catalog similarly.

Associating an Access Group With a Category

By associating an access group with a category of master data, you grant access to the data in the category to individual users in the access group.

NOTE: For a category and all of its subcategories to be visible only to the access groups associated with it, the category's Private flag must be set or the Private flag of the catalog or a category from which the category descends must be set.

To associate an access group with a category

- 1** Choose View > Site Map > Catalog Administration > Access Groups.

The Catalogs list appears.

- 2** Drill down on a catalog name.

The Categories list for the catalog appears.

- 3** Click the Access Groups view-level tab.

- 4** In the Access Groups list, add a new record.

A multi-value group appears that lists access groups.

- 5** Select an access group, and then click Add.

The access group appears in the Access Groups list.

- 6** In the Access Groups list, click Save.

- 7** Select an access group, and then click Add.

The access group appears under the Access Group tab.

- 8** Complete the following fields, using the guidelines provided in the following table, and then click Save.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer this category.
Cascade	Set this flag to automatically associate this access group with this category's descendent categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendent categories.

You can disassociate an access group from a catalog similarly. When an access group is disassociated from a category, it is automatically disassociated from all of the categories descendent categories.

Supplemental Access Control

The following sections contain access control information that is supplemental to the basic access control mechanisms.

Creating and Administering Roles

Siebel applications administrators can create roles to further increase the usability of Siebel applications. Application administrators use the Group Administration screens to create and administer roles.

When you create roles and assign users to these roles:

- By default, users only see the screen tabs and view tabs for their roles. These are the views required most often for users holding that job function.

Users can still go to site map and see all screens that they have access to in their responsibility. If they select a screen from the site map, a screen tab will be created for that screen which will only be available for that session.

Users can override the default screen and view tab settings for their roles. There is a user preference setting that allows users to select the screen and view tabs that they want to see.

- Users have a task list for their role on their home page, with hyperlinks that take them directly to the views they use most frequently.
- Administrators can base personalization on role. For example, they can hide applets or display messages in salutation applet based on role.

CAUTION: Do not confuse roles defined in the Siebel application interface (as described in this section) with roles defined by an LDAP or ADS directory attribute. Roles in LDAP or ADS directories are collections of responsibilities that strictly enforce access to views and data records within Siebel applications. Roles defined in the application interface allow application administrators to increase the usability and deployability of the application by tailoring the product to groups of users.

To define a role in the application interface, you might create a role named Sales Representative. You would associate it with the screens and views that sales representatives commonly use, such as certain views of the Opportunity and Contact screens. In addition, you would associate it with a list of tasks that sales representatives commonly perform, such as a task named View and Update Opportunities.

Then you can associate users with the role of Sales Representative. When these users log into a Siebel application, they would only see the screen tabs for the screens they commonly use. There might just be eight or ten screen tabs, so they would not have to scroll through the page tabs to find the one they want.

In addition, their home page would include an applet with the title Tasks, which would have hyperlinks that take them directly to the views they use to perform these tasks. For example, in the Sales Representatives Tasks list of the home page, they could click View and Update Opportunities to go directly to the view they use to add an opportunity.

The home page can also be configured to display a salutation with an operational message based on the role, an analytics report specified for the role, and alerts targeted to specific roles. You do this by using the Personalization Administration screen to personalize the home page based on the user's primary or non-primary roles.

To use roles, you must:

- Create roles
- Associate tasks with each role
- Specify the screen tab and view tab layout for each role
- Assign users to roles in one of two ways:
 - Associate employees with roles in the User Administration, Employee Administration, or Partner Administration view.
 - Make roles available to partner companies, so delegated administrators can associate partner employees with roles. For more information, see *Siebel Partner Relationship Management Administration Guide, MidMarket Edition*.

Creating Roles

You should create roles that represent the functional positions of a Siebel user in your business model, such as Sales Representative, Sales Manager, and Compensation Specialist.

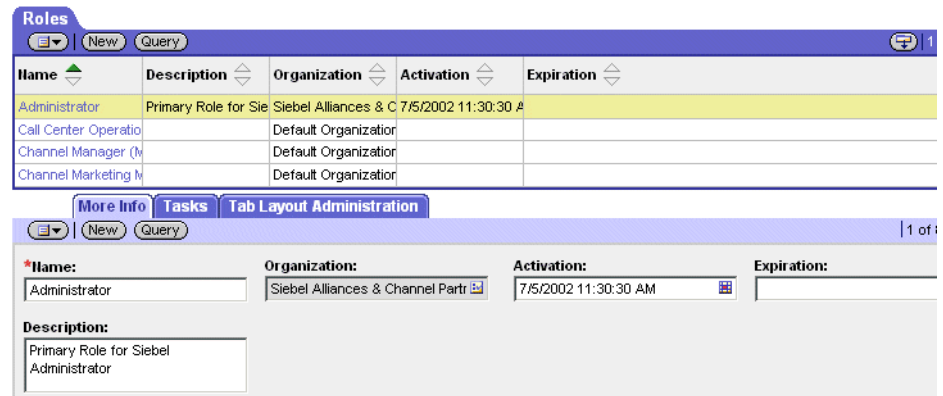
You can create roles that are appropriate for both employees and partner employees.

To create a role

- 1** Log in as an administrator and choose View > Site Map > Group Administration > Roles.
- 2** In the Roles list, click the New button, and enter information about the role in the new record.

Field	Comment
Name	Enter the name of the role.
Description	Optionally, enter a description of the task for your own use.
Organization	Click the select button and choose all of the organizations where this role will be available. Add partner organizations here only if you want delegated administrators to be able to assign the role to new partner users.
Activation	Optionally, enter the date when this role will become available for use.
Expiration	Optionally, enter the last date when this role will be available for use.

The following figure shows a list of roles and More Info about a role.



Associating Tasks with a Role

After creating a role, enter the tasks commonly performed by employees who have that role, which you want to appear in the task list on the home page for these employees.

For each task, enter a caption and select an image file. These will be displayed as a hyperlink in the task list. Enter a description, which will also be displayed in the task list, underneath the caption.

In addition, for each task, specify the view where the task is performed. When the user clicks on the hyperlink for this task on the home page, this view will appear.

To associate tasks with a role

- 1 Log in as an administrator and choose View > Site Map > Group Administration > Roles.
- 2 In the Roles list, select the role you want to associate tasks with.
- 3 Click the Tasks view tab.

- In the Tasks list, add a new record for each task associated with this role, and enter information about each task in the new records.

Field	Comment
Name	Enter the name of the task.
Caption	Enter a caption for the task that will be displayed as a hyperlink in the task list.
Description	Enter a description of the task that will be displayed under the caption in the task list.
Destination View	Click the select button and choose the view that will appear when the user clicks the hyperlink for this task.
Sequence	Optionally, specify the order in which this task will be displayed in the task list for this role on the home page. If this field is left blank, tasks will be displayed in the order that you list them here.
Image	Select the graphic image that will be displayed as a hyperlink to the left of this task in the task list.
Group	This field is be used if search specifications are applied to filter the tasks that will be displayed in the task applet, if multiple task applets are associated with the role.

The following figure shows tasks associated with a role.

The screenshot displays the 'Roles' configuration window. The top section shows details for a role named 'Call Center Operations Rep', including its organization ('Default Organization') and activation/expiration dates. Below this is a 'Description' field. The bottom section shows a 'Tasks' tab with a list of tasks. The task list has columns for Name, Caption, Description, Destination View, Sequence, Image, and Group.

Name	Caption	Description	Destination View	Sequence	Image	Group
Identify the Custome	Identify the Custome	Search for the cont	Contact List View		applet_contact	Home Page Tasks
Create New Lease	Create New Lease		My Agreement List		hm_pg_register_prc	Home Page Tasks
Validate Lease Terr	Validate Lease Terr		FS Agreement Line		seed_eadvisor	Home Page Tasks
Check Customer Cr	Check Customer Cr	Check for customer	DNB All Account Lis		hm_pg_chk_my_bill	Home Page Tasks

Specifying the Tab Layout for a Role

Next, specify which screen tabs and view tabs are displayed for each role.

You must select an application in tab layout because you may be administering roles for a different application other than the one you are logged into as an administrator. For example, you use the Siebel Partner Manager to administer roles that partners will see when they use the Siebel Partner Portal.

To let you manage screens and views for multiple applications, tab layout administration uses three lists:

- **Tab Layout Administration list.** Includes all the Siebel applications in the repository.
- **Screen Tab Layout list.** Specifies which screens are displayed for the role by each application.
- **View Tab Layout list.** Specifies which views are displayed for the role by each screen.

Figure 33 shows the Screen Tab Layout and View Tab Layout for a role.

The screenshot shows the Siebel Tab Layout Administration interface. It has three main sections:

- Application Name:** A list of applications including Corba Object Manager, Siebel CRA, Siebel ERM, Siebel Field Service, Siebel Marketing Enterprise, Siebel Mobile Connector, and Siebel Partner Manager.
- Screen Tab Layout:** A table with columns for Order, Name, and Hide. It lists three screens: Home (Order 1), Service (Order 2), and Activities (Order 3).
- View Tab Layout:** A table with columns for Order, Name, Type, Hide, and Default View. It lists two views: My Activities (Order 1, Default View checked) and My Delegated Activi (Order 2).

Figure 33. Tab Layout for a Role

To specify the tab layout for a role

- 1** Log in as an administrator and choose View > Site Map > Group Administration > Roles.
- 2** In the Roles list, select the role you want to associate tasks with.
- 3** Click the Tab Layout Administration view tab.
- 4** In the Tab Layout Administration list, select an application used by the role.
- 5** The Screen Tab Layout list displays all the screens used by the selected application:
 - a** Select the Hide check box for any screens whose screen tabs will not be displayed.
 - b** Change the numbers in the Order field to change the sequence in which the screen tabs are displayed.
- 6** Select each record in the Screen Tab Layout list, and the View Tab Layout list displays all the views for that screen:
 - a** Select the Hide check box for any views whose view tabs will not be displayed.
 - b** Change the numbers in the Order field to change the sequence in which the screen tabs are displayed.

Associating Users with Roles

After a user is associated with a role, that user will see the tasks of that layout in the home page applet and will see the tab layouts defined for that task.

You associate employees (or other types of users) with the roles using the User Administration screen.

You can also associate partner employees with roles using the User Administration screen, but if you are working with multiple employees of a single partner company, it is better to use the Partner Administration screen to display all the employees of a partner company.

Figure 34 shows a list of roles associated with an employee.

Primary	Name	Description	Organization	Activation	Expiration
	Call Center Operatio		Default Organization		
✓	Consultant		Default Organization		

Figure 34. Associating an Employee With a Role

To associate an employee or user with a role

- 1 Log in as an administrator and choose View > Site Map > User Administration > Employees.

You can also use the following views to associate users with roles:

- View > Site Map > User Administration > Users
 - View > Site Map > Partner Administration > Registered Partners > User Assignments
- 2 In the Employees list, select the record of the Employee you want to associate with a role.
 - 3 In the More Info form, click the show more button.
 - 4 In the More Info form, in the Role field, click the select button.
 - 5 In the Role dialog box, if the role you want is not already in the Role list, click New and use the Add Roles dialog box to select the role.
 - 6 In the Role dialog box, select the role you want to associate with the employee, make sure it is selected as the primary role, and click OK.

Creating Role-Based Personalization

You can use roles to define which applets appear on an application home page. This allows you to:

- Vary applets based on job function
- Avoid complicated home pages
- Optimize performance by minimizing unnecessary applets

The following is an example of restricting the Calendar Home Page To Do List based on roles. You can use it as a model for role-based personalization in your own applications.

- 1** Log in as an administrator and choose View > Site Map > Personalization Administration > Applets.

A list of applets appears.

- 2** Select the Calendar Home Page To Do List applet.

- 3** Change the Conditional Expression to the following:

```
GetProfileAttr("Primary User Role Name") IS NULL OR  
GetProfileAttr("Primary User Role Name") = 'Field Sales  
Representative' OR GetProfileAttr("Primary User Role Name") =  
'Sales Operations' OR GetProfileAttr("Primary User Role Name") =  
'Consultant' OR GetProfileAttr("Primary User Role Name") =  
'Project Manager'
```

This example restricts the Calendar Home Page To Do List applet to users not associated with any role or users associated with one of the following roles: Field Sales Representative, Sales Operations, Consultant, or Project Manager.

Configuring Visibility of Pop-Up and Pick Applets

Pop-up visibility determines what data will be shown when a pop-up pick applet is displayed, for example, when a user associates a contact with an account, or adds a sales representative to the sales team.

Pop-up visibility is usually set using the Popup Visibility Type property of the business component object in Siebel Tools. When pop-up visibility is set in this way, any pop-up based on that business component will show the same data for all users.

NOTE: This section provides configuration background information. It does not provide detailed instructions for working in Siebel Tools. For information about using Siebel Tools, see *Siebel Tools Reference, MidMarket Edition*.

There are often circumstances where you need greater flexibility when determining what data should be shown in pop-up pick applets. For example:

- Most employees of your company only need to see positions for your organizations when they are assigning a sales representative to the sales team.
- Partner Managers need to see positions for your organization, as well as the partner organizations that they manage.

There are also many scenarios where your partners should have more restrictive visibility than your employees.

In order to meet this business requirement, Siebel eBusiness Applications have three capabilities that allow the developer to override the visibility set in the Business Component Popup Visibility Type property at the business component level in favor of another setting. The developer can:

- Set visibility of the Pick-List Object
- Use the visibility Auto All property
- Use the Special Frame Class and User Property

Setting Visibility of the Pick List Object

Developers can override the visibility set at the business component level by setting a different visibility type on the Pick List object, in the Visibility Type property.

When you do this, you override the visibility set at the business component level in a specific instance of that business component for all users of that instance.

Using the Visibility Auto All Property

For both Pick List Visibility Type and Business Component Pop-up Visibility Type, you can use the Visibility Auto All property to override the visibility type property.

This property will check the current user's responsibility to see if it includes the All Across Organizations view based on the same business component. If the view is found, this visibility type will be overridden and the user will get *All* visibility on the object in question. Otherwise, the visibility type will not be overridden.

For example, if the pop-up visibility on the Opportunities business component is set to Organization with Auto All set to true, most users will see all opportunities for their own organization in an Opportunity pick applet. Users who also have access to the All Opportunities Across Organizations view will see all available Opportunities regardless of organization.

This property makes visibility consistent across views and pop-up pick applets.

This property can override any other visibility type, including Sales Rep, Manager, Organization, and so on. In addition to the Business Component and Pick List properties, this property can be set on the Link object as well.

This property is often used for executives or administrative users, who would usually have access to all of the data in your Siebel application.

Using the Special Frame Class and User Property

The developer can use a special frame class and user property to set visibility for a pick applet on the applet object depending on which application is being used.

For example, if users are running Siebel Sales, the Pick Positions applet for the Sales Team will show positions only for the user's organization.

In order to override the pop-up visibility set at the business component level, the developer must do the following:

- Change the frame class of the applet to `CSSSWEFrameListVisibilityPick`
- Add an applet user property called `Override Visibility`, with the following values:
 - Name: `Override Visibility: [Application Name]`
 - Value: `[Visibility Type]` where the developer can choose from the standard visibility types

Merging Organizations

CAUTION: Siebel Systems does not recommend merging organizations. Because many business objects are multi organizational, you may disrupt these relationships to a significant extent and get unexpected results.

Access Control

Supplemental Access Control

This section provides troubleshooting tips and information about security-related issues that may occur in Siebel applications.

User Authentication Issues

This section describes problems that may occur when authenticating users.

User is unable to work in the Server Administration screen

The server administration component performs its own authentication by verifying that the Siebel user ID it gets from the application object manager is the user name for a database account. Your external authentication system, either Web SSO or Siebel security adapter authentication, returns the user's Siebel user ID and, typically, a database account used by many users from an LDAP or ADS directory.

To allow users to work in the Server Administration screen, for each user in this relatively small group, you must create a database account with the user's Siebel user ID as its user name.

Adding users or changing passwords is not reflected in the directory

If you add users or change passwords in a Siebel application and the changes are not reflected in the directory, make sure the SecExternalUserAdministration parameter is set to FALSE. For more information, see [“System Preferences” on page 175](#).

Having trouble using database authentication for mobile Web clients

Check to see if password encryption is enabled for the client. You cannot use database encryption if you have enabled password encryption because this would require the mobile client to use an encrypted password to log in to the local database.

Having trouble running the LDAP/ADSI Configuration Utility

Try running the utility from the machine that hosts the Siebel application you want to configure. The utility works best if run locally, rather than over the network.

Responsibilities in the directory conflict with responsibilities in Siebel applications

Siebel Systems recommends assigning user responsibilities in the directory or by using a Siebel application, but not both. For more information, see [“Roles” on page 137](#).

Upgrading my Siebel application appears to disable checksum validation

You must recalculate the Security Adapter CRC checksum value whenever you upgrade your Siebel applications. For more information, see [“Checksum Validation” on page 149](#).

“Web Authentication Failed” error message appears in an application log file

If your installation is configured for Web SSO (without anonymous browsing) and the ProtectedVirtualDirectory parameter is not set, this message may appear.

To fix this error, set the ProtectedVirtualDirectory parameter in the eapps.conf file to the same value as the application directory. For example:

```
[ /eSales ]  
ProtectedVirtualDirectory=/eSales
```


User Registration Issues

This section describes problems that may occur when registering users. For additional information about troubleshooting workflow processes, see *Siebel Business Process Designer Administration Guide, MidMarket Edition*.

Workflows do not appear in the Workflow Administration screen

Your server or application is probably running on a different language from the database. For example, a DEU installation is running against an ENU database.

Check your setup. Using Server Manager, connect to the server and run `list param lang` to verify. If the language code is incorrect, you can run `change parameter lang=language code` where *language code* is your three-letter database language code. Restart the server.

When I click New User, either nothing happens or an error appears

Possible causes include:

- One or more of the necessary User Registration workflows have not been activated.
- The language of your application setup does not match the language of the database.
- The workflow is not activated properly.

To correct this problem:

- Activate the workflow processes described in [“Activating Workflow Processes” on page 192](#).
- Using Server Manager, connect to the server and run `list param lang` to verify. If the language code is incorrect, you can run `change parameter lang=language code` where *language code* is your three-letter database language code. Restart the server.

When I click Finish, an “Error updating business component at step ‘Insert New User’” message appears

The problem is often that the user being created already exists in the LDAP directory server. The LDAP directory server is not refreshed and is shared by everyone. The user you are trying to create may be new to the database but may already exist in the LDAP directory. This problem commonly occurs if the directory is not refreshed after deployment testing.

Try to create another user or use the LDAP console to check whether the user exists in the directory. Connect to the LDAP server, but instead of creating a new user, right-click on People and select Search.

After I click Finish, the “View not accessible” message appears

The user was successfully created and was able to log in. However, the user that was created did not receive the appropriate responsibility and cannot access the view.

Change the New Responsibility field for the Anonymous User of the application to one that contains the necessary views.

When I click the New User link, nothing happens

Most likely, some or all of the User Registration workflow processes have not been activated; or if they are, the server needs to be restarted.

In the Server Administration screen, restart only the necessary object managers. Restarting the server will also work.

When I click Next in a User Registration view, nothing happens

There may be another workflow that is being triggered and is disrupting the User Registration workflow. It is also possible that not all necessary workflows have been activated. You must activate all the necessary workflows.

To deactivate a disruptive workflow:

- In the Runtime Events Administration screen, click the Events view.
- Query for Object Name is null. Aside from some application type events, there should be nothing else. In particular, be wary of any records whose Action Set Name begins with “Workflow.” Such a record indicates that the workflow is triggered every time the event specified in the Event field happens. This can be particularly disruptive if the event is common, such as ShowApplet or WriteRecord. The Object Name normally constrains the actions to trigger only when the specified event occurs within the context of the object; for example, a specific business component or applet.
- If there is a suspicious Event, drill down on the Action Set Name and note the ID following the string ProcessId in the Business Service Context field. Query against the database to find the suspect workflow: `select NAME from S_WF_STEP where ROW_ID = 'xxx'`, where xxx is the previously noted ID.

That workflow is the disruptive one. Deactivate it.

When I click Finish, an error is returned

Possible causes include:

- The SecExternalUserAdministration system preference is not set to FALSE.
- The SecThickClientExtAuthent system preference is not set to TRUE.
- The server has not been restarted since setting the system preferences. For information about the system preferences related to user authentication, see [“System Preferences” on page 175](#).

Check to see if the user exists in the Person view in the User Administration screen. If the user exists but was not given an entry in the LDAP server, then that user would not be able to log in. You can also verify this by trying to create a user in the User view. If you can set the user ID and password, try to log in as that person.

Access Control Issues

This section describes problems related to access control.

Employee user has trouble logging in to a Siebel customer application

Siebel Systems does not recommend using an Employee login account to access a customer application (such as eBrokerage). Instead, give the user a separate login account for the application.

No data appears in a view that has Manager access control

Check the position hierarchy and make sure the job position of the employee trying to access the view has subordinate positions. Views with Manager access control (for example, My Team's Opportunities) do not display data to an employee if the employee's position has no subordinate positions. Not even the employee's own records will appear.

Cannot delete division records

You cannot delete division records because business components throughout your Siebel applications refer to organizational records. Deleting a division might cause invalid references on transactional records. However, you can rename a division or promote a division to an organization.

Cannot modify seed responsibility

Seed responsibilities can not be modified or deleted. Instead, make a copy of the seed responsibility you want to modify and make changes to the copy.

Excessive synchronization time for some mobile users

Make sure the Local Access control field in the Responsibility View list is set properly. This setting determines which views mobile users can work in offline. For faster synchronization time, reduce the number of views that have local access. For more information, see [“Local Access” on page 292](#).

Encryption Issues

This section describes problems related to encryption.

Having trouble encrypting numeric data with RC2 encryption

Siebel Systems does not support RC2 encryption for numeric data. To encrypt a calculated numeric field, map the field to a string field, and then set the encryption property of the string field to true. The get-value and set-value methods for the calculated field will take care of the conversion between numeric data and string data. As long as the business component uses the calculated field, encryption and decryption is transparent to the application. The only limitation for this work around is that sorting and direct queries can not be performed on a calculated field.

Siebel Application Configuration File Names

B

This section lists the names of configuration files used by Siebel eBusiness Applications.

Configuration Files

[Table 20](#) contains the names of Siebel application configuration files for MidMarket Edition products.

Table 20. Siebel Application Configuration File Names

Application	Configuration File Name
Siebel Call Center	uagent.cfg
Siebel PRM	scw.cfg
Siebel eCustomer	ecustomer.cfg
Siebel eSales	esales.cfg
Siebel eService	eservice.cfg
Siebel Sales	siebel.cfg
Siebel Service	service.cfg

Siebel Application Configuration File Names

Configuration Files

When you install your Siebel eBusiness Applications, you are provided seed data that is related to authentication and to user access to Siebel applications. This section includes instructions for using these seed data.

In the tables in this section, the term “Customer applications” represents the group of Siebel eSales, eService, and eCustomer.

Seed Employee

One Employee record is provided as seed data at installation, as described in [Table 21](#). This record does not have a database login or a responsibility, but, like other employees, it does have a position and an organization.

Customer users, such as Siebel eService users, are not assigned their own position or organization. When a customer user logs in, the application programmatically associates the proxy employee with the user. The proxy employee provides the following functions:

- Data subsequently created by the user is associated with the organization of the proxy employee, which allows the data to display in views that implement organization access control.
- The user can see data created by the user and by others in views that implement organization access control.

The proxy employee is specified at the application level as a name server parameter.

For information about associating the proxy employee with an application, see [“Siebel Name Server Parameters” on page 172](#).

For information about organization access control, see [“Access Control Mechanisms” on page 265](#).

Table 21. Proxy Employee Seed Data Field Values

Last Name	First Name	User ID	Responsibility	Position	Organization
Proxy	Employee	PROXYE	None	Proxy Employee	Default Organization

Seed Users

[Table 22](#) describes non employee User records provided as seed data.

Table 22. User Seed Data Field Values

Last Name	First Name	User ID	Responsibility	New Responsibility	Used by These Applications
Customer	Guest	GUESTCST	Web Anonymous User	Web Registered User	Customer applications
Channel Partner	Guest	GUESTCP	Unregistered Partner Agent		PRM

Seed Responsibilities

Responsibility records are provided as seed data, as described in [Table 23](#). Responsibilities provided for the seed data User records allow users to see views intended for anonymous browsing, including views from which users can self-register or log in. Other responsibilities are assigned programmatically to self-registering users or are assigned to users manually by internal administrators or delegated administrators.

Table 23. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
Web Anonymous User	Default Organization	Views provided for anonymous browsing	Customer applications
Web Registered User	Default Organization	Views provided for a typical registered user	Customer applications
Web Delegated Customer Administrator	Default Organization	Includes views in the Web Registered User responsibility plus views for administering users	Customer applications
Web Corporate User	Default Organization	Views for eSales corporate user	eSales
Web Purchasing Manager	Default Organization	Views for eSales purchasing manager	eSales
Unregistered Partner Agent	Default Organization	Views provided for anonymous browsing	PRM
Partner Relationship Manager	Default Organization	Views for PRM partner relationship manager	Siebel PRM
Partner Operations Manager	Default Organization	Views for PRM partner operations manager, including views for administering users	Siebel PRM
Partner Sales Manager	Default Organization	Views for PRM partner sales manager	Siebel PRM
Partner Sales Rep	Default Organization	Views for PRM partner sales rep	Siebel PRM
Partner Service Manager	Default Organization	Views for PRM partner service manager	Siebel PRM
Partner Service Rep	Default Organization	Views for PRM partner service rep	Siebel PRM

To see the views included in a responsibility

- 1 Navigate to the Application Administration screen.
- 2 From the Show drop-down list, select Responsibilities.
- 3 In the Responsibilities list, select a responsibility.

The views for the responsibility appear in the Views list.

Seed Position and Organization

The Proxy Employee Position and the Default Organization Division records are provided as seed data. The position exists within the division, and the division is its own organization. The position and division are both assigned to the seed data Employee record.

Seed Database Login

One database login is provided as seed data. It is intended to be used for all users logging in through an external authentication system, and should not be assigned to any individual user.

The login credentials are login = LDAPUSER and password = LDAPUSER. It is strongly recommended that an administrator change the password.

Seed Data

Seed Database Login

Index

A

- access control
 - See also* Access Group access control; catalogs
 - about basic access control 248
 - Access Group, about 275
 - accessible data, sub-organization view 304
 - All access control 274
 - Catalog access control view 305
 - catalogs, overview 250
 - customer data 250
 - defined 248
 - license key, role of 290
 - Manager access control 269, 303
 - master data 249
 - Organizational 304
 - organization-based access control 270
 - personal access control 266
 - personal access control, for controlling views 303
 - position-based access control 267
 - responsibilities, role of 138
 - Sales Team 303
 - single-position access control, about 268
 - single-position access control, Manager view 303
 - strategies 277
 - sub-organization access control 273
 - team access control, about 268
 - view level mechanisms 249
 - view properties, displaying 302
 - visibility applet type 303
- access control, business component view
 - manager setting 270
 - role of 290
 - single or multiple organization 273
 - single-position view mode 268
 - sub-organization setting 274
 - team setting 269
- access control, implementing
 - application, role of 289
 - Owner party type 296
 - private or public record, flag setting 297
 - responsibilities, about 289
 - responsibilities, associating with users 291
 - visibility applet, role of 290
 - Visibility field 297
 - Visibility MVField 297
 - Visibility MVLink 298
 - visibility properties, role of 290
- Access Group access control
 - See also* access control; catalogs
 - about 275
 - administrative tasks, listed 313
 - basic principles 308
 - business scenario 309
 - inheritance rules 308
- Access Group party type, defined 255
- access groups
 - associating with categories 321
 - associating with data 319
 - associating with master data catalog 319
 - catalog access control 276
 - creating 317
 - disassociating from catalog 320
 - disassociating with categories 321

- hierarchy, modifying 318
 - members, adding 317
- Account base and extension tables,
 - illustration 261
- account policies 179
- Active Directory Server. *See* ADS
- Active Directory Services Interface adapter.
 - See* ADSI adapter
- adapter-defined user name
 - deployment option 84
 - implementing 154
- Admin mode, visibility 275, 305
- administrative tasks, employees
 - deactivating 230
- administrative tasks, organizational
 - company structure, setting up 278
 - divisions, setting up 283
 - organizations, setting up 281
- administrative tasks, positions and responsibilities
 - positions, setting up 286
 - responsibilities, defining 288
- ADS
 - ADS server, configuring as directory 113
 - ADS server, password assignment 113
 - ADS server, setting up 112
 - directory, user management
 - recommendation 78
 - password storage and use 76
- ADSI adapter
 - ADSI client requirement 78
 - ApplicationPassword parameter 170
 - delegated administrator, availability
 - of 236
 - deployment options 84
 - deployment options, listed 80
 - passwords 76
 - security adapter process overview 74
 - system preferences 84
 - UseSSL parameter 170
- ADSI adapter, setup scenario
 - about implementing 85
 - authentication directory, creating 87
 - configuration file parameter values, table
 - of 92
 - configuration file parameter, usage
 - guidelines 93
 - database login, creating 87
 - directory records, about 89
 - installation prerequisites 86
 - process overview 86
 - restarting servers 98
 - server name parameters, editing 97
 - system preferences, usage guidelines 98
 - testing 99
 - user records, adding 90
 - users, creating 88
- All access control
 - about 274, 303
 - mobile user restriction 293
- AllowAnonUsers parameter
 - about 165
 - ADSI adapter setting 123
 - anonymous browsing, setting for 186
 - LDAP and ADSI configuration setting 93
- AnonPassword parameter 163
- AnonUserName parameter 187
- AnonUserPool parameter
 - about 163
 - eapps.cfg setting 92, 119
- anonymous browsing
 - about 185
 - AllowAnonUsers parameter 186
 - AnonUserPool 163
 - anonymous user, role of 185
 - configuration parameters, setting 186
 - implementing 159
- anonymous user
 - about 89, 185, 190
 - automatically-populated fields 191
 - implementing 158
 - parameter controlling 165
 - seed data responsibilities, about
 - using 186
 - user record in Siebel database 90
 - Web SSO authentication 115

- AnonymousPassword parameter 92, 118
 - AnonymousUserName parameter 92, 118
 - applets
 - access control 302
 - business component and visibility 301
 - defined 299
 - display name and visibility 301
 - pick applet visibility 331
 - special frame class for visibility 332
 - viewing properties 300
 - visibility properties, about 300
 - application
 - access control, implications of 289
 - license key and view visibility 290
 - application configuration files. listed 343
 - application user
 - about 89
 - password encryption 147
 - qualities of 145
 - setting up 145
 - Web SSO authentication 115
 - write privileges 225, 236
 - ApplicationPassword parameter
 - about 170
 - LDAP and ADSI setting 95
 - ApplicationUser parameter
 - about 170
 - LDAP and ADSI settings 95
 - APPUSER 89
 - APPUSERPW 89
 - attributes, password storage 76
 - audience for guide 11
 - audit trail 22, 43
 - authentication
 - architecture differences between standard and dedicated Web clients 79
 - methods, comparison table 66
 - methods, overview 65
 - authentication manager
 - See also* database authentication; security adapter authentication; Web SSO authentication
 - process overview 68
 - remote configuration file
 - requirement 152
 - role of 65, 67
 - authentication options
 - adapter-defined user name, implementing 154
 - anonymous browsing, implementing 159
 - anonymous user, implementing 158
 - application user, password encryption 147
 - application user, setting up 145
 - checksum validation 149
 - credentials password encryption 143
 - password encryption 140
 - remote configuration 150
 - roles 137
 - secure login 139
 - secure socket layer, implementing 152
 - shared database account, implementing 153
 - user specification source, implementing 157
 - auto login cookie 178, 182
- ## B
- BaseDN parameter 94, 121, 167
 - business component view mode
 - about data access 295
 - manager setting 270
 - role in access control 290
 - single or multiple organization setting 273
 - single-position setting 268
 - sub-organization setting 274
 - team setting 269
 - viewing mode and visibility fields 295
 - visibility fields 296
 - business components
 - All access control 274
 - control properties, displaying 302
 - overriding visibility 332
 - self-registration 191

- self-registration views 196
- view construction example 306
- visibility applet, about 302
- visibility applet, role in access control 290
- visibility properties, role in access control 290
- business services, custom 197

C

- Cascade flag 308
- Catalog access control view 305
- catalogs
 - See also* Access Group access control
 - about 251
 - about accessing 250
 - about user experience 313
 - access control strategy 277
 - access control, types of 276
 - Access Group access control principles 308
 - access groups, associating with data 319
 - administrative tasks, listed 314
 - associating access group and data 319
 - categories, role of 251
 - controlling access to categories 308
 - disassociating access groups 320
 - granting access to 276
 - navigating 313
 - properties of 251
 - role in master data 250
- categories
 - access groups, associating with data 319
 - administration tasks, listed 314
 - associating with access groups 321
 - company structure, described 278
 - controlling access to 308
 - disassociating with access groups 321
 - inheritance rules 308
 - relation to catalog 251
- categorized data
 - See also* catalogs
 - about user experience 313
- CERT_SUBJECT variable 163
- checksum utility
 - system preference 176
 - validation, setting up 149
- company structure
 - categories, described 278
 - setting up 278
- configuration file
 - activating changes in application configuration file 165
 - adapter name parameter 166
 - AllowAnonUsers parameter 165
 - ApplicationPassword parameter 170
 - ApplicationUser parameter 170
 - authentication parameters 165
 - BaseDN parameter 167
 - comments, designating 165
 - CredentialsAttributeType parameter 168
 - DllName parameter 167
 - eapps.cfg sample parameters 162
 - editing, about 165
 - EncryptApplicationPassword parameter 170
 - EncryptCredentialsPassword parameter 170
 - eservice.cfg sample 138
 - parameter values, table of 92
 - parameter values, usage guidelines 93, 118, 120
 - PasswordAttributeType parameter 168
 - PortName parameter 167
 - relation to client 164
 - remote configuration file requirement 152
 - roles, setting 138
 - RolesAttributeType parameter 169
 - SecureLogin parameter 165
 - ServerName parameter 167
 - SharedCredentialsDn parameter 171
 - SiebelAdapterUsername parameter 171
 - SingleSignOn parameter 170
 - SslDatabase parameter 169
 - TrustToken parameter 171

- UseAdapterUsername parameter 171
 - UseRemoteConfig parameter 171
 - UserNameAttributeType parameter 168
 - UseSSL parameter 170
 - contact users
 - about 231
 - new record, adding 232
 - organizational association 271
 - promoting from contacts 234
 - cookieless session 181
 - cookies
 - auto login cookie 178, 182
 - cookieless mode 181
 - cookieless session 182
 - dynamically generated 181
 - session cookie, about 181
 - credentials
 - authentication against directory 81
 - credentials password encryption 143
 - CredentialsAttributeType parameter 168
 - EncryptCredentialsPassword parameter 170
 - login page 177
 - role in ADSI authentication 74
 - role in LDAP authentication 74
 - security adapter authentication process 82
 - as URL parameters 179
 - CredentialsAttributeType parameter 95, 122, 168
 - CSSSWEFrameListVisibilityPick 333
 - CSSSWEFrameUserRegistration class 199, 207
 - customer data, role in access control 250
- D**
- data, categorized 313
 - database access 42
 - database authentication
 - compared to other methods 66
 - delegated administration, availability of 236
 - implementing 72
 - limitations of 71
 - overview 70
 - password encryption 140
 - password encryption option 72
 - process overview 71
 - secure socket layer (SSL) option 72
 - self-registration 188
 - database login, creating 87, 112
 - DBA password, changing 33
 - DBO password, changing 30
 - dedicated web client. *See* Siebel Dedicated Web Client
 - deduplication
 - about 207
 - deduplication check, disabling 210
 - fields, modifying 209
 - Default Organization Division records, seed data 349
 - delegated administration
 - administrator access 237
 - authentication requirements 236
 - delegated administrator responsibility, restricting 292
 - new customers, registering 238
 - partner applications, about 240
 - partner user, registering 241
 - registering users, about 237
 - responsibilities, assigning 243
 - write privileges, user directory 236
 - delegated administrators
 - about 236
 - inheritance of responsibilities 235
 - New Responsibility field, editing 235
 - deployment options, LDAP and ADSI adapters 84
 - directory
 - administration setting 175
 - application user, role of 145
 - application user, setting up 145
 - checking credentials against 81
 - creating users in 114
 - creating, process overview 87
 - directory records, about 89

- implementing and testing, process
 - overview 86
 - permissions record parameter 170
 - requirements 75
 - role of 73
 - shared database account deployment
 - option 84
 - user privileges, about 77
 - user records, adding 90
 - user, creating 88
 - Division
 - base and extension tables,
 - illustration 262
 - relation to organization 263
 - divisions
 - division records, deleting 283
 - role of 283
 - setting up 283
 - divisions in Organization party type 265
 - DllName parameter 93, 121, 167
 - duplicate users
 - deduplication fields, modifying 209
 - self-registration deduplication check,
 - disabling 210
- E**
- eapps.cfg file. *See* configuration file
 - Employee base and extension tables,
 - illustration 259
 - employee user
 - active position, changing 246
 - defined 259
 - Employee data model 259
 - minimum requirements 226
 - new record, adding 227
 - position, active 245
 - position-based access control 267
 - primary position, changing 246
 - relation to partner user 230
 - responsibilities, assigning 294
 - seed data record 346
 - employees
 - assignment rules, about 229
 - availability, setting up 229
 - deactivating 230
 - utilization charts, producing 229
 - EncryptApplicationPassword
 - parameter 96, 123, 170
 - EncryptCredentialsPassword
 - parameter 96, 123, 170
 - encryption 19
 - business component 54
 - credentials password 143
 - password 53, 140
 - Siebel Server 49
 - types of 46
 - eservice.cfg file, LDAP sample 138
 - external authentication
 - anonymous user record 185
 - dedicated Web clients, including 79
 - login credentials 184
 - password storage requirement 76
 - remote configuration option, about 79
 - remote security configuration file
 - requirements 152
 - system testing 99
 - testing Web SSO 125
- F**
- fields, self-registration
 - designating as required 199
 - locating 198
 - required property, removing 201
 - FindContact method
 - Forgot Your Password, modifying 214
 - input fields, adding or deleting 222
 - firewalls 37
 - Forgot Your Password
 - about 212
 - architecture 213
 - comparison fields, about modifying 218
 - comparison fields, modifying 218
 - input fields, adding or deleting 222
 - new password, retrieving 212
 - null fields, processing of 215
 - process property, creating 220

- Query User step parameters 214
 - workflow process, about modifying 214
- frame class 333
- G**
- Group Access control view 304
- GUESTCP 347
- GUESTCST 347
- GUESTPW 89
- H**
- high interactivity client, self-registration 188
- I**
- IIS Admin service, restarting 125
- IIS Web server, configuring 113
- Info Center Explorer 313
- internal administrator, modifying New Responsibility field 235
- K**
- key exchange 52
- L**
- LDAP adapter
 - ApplicationPassword parameter 170
 - delegated administrator, availability of 236
 - deployment options 80, 84
 - security adapter process overview 74
 - SsIDatabase parameter 169
 - system preferences 84
- LDAP adapter, setup scenario
 - about 85
 - authentication directory, creating 87
 - configuration file parameter values, table of 92
 - configuration file parameters, usage guidelines 93
 - database login, creating 87
 - directory records, about 89
 - installation prerequisites 86
 - process overview 86
 - restarting servers 98
 - server name parameters, editing 97
 - system preferences, usage guidelines 98
 - testing 99
 - user records, adding 90
 - users, creating 88
- LDAP/ADSI configuration utility 129
- LDAPUSER 87
- license agreement, replacing default text 196
- license key, role in view visibility 290
- Lightweight Directory Access Protocol adapter. *See* LDAP adapter
- Local Access flag 292
- login account policies, about implementing 179
- login form
 - additional features 178
 - sample 177
- login page, sample 177
- login password, storage of 76
- login requirements for views, setting or removing 187
- logon, database authentication overview 70
- M**
- Manager access control, about 269
- Manager visibility 270, 274, 303
- manager-subordinate relationship, about 270
- master data
 - access control 275
 - access control strategy 277
 - associating with access group 319
 - organization of 250
 - role in access control 249
- mobile users
 - accessible views 293
 - authentication, restriction 83
 - positions and visibility rules 286

N

- name server parameters
 - editing 97, 98
 - setting, guidelines for 123
- New Responsibility field
 - about 191
 - modifying 235
 - population of 234
- null fields 215

O

- Organization base and extension tables, illustration 263
- Organization group type, administrative tasks 315
- Organization party type
 - defined 263
 - distinguishing features 254
 - divisions, about 265
 - relationship rules 265
- Organizational visibility 304
- Organization-based access control
 - about 270
 - active organization and view access 292
 - associating responsibilities 292
 - multiple organization access, identifying views with 273
 - organization-enabled data, table of 272
 - single and multiple organizations 271
- organizations
 - about 280
 - benefits of 279
 - divisions, role of 283
 - multiple organizations, reasons for 279
 - positions, changing 285
 - setting up 281
- Owner party type 296
- Owner Type Position view mode 303

P

- parties. *See* party types
- partner applications

- delegated administrators, role of 240
- primary position, changing 246
- responsibilities, assigning 243, 294
- Partner Organization base and extension tables, illustration 264
- partner user
 - about 230
 - new user, registering 241
 - position-based access control 267
 - responsibilities, assigning 243, 294
- Party base and extension tables, illustration 255
- Party data model 255
- party types
 - about 252
 - access control, categorized master data 275
 - Access Group party type 255
 - defined 252
 - determining user access 296
 - Organization party type 254
 - parties, defined 252
 - Person party type 252
 - relationships among party types 265
 - table of 252
 - User List party type 255
 - user lists, adding users 316
 - user lists, creating 315
- PasswordAttributeType parameter 95, 122, 168
- passwords
 - See also* Forgot Your Password
 - changing 245
 - encryption 140
 - encryption option, database authentication 72
 - Forgot Your Password architecture 213
 - Forgot Your Password link 212
 - new password, retrieving 212
- permissions, authentication directory parameter 170
- Person

- contrasted with User 258
 - responsibilities, assigning 294
 - Person base and extension tables, illustration 258
 - Person data type, defined 256
 - Person party type, defined 252
 - Personal access control 266, 303
 - Personal visibility 266, 268
 - physical deployment 35
 - pick applet visibility 331
 - Pick List object 332
 - Popup Visibility Type property 331
 - port numbers 40
 - Port parameter 94, 121
 - PortName parameter 167
 - Position base and extension tables, illustration 260
 - position-based access control, about implementing 267
 - positions
 - about 284
 - active position, about 245
 - active position, changing 246
 - active position, designating 267
 - administrative tasks, listed 314
 - changing within organization 285
 - contact users 231
 - deleting 285
 - multiple employees, about 284
 - parent-and-child relationships 285
 - partner users and delegated administrators 241
 - Position data model 260
 - position hierarchy 270
 - position, defined 267
 - primary position 267
 - primary position, changing 246
 - renaming, cautions about 285
 - role in employee definition 259
 - setting up 286
 - Private Field flag 297
 - process properties, creating 220
 - ProtectedVirtualDirectory parameter 92, 119, 164
 - proxy employee 271
 - Proxy Employee Position, seed data 349
 - PROXYE 346
- Q**
- Query User parameters 215
- R**
- RC2 encryption 56
 - referential data, access control strategy 277
 - registered users
 - See also* self-registration
 - about 183
 - Remember My User ID and Password feature 178, 182
 - remote configuration option
 - applicable authentication strategies 150
 - external authentication, about implementing 79
 - implementation guidelines 151
 - Resonate 39
 - responsibilities
 - See also* visibility
 - about 287
 - access control, implications of 289
 - accessing views locally 292
 - Administrative views 288
 - anonymous user 186
 - assigned by delegated administrator 238
 - assigning 138
 - assigning to employee user 294
 - assigning to Partner 294
 - assigning to Person 294
 - assigning to User 294
 - associating with organizations 292
 - associating with partner organizations 241
 - defined 291
 - defining 288

- inheritance of 234
 - New Responsibility field 234
 - relation to job function 287
 - responsibility fields and self-registration 191
 - role of 137
 - seed data 348
 - seed data, modifying 186
 - seed responsibilities, modifying or deleting 287
 - System Preferences view, limiting access 287
 - using roles to associate 76, 137
 - roles
 - applicable authentication strategies 137
 - assigning 138
 - configuration file setting 138
 - storing in directory 76, 137
 - RolesAttributeType parameter 169
 - sample setting, eservice.cfg 138
 - Siebel application setting 96, 123
 - RSA encryption 15
- S**
- S_CONTACT table 256
 - S_EMP_PER table 259
 - S_ORG_INT table 255
 - S_PARTY table 255
 - S_PER_RESP intersection table 258
 - S_USER table 258
 - SADMIN password 28
 - Sales Team access control 303
 - screen, defined 248
 - SecExternalUserAdministration parameter 192
 - SecExternalUserAdministration system preference 124, 175
 - SecThickClientExtAuthent system preference 124, 175
 - secure adapter communications
 - deployment option 85
 - Secure Login deployment option 85
 - secure login, implementing 139
 - secure socket layer (SSL)
 - ADS directory recommendation 78
 - database authentication option 72
 - deployment option 85
 - implementing 152
 - login form transmission parameter 165
 - SsIDatabase parameter 169
 - SecureLogin parameter 93, 120, 165
 - security
 - architecture 16
 - configuring for 25
 - industry standards 15
 - overview 13
 - security adapter
 - See also* LDAP adapter; ADSI adapter
 - administrator login requirement 225
 - deployment options. listed 80
 - directory requirements 75
 - EncryptApplicationPassword parameter 170
 - external security adapters, about
 - implementing 74
 - operation modes 74
 - overview 73
 - SharedCredentialsDn parameter 171
 - single application access 81
 - security adapter authentication
 - adapter-defined user name,
 - implementing 154
 - administration through Web client 192
 - anonymous browsing,
 - implementing 159
 - anonymous user, implementing 158
 - application user, password encryption 147
 - application user, setting up 145
 - architecture diagram 81
 - as authentication service 81
 - benefits 82
 - checksum validation 149
 - compared to other methods 66
 - credentials password encryption 143
 - login password storage 76

- password encryption 140
- remote configuration option, about 150
- roles, use of 137
- secure socket layer, implementing 152
- set-up, process overview 83
- shared database account,
 - implementing 153
- user specification source,
 - implementing 157
- Security Adapter CRC system
 - parameter 176
- Security Adapter CRC system
 - preference 124
- seed data
 - anonymous user, about 90
 - anonymous user, using 186
 - database login 349
 - Default Organization Division
 - records 349
 - Employee record 346
 - GUESTCST user 186
 - non-employee User records 347
 - position hierarchy 270
 - proxy employee 346
 - Proxy Employee Position 349
 - responsibilities seed data chart 348
 - responsibilities, modifying 186
 - self-registration workflow processes,
 - revising 196
 - workflow processes, about
 - modifying 195
- self-registration
 - about 188
 - application-specific examples 188
 - business components 191
 - components of self-registration 190
 - configuration parameter 192
 - deduplication check, disabling 210
 - deduplication, about 207
 - license agreement, replacing default 196
 - registering, user perspective 189
 - views, about modifying 195
- self-registration fields
 - adding fields to a view 202
 - automatic population 191
 - class specification 199
 - data collection process overview 201
 - designating as required 199
 - locating 198
 - modifying deduplication fields 209
 - modifying fields 203
 - preventing duplicate user updates 207
 - required property, removing 201
 - virtual fields, use of 196
- self-registration workflow processes
 - about 192
 - activating 194
 - adding fields to views 202
 - data collection overview 201
 - deduplication checks, disabling 210
 - modifying deduplication fields 209
 - new applets, including 206
 - preventing duplicate user updates 207
 - seed data, revising 196
 - viewing 193
 - views, table of 194
- ServerName parameter 94, 121, 167
- session cookies
 - about 52
 - Siebel Web Engine 181
- shared database account deployment
 - option 84
- shared database account,
 - implementing 153
- SharedCredentialsDN parameter 96, 123
- SharedCredentialsDn parameter 171
- Siebel database
 - adding user records 90
 - position, role of 226
 - user records, adding 90, 116
- Siebel Dedicated Web Client
 - compared to standard Web client 79
 - configuration file 164
 - security adapter system preference 175
- Siebel object manager, ADSI adapter
 - requirements 78

- Siebel Server
 - configuration file 164
 - restarting 125
 - Siebel Web Client, administering security
 - adapter authentication 192
 - Siebel Web Engine
 - configuration parameters, sample 162
 - cookies automatically generated 181
 - Siebel Web Server Extension (SWSE)
 - role in database authentication 71
 - Web server communication DLL 111
 - SiebelAdapterUsername parameter 171
 - SiebelUsernameAttributeType
 - parameter 96, 123
 - single application access 81
 - single parties. *See* parties; Party data model;
S_PARTY table
 - single sign on. *See* Web SSO entries
 - single-position access control 268, 303
 - SingleSignOn parameter 92
 - about 170
 - about deleting 96
 - guideline for setting in eapps.cfg 92
 - suggested setting in eapps.cfg 118
 - SISNAPI (Siebel Internet Session API) 20
 - skills
 - about adding 278
 - spoofing attacks, protecting against 163
 - sscfadsi.dll 121
 - sscfldap.dll 167
 - SslDatabase parameter
 - about 169
 - about deleting 96
 - SSL communication 15
 - standard interactivity, self-registration 188
 - standard Web client and dedicated Web
 - client, compared 79
 - sub-organization access control
 - about 273
 - accessible data 304
 - system preferences
 - editing 176
 - listed 84, 175
 - usage guidelines 98
 - system preferences, setting 124
- T**
- Team access control 268
 - test user
 - about 89
 - Siebel database, adding records for 90
 - Web SSO authentication 115
 - testing external authentication system 99
 - TESTPW 89
 - TESTUSER 89
 - transaction data, access control
 - strategies 277
 - TrustToken parameter 92
 - about 171
 - about deleting 96
 - guideline for setting in eapps.cfg 92
 - spoofing attacks 163
 - suggested entry, eapps.cfg 118
- U**
- Unicode support 61
 - unregistered users
 - See also* anonymous user
 - 183
 - anonymous user record 185
 - configuration parameters 186
 - granting view accessibility 185
 - maximum number allowed 163
 - parameter controlling 165
 - seed anonymous user, about 186
 - URL parameters, entering credentials
 - as 179
 - UseAdapterUsername parameter 96, 123,
171
 - User
 - contrasted with Employee 259
 - defined 258

- responsibilities, assigning 294
 - seed data 347
 - User data model 258
 - User business component, underlying tables 226
 - user credentials
 - source designation parameter 164
 - user directory
 - self-registration parameter 192
 - write privileges 225, 236
 - User List party type, defined 255
 - User lists
 - adding users 316
 - creating 315
 - user profile
 - about updating 244
 - passwords, changing 245
 - personal information, editing 244
 - user records
 - adding to Siebel database 90
 - data collection, process overview 201
 - user registration
 - about 183
 - requirements 184
 - seed data 184
 - User Registration business component
 - comparison fields, modifying 218
 - deduplication fields, excluding 208
 - deduplication fields, modifying 209
 - Forgot Your Password architecture 213
 - new applets 207
 - populating new fields in 203
 - Query User step parameters 215
 - self-registration views 196
 - virtual fields, writing data to 220
 - User Registration business service 214
 - User specification source
 - about 107
 - implementing 157
 - UseRemoteConfig parameter 96, 123, 151, 171
 - UserNameAttributeType parameter
 - about 168
 - ADSI suggested entry 122
 - LDAP suggested values 95
 - users, registered. *See* registered users; self-registration
 - users, unregistered. *See* unregistered users
 - UserSpec parameter 92
 - about 163
 - about deleting 92
 - eapps.cfg suggested value 118
 - UserSpecSource parameter 92
 - about 164
 - about deleting 92
 - eapps.cfg suggested value 118
 - UseSSL parameter
 - about 170
 - about deleting 96
- ## V
- view accessibility, unregistered users 185
 - views
 - adding fields 202
 - displaying view properties 302
 - explicit login requirements, setting or removing 187
 - group access control 304
 - license key and visibility 290
 - limiting access to 287
 - modifying fields 203
 - new applets, including 206
 - responsibility, role in access 291
 - self-registration views, related business components 196
 - self-registration workflow views, table of 194
 - view construction, example 306
 - view, defined 248
 - virtual directories
 - creating 110
 - ProtectedVirtualDirectory parameter 164
 - virtual fields
 - data collection, role in 201
 - self-registration process, role of 196
 - writing data to 220
 - visibility

- See also *access control entries*
 - See also *responsibilities*
 - All 303
 - Manager 270
 - Personal 266, 268
 - positions, role of 284
 - responsibilities, role of 287
 - view visibility properties 290
 - visibility fields 296
 - visibility applet
 - access control, types of 303
 - business component and view connection 290
 - field display, role in 302
 - view construction example 306
 - Visibility Auto All property 332
 - Visibility MVField 297
 - Visibility MVLink 298
 - Visibility Type property 332
- W**
- Web client users, authentication
 - compatibility 83
 - Web server. *See* Siebel Web Server Extension (SWSE)
 - Web SSO
 - anonymous browsing,
 - implementing 159
 - anonymous user, implementing 158
 - application user, about 145
 - application user, password
 - encryption 147
 - checksum validation 149
 - credentials password encryption 143
 - secure socket layer, implementing 152
 - security adapter process overview 74
 - shared database account,
 - implementing 153
 - user credential source designation 164
 - user specification source,
 - implementing 157
 - virtual directory 164
 - Web SSO adapter
 - adapter-defined user name,
 - implementing 154
 - ApplicationUser parameter 170
 - BaseDN parameter 167
 - CredentialsAttributeType parameter 168
 - deployment options, listed 80
 - DllName parameter 167
 - EncryptCredentialPassword parameter 170
 - PasswordAttributeType parameter 168
 - PortName parameter 167
 - remote configuration option, about 150
 - roles, use of 137
 - RolesAttributeType parameter 169
 - ServerName parameter 167
 - SingleSignOn parameter 170
 - SslDatabase parameter 169
 - TrustToken parameter 171
 - UserNameAttributeType parameter 168
 - UseSSL parameter 170
 - Web SSO authentication
 - about 104
 - architecture 104
 - authentication process, overview 105
 - compared to other methods 66
 - implementation considerations 105
 - implementation setup tasks, listed 106
 - implementation, about 106
 - self-registration 188
 - user specification source option 107
 - Web SSO, setup scenario
 - ADS server, configuring as directory 113
 - ADS server, password assignment 113
 - ADS server, setting up 112
 - configuration parameters, usage
 - guidelines 118, 120
 - creating users in the directory 114
 - database login, creating 112
 - IIS Web server, configuring 113
 - installation requirements 109
 - name server parameters, setting
 - guidelines 123
 - sample configuration 108

- servers, restarting 125
- setup tasks 109
- system preferences, setting 124
- testing 125
- user records, adding to Siebel
 - database 116
 - virtual directories, creating 110
- Windows NT, ADSI client requirement 78
- workflow processes
 - activating 194
 - custom business services, about 197
 - revising 197
 - seed data, revising 196
 - seed processes, about modifying 195
 - self-registration 192
 - self-registration workflow views, table
 - of 194
 - viewing 193
- WWW Publishing Service, restarting 125

