Siebel Security Guide

Version 8.0, Rev. C

February 2011

ORACLE

Contents

Chapter 4: Physical Deployment and Auditing

Chapter 5: Communications and Data Encryption

Chapter 6: Security Adapter Authentication

Chapter 8: Security Features of Siebel Web Server Extension

Chapter 9: User Administration

Chapter 10: Configuring Access Control

Appendix A: Troubleshooting Security Issues

Appendix B: Configuration Parameters Related to Authentication

Appendix C: Seed Data

Appendix D: Addendum for Siebel Financial Services

Index

1 What's New in This Release

What's New in Siebel Security Guide, Version 8.0, Rev. C

Table 1 lists some of the changes in this version of the documentation to support this release of the software.

Table 1. New Product Features in Siebel Security Guide, Version 8.0, Rev. C

Topic	Description
"Security Settings for the Web Browser" on page 29	Modified topic. Additional information is provided on Siebel Business Applications' support for the security features provided by Microsoft Internet Explorer, Windows XP, and Vista.
"Changing System Administrator Passwords on Microsoft Windows" on page 34 "Changing the Siebel Administrator Password on UNIX" on page 36	Modified topics. After changing the Siebel administrator database account password, you must re-create the Siebel Server system service using the new administrator password.
"Securing Communications Between the Siebel Web Client and Actuate Active Portal" on page 58	Modified topic. You must enable Secure Sockets Layer (SSL) for communication between the Siebel Web Client and the Actuate Active Portal if you have enabled SSL for communications between the Siebel Server, the Web server, and the Siebel Web Client.
"Using the Siebel Strong Encryption Pack with Siebel Reports Server" on page 60	New topic. It describes the steps you must perform to use the Siebel Strong Encryption Pack with Siebel Reports Server.
"About Certificates and Key Files Used for SSL Authentication" on page 67	Modified topic. The information on the supported certificate file formats has been updated. Additional information is provided on using certificates that use encryption key sizes larger than 1024 bits.
"Installing Certificate Files" on page 69	Modified topic. When you use the mwcontrol utility to install a certificate file, the certificate file must be located on a local volume. The mwcontrol utility is only used for installing certificate authority and certificate files if you are implementing SSL for the EAI HTTP Transport business service.
"Configuring SSL Mutual Authentication" on page 72	Modified topic. Client authentication using EAI HTTP Transport for outbound Web services is supported in the current release.

Table 1. New Product Features in Siebel Security Guide, Version 8.0, Rev. C

Topic	Description
"Requirements for Data Encryption" on page 84	Modified topic. When creating a link object to define a one-to-many relationship between two business components, the source and destination fields specified in the link object definition must not be encrypted fields.
"Configuring Encryption and Search on Encrypted Data" on page 87	Modified topic. You cannot encrypt columns in database tables without the assistance of Oracle's Application Expert Services.
"Installing the Siebel Strong Encryption Pack" on page 98	Modified topic. After installing the Siebel Strong Encryption Pack, you must reencrypt the Siebel administrator password.
"Reencrypting Masked Parameters" on page 102	Modified topic. The parameters that you must reencrypt if you increase the encryption level are described. Information is also provided on where each parameter can be changed.
"Comparison of LDAP and ADSI Security Adapters" on page 116	New topic. It describes the differences in functionality provided by the Lightweight Directory Access Protocol (LDAP) and Active Directory Services Interfaces (ADSI) security adapters.
"About Installing LDAP Client Software" on page 122	Modified topic. The instructions for installing the IBM LDAP Client and IBM GSKit have been amended.
"Installing the IBM LDAP Client and IBM GSKit on Oracle Solaris" on page 124	Modified topic. Before installing the IBM LDAP Client and GSKit on Oracle Solaris, you must relocate any non-IBM LDAP files that exist on Oracle Solaris.
"About Migrating from Database to LDAP or ADSI Authentication" on page 156	New topic. It describes the issues you must consider when migrating from database authentication to LDAP or ADSI authentication, and it outlines the tasks involved.
"Configuring Adapter-Defined User Name" on page 169	Modified topic. The OM - Username BC Field parameter is case sensitive. The value specified for this parameter must match the value specified for the parameter in Siebel Tools.
"Logging Out of Siebel Business Applications" on page 201	New topic. To log out of Siebel Business Applications that use standard interactivity mode, you must choose File and then Close from the Web browser menu.
"Deactivating an Employee" on page 236	Modified topic. To assign an employee a status of inactive, you must change the employee's status to Terminated.
"Creating Task Links for a Responsibility" on page 303	Modified topic. You can create hyperlinks between a responsibility and the tasks associated with it. These task links are then displayed on the home page for employees assigned the responsibility.
"About Using the Special Frame Class and User Properties" on page 312	Modified topic. To override the visibility of an MVG applet set at the business component level, change the frame class of the applet to CSSSWEFrameListVisibilityMvg.

Table 1. New Product Features in Siebel Security Guide, Version 8.0, Rev. C

Topic	Description
“Parameters for Database Authentication” on page 341	Modified topic. The description of the Propagate Change parameter has been revised. An administrator can change only the password associated with his or her own login ID using the Administration - User screen.
“Parameters for LDAP or ADSI Authentication” on page 342	Modified topic. If you use the LDAP security adapter to authenticate against Microsoft Active Directory, set the value of the Password Attribute Type parameter to either unicodePWD or userPassword, depending on the code page used by the directory server.

What’s New in Siebel Security Guide, Version 8.0, Rev. B

Table 2 lists some of the changes in this version of the documentation to support this release of the software.

Table 2. New Product Features in Siebel Security Guide, Version 8.0, Rev. B

Topic	Description
“Types of Encryption” on page 63	Modified topic. Communications encryption between the Siebel Server and the Database Server is performed externally to Siebel Business Applications. Contact your RDBMS vendor for information on how to configure communications encryption between the Siebel Server and the Database Server.
“Enabling SSL Acceleration for Web Server and Web Client Communications” on page 80	New topic. In Siebel 8.0, you can deploy SSL acceleration for communications between Siebel Web Clients and the Web Server.
“Modifying the Input File” on page 94	Modified topic. You can optionally specify the WHERE clause, the N flag, and the H flag for each column in the encrypt_colums.inp file. Optional flags are specified on the line following the column name line.
“Running the Encryption Upgrade Utility” on page 95	Modified topic. Added a warning that you must not run the Encryption Upgrade utility with the NONE parameter specified on the same data twice. If you do, you will encrypt data that is already encrypted, leading to a permanent loss of data.
“Using Database Authentication with MS SQL Server” on page 114	Modified topic. If you implement database authentication and you are using Siebel 8.0 with a Microsoft SQL Server database, ensure that you select the appropriate ODBC DSN configuration settings. Select the SQL Server authentication option to ensure that Siebel Web clients cannot log in to Siebel Business Applications without providing a password.

Table 2. New Product Features in Siebel Security Guide, Version 8.0, Rev. B

Topic	Description
“Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client” on page 128	New topic. After installing the IBM LDAP Client, you must add the directory path of the IBM LDAP 6.0 libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) script file.
“Configuring Secure Communications for Security Adapters” on page 166	Modified topic. If you use the LDAP security adapter to authenticate against Active Directory, you must enable SSL if you want to manage user passwords or create new users in the Active Directory.
“Security Adapters and the Siebel Developer Web Client” on page 173	Modified topic. Integrated Security functionality is only supported for Siebel Developer Web clients that access Oracle and Microsoft SQL Server databases. This functionality is not available for Siebel Web clients or Siebel Mobile Web clients.
“Administering Access Control for Business Processes” on page 310	New topic. Business processes can be accessed by all users by default, unless the administrator restricts access to a specified business process.

Additional Changes

The following additional changes have been made:

- *Siebel Bookshelf* is available on Oracle Technology Network (OTN) and Oracle E-Delivery. It might also be installed locally on your intranet or on a network location.
- *Siebel System Requirements and Supported Platforms* is located on OTN.
- Other Siebel CRM documentation (Release Notes, Maintenance Release Guides, Technical Notes, Alerts, Troubleshooting Steps, FAQs, Error Messages) is located on My Oracle Support.

What’s New in Siebel Security Guide, Version 8.0, Rev A

Table 3 lists some of the changes in this version of the documentation to support this release of the software.

Table 3. Changes in Siebel Security Guide, Version 8.0, Rev A

Topic	Description
“Firewall and Proxy Server Support” on page 50	Modified topic. Now includes examples to illustrate Siebel Business Applications’ support for rewriting of the host names and IP addresses of Web servers.
“About Selecting Port Numbers” on page 54	Modified topic. Now includes the range of dynamic port numbers that Siebel Business Applications use.
“About Siebel Security Adapters” on page 110	Modified topic. Provides guidelines on the type of security adapter to use with Siebel Server batch, infrastructure and system management components.

Table 3. Changes in Siebel Security Guide, Version 8.0, Rev A

Topic	Description
"About LDAP or ADSI Security Adapter Authentication" on page 115	Modified topic. Outlines enhancements to the Siebel LDAP security adapter for release 8.0.
"About Configuring Visibility of Pop-Up and Pick Applets" on page 311	Modified topic. Describes how to use the applet user property Override Visibility View and the business component user property Popup Visibility Auto All.

What's New in Siebel Security Guide, Version 8.0

Table 4 lists some of the changes in this version of the documentation to support this release of the software.

Table 4. Changes in Siebel Security Guide, Version 8.0

Topic	Description
"Changing Passwords in the Siebel Management Framework" on page 40	New topic. Describes how to implement Siebel user account password changes in the Siebel Management Framework.
"Changing the Siebel Enterprise Security Token" on page 44	Modified topic. The Web Update Protection Key is now called the Siebel Enterprise Security Token. The corresponding eapps.cfg parameter WebUpdatePassword is now SiebelEntSecToken.
"Managing Encrypted Passwords in the eapps.cfg File" on page 45	Modified topic. The value for the Trust Token (alias TrustToken) in the eapps.cfg file can now be encrypted.
"Auditing for Data Continuity" on page 57	Modified topic. Siebel Business Applications can now maintain an audit trail of when business component fields have been viewed or exported and who viewed or exported business component fields.
"Process of Configuring Secure Communications" on page 66	Modified topic. Describes changes to the Siebel Configuration Wizard used to configure secure communications.
"About Data Encryption" on page 83	Modified topic. This topic now includes formulae to calculate the amount of space to allocate for encrypted data.
"Managing the Key File Using the Key Database Manager" on page 89	Modified topic. The number of characters that you specify for a key cannot exceed 255.
"About Upgrading Data to a Higher Encryption Level" on page 92	Modified topic. The input file for the Encryption Upgrade Utility now supports use of the SQL WHERE keyword.
"Installing the Siebel Strong Encryption Pack" on page 98	New topic. Describes how to install the Siebel Strong Encryption Pack.

Table 4. Changes in Siebel Security Guide, Version 8.0

Topic	Description
“About User Authentication” on page 107	Modified topic. The security adapter used for authentication against Lightweight Directory Access Protocol (LDAP)-compliant directories has been enhanced to include authentication against Microsoft Active Directory.
“About Installing LDAP Client Software” on page 122	Modified topic. This release uses upgraded versions of the LDAP client and GSKit. This topic now describes how to install the LDAP client and GSKit on Linux.
“Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard” on page 134	Modified topic. Describes changes to the Siebel Configuration Wizard used to configure LDAP and ADSI security adapter.
“Configuring Secure Communications for Security Adapters” on page 166	Modified topic. To configure Secure Sockets Layer (SSL) for the Active Directory Services Interface (ADSI) security adapter, you must set the profile parameter UseSsl to TRUE.
“Configuring the Shared Database Account” on page 167	Modified topic. Database credentials for the shared database account can be stored as profile parameters when you use the LDAP security adapter. This functionality is not available if you use the ADSI security adapter.
“Managing Tasks Through Responsibilities” on page 302	New topic. A Siebel administrator can now control who accesses tasks.
“Siebel Application Configuration File Parameters” on page 348	Modified topic. Includes a description of the DisableReverseProxy parameter. Set a value for this parameter as described if you deploy IBM Tivoli Access Manager WebSEAL to authenticate users of Siebel Business Applications with high interactivity in a Web Single Sign-On deployment.
“Seed Responsibilities” on page 354	Modified topic. This release includes three new seed responsibilities that you must assign to Siebel users in the Siebel Management Framework.

2 About Security for Siebel Business Applications

This chapter provides an overview of security resources available for Siebel Business Applications and an overview of configuring security. It contains the following topics:

General Security Concepts

When assessing the security requirements 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.

Industry Standards for Security

Siebel Business Applications adhere to common security standards to facilitate the integration of its applications into the customer environment. Siebel Business Applications are designed so that customers can choose a security infrastructure that best suits their specific business requirements.

Supported standards include:

- **LDAP and ADSI.** Siebel Business Applications provide preconfigured integration with LDAP and ADSI for user authentication purposes. For more information, see "Security Adapters for LDAP and ADSI Authentication" on page 23 and Chapter 6, "Security Adapter Authentication."
- **Communications encryption.** Siebel Business Applications support the use of the following technologies for communications encryption:
  - **SSL encryption and authentication.** Protection of communications between Siebel Business Application components (that is, Siebel Servers and Web servers) by using the SSL, version 3.0 capabilities of supported Web servers.

    For information about the supported uses of SSL in Siebel Business Applications, see "Types of Encryption" on page 63. For information about configuring SSL, see "Process of Configuring Secure Communications" on page 66. For information on how to use SSL to secure user login credentials, see "Implementing Secure Login" on page 200. For information on how to configure Siebel Business Applications so that specific views use SSL over HTTP (HTTPS protocol), see "Configuring a Siebel Web Client to Use SSL" on page 199. For information on how communications between Siebel Servers and directory servers can use SSL, see "Configuring Secure Communications for Security Adapters" on page 166.

    Communications between Siebel Servers and email servers can use SSL. For more information, see *Siebel Communications Server Administration Guide*.
  - **RSA communications encryption.** Communication between Siebel components can be encrypted using RSA encryption algorithms. For more information, see "Process of Configuring Secure Communications" on page 66.

    For supported UNIX or Windows environments, or environments in which both operating systems are supported, Siebel Business Applications support RSA Bsafe. RSA Bsafe is FIPS 140-1 certified.
  - **Microsoft Crypto.** Siebel Business Applications support Microsoft Crypto for supported versions of Microsoft Windows. If the Siebel Server and the Web server are installed on the same computer running Microsoft Windows, then you cannot use Microsoft Crypto. You can use it only when these components run on different Microsoft Windows computers.

    For more information, see "Process of Configuring Secure Communications" on page 66 and "Types of Encryption" on page 63.
- **X.509 certificates.** Siebel Business Applications use the SSL capabilities of supported Web servers to enable authentication based on X.509 client certificates. For more information, see "Digital Certificate Authentication" on page 195.
- **RSA SHA-1 password hashing.** Siebel user passwords can be hashed using the RSA SHA-1 algorithm. For more information, see "About Password Hashing" on page 157.

- **AES and RC2 data encryption.** Siebel data can be encrypted using either Advanced Encryption Standard (AES) or RC2. Multiple key lengths are supported for AES and RC2. For encryption lengths greater than 56-bit RC2, you must install the Siebel Strong Encryption Pack. For more information, see "About Data Encryption" on page 83.

Siebel Business Applications do not provide direct support for the Security Assertion Markup Language (SAML) standard, but this standard can be implemented using third-party authentication products.

About Security Products Supported by Siebel

To augment the security of your Siebel Business Applications deployment, Oracle has alliances with leading security providers. Providers are listed in the Security solution category at

http://www.oracle.com/partnerships/isv/integration/search.html

Oracle also provides a suite of security products, some of which have been certified for use with Siebel:

- For information on the Oracle Identity Management products, go to

  http://www.oracle.com/products/middleware/identity-management/identity-management.html

- For information on the Oracle Identity Management products that are certified for use with Siebel, go to

  http://www.oracle.com/technology/software/products/ias/files/idm_certification_101401.html

  Press CTRL + F to display the Find dialog box, and search on Siebel.

For more information about third-party products supported or validated for use with Siebel Business Applications, see *Siebel System Requirements and Supported Platforms* on Oracle Technology Network.

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
- Web browser security settings

User Authentication for Secure System Access

Siebel Business Applications provide an open authentication architecture that integrates with a customer's selected authentication infrastructure. For more information, see Chapter 6, "Security Adapter Authentication," and Chapter 7, "Web Single Sign-On Authentication."

Siebel Business Applications support these types of user authentication:

- Database authentication

  A database security adapter is provided to support this type of user authentication.

- Lightweight Directory Access Protocol (LDAP) and Active Directory Services Interface (ADSI) authentication

  LDAP and ADSI security adapters are provided to support these types of user authentication.

- Web Single Sign-On (Web SSO)

Customers can also develop custom security adapters using a security adapter SDK.

NOTE: The exact valid character set for a Siebel username depends on the underlying authentication system. For database, LDAP, ADSI, or Web SSO authentication, see documentation from your vendor.

These authentication mechanisms apply whether users access Siebel Business Applications from within a LAN or WAN, or remotely. Figure 1 on page 22 shows a logical view of the three primary types of user authentication within a Siebel site.

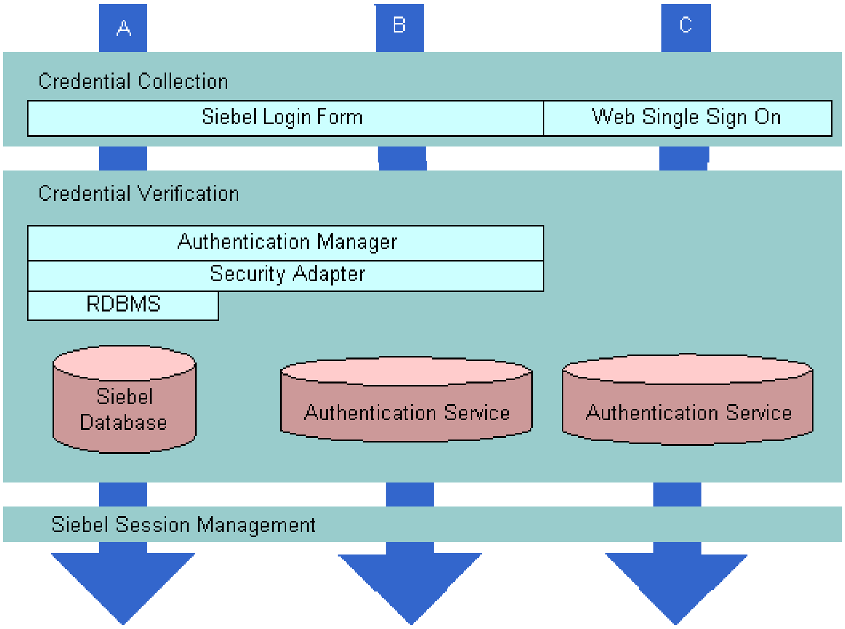


Figure 1. Logical Diagram of User Authentication Methods Within a Siebel Site

Security Adapter for Database Authentication

Siebel Business Applications provide a database security adapter mechanism for credential collection and verification. The default login form collects Siebel username and password credentials. The security adapter works with the underlying security systems of the database to verify users' credentials.

With database authentication, each user must have a valid database account in order to access Siebel Business Applications. The database administrator (DBA) must add all user database accounts. Database authentication deployment supports password hashing for protection against hacker attacks.

All Siebel Business Applications can use database authentication, which is configured as the default. However, some functionality provided by Siebel Business Applications, such as workflow processes to support user self-registration or forgotten password scenarios (capabilities commonly used in customer applications), require authentication using LDAP or ADSI security adapters. For this reason, database authentication is rarely used with customer applications.

Security Adapters for LDAP and ADSI Authentication

For employee or customer applications, Siebel Business Applications include a preconfigured security adapter interface to allow organizations to externalize credential verification in an LDAP or ADSI directory. The interface connects to a security adapter, which contains the logic to validate credentials to a specific authentication service.

Siebel Business Applications customers can therefore verify user credentials with security standards such as LDAP or ADSI.

Siebel Business Applications have developed security adapters for leading authentication services:

- LDAP security adapter integration is currently certified and supported for Oracle Internet Directory, IBM Directory Server, Novell NDS eDirectory, Sun Java System Directory Server, and Microsoft Active Directory.
- ADSI security adapter integration is certified and supported for Microsoft Active Directory.

For information about third-party products supported or validated for use with Siebel Business Applications, see *Siebel System Requirements and Supported Platforms* on Oracle Technology Network. You can also build security adapters to support a variety of authentication technologies. For information on custom security adapters, see "Security Adapter SDK" on page 24.

Web Single Sign-On

Siebel Business Applications offer customers the capability of enabling a single login across multiple Web applications—also known as Web Single Sign-On (SSO). Siebel Business Applications provide a configurable mechanism for communicating with Web SSO infrastructures, identifying users, and logging users into Siebel Business Applications.

With Web SSO, users are authenticated independently of Siebel Business Applications, such as through a third-party authentication service, or through the Web server.

Oracle has alliances with leading security providers for Web SSO integration. Providers are listed in the SSO solution category at http://www.oracle.com/partnerships/isv/integration/search.html.

For information on the Oracle Identity Management products that are certified for use with Siebel, see "About Security Products Supported by Siebel" on page 21.

Security Adapter SDK

Oracle offers the Siebel Security Adapter Software Developers Kit (SDK) to allow companies to build additional security adapters. Such additional adapters can support other authentication technologies such as digital certificates, biometrics, or smart cards.

For example, a security adapter can be created for a device such as the RSA Secure ID token—a portable device that provides users with a key that changes after one minute. When a security adapter for this device is deployed, only by supplying both the currently displayed key and the user's password or other credentials can the user gain access to Siebel Business Applications.

The security adapter interface is critical to the Siebel architecture because, for most Siebel Business Applications 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. The underlying SDK is based on an IBM SDK.

The Siebel Security Adapter SDK is described in 476962.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Technical Note 415.

End-to-End Encryption for Data Confidentiality

Stored data can be selectively encrypted at the field level, and access to this data can be secured. In addition, data can be converted into an encrypted form for transmission over a network. Encrypting communications safeguards such data from unauthorized access. 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 Server, to the database, and back. Figure 2 on page 25 shows the types of encryption available for communications within the Siebel environment.

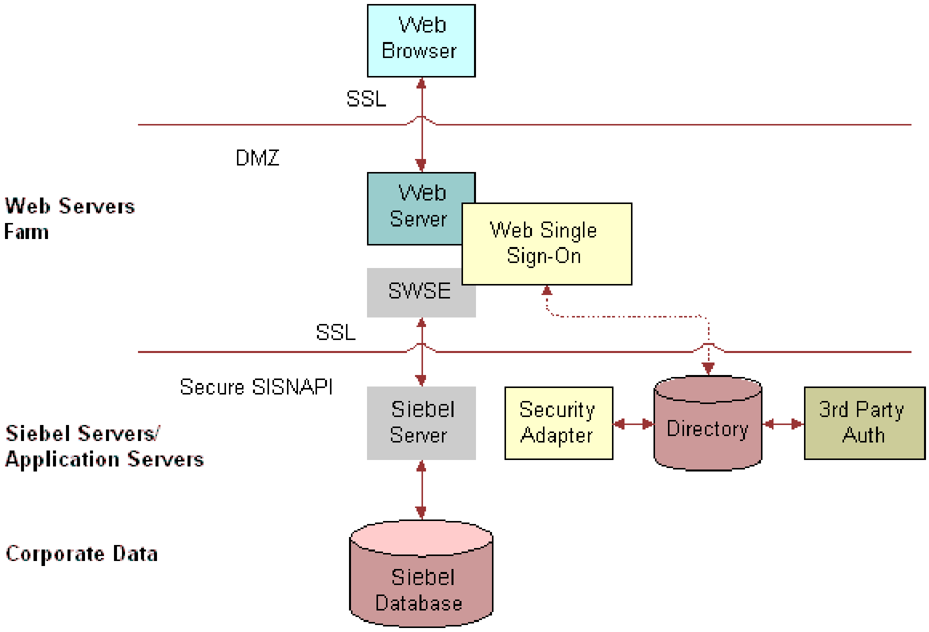


Figure 2. Encryption of Communications in the Siebel Environment

Client Browser to Web Server

Siebel Business Applications run using the Siebel Web Client in a standard Web browser. When a user accesses Siebel Business Applications, a Web session is established between the browser and the Siebel Server, with the Web server in between. Secure Sockets Layer (SSL) protects against session hijacking when sensitive data is transmitted. Siebel Business Applications support 128-bit SSL data encryption, an extremely secure level of protection for Internet communications.

Customers using SSL can configure which Web pages (known as views) within Siebel Business Applications use SSL in the following scenarios:

- Use SSL only on the login view to protect password transmission. See “Login Security Features” on page 200.
- Use SSL for additional specific views (this option is available for standard interactivity applications only). See “Configuring a Siebel Web Client to Use SSL” on page 199.
- Use SSL for the entire application. See “Configuring a Siebel Web Client to Use SSL” on page 199.

Web Server to Siebel Server

Siebel Business Applications 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 Secure Sockets Layer (SSL) or embedded encryption from RSA or Microsoft Crypto APIs. These technologies allow data to be transmitted securely between the Web server and the Siebel Server.

For more information, see "Process of Configuring Secure Communications" on page 66.

Siebel Server to Database

For secure transmission between the database and the Siebel Server, data can be encrypted using the proprietary security protocols specific to the database that a customer is using.

Database Storage

Siebel Business Applications allow customers to encrypt sensitive information stored in the database so that it cannot be viewed without access to Siebel Business Applications. Customers can configure Siebel Business Applications to encrypt 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. Siebel Business Applications support data encryption using AES and RC2 algorithms.

For more information, see "About Data Encryption" on page 83.

Controlling Access to Data

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

- View-level access control to manage which application 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 a unified method of administering access to many content items for many users.

For more information, see Chapter 10, "Configuring Access Control."

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 Business Applications a user can access, based on the functions assigned to that user. In Siebel Business Applications, these functions are called *responsibilities*.

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

Each user’s primary responsibility also controls the user’s default screen tab layout and tasks.

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 who have to view particular data records to access that information.

Siebel Business Applications use three types of record-level access: position, organization, and access group. 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 manager.

- Similarly, an organization—such as a branch of an agency or a division of a company—is a grouping of positions that map to the physical hierarchy of a company. Those employees assigned to a position within a certain organization are granted access to the data that has been assigned to that organization. Visibility to data can be set up to restrict employees from accessing data outside their own organization.
- An access group is a less-structured collection of users or group of users, such as a task force. Groups can be based on some common attribute of users, or created on an ad hoc basis, pulling together users from across different organizations and granting them access to the same data.

Support for Auditing in a Siebel Environment

Siebel Business Applications support various degrees of auditing:

- At the simplest level, each data record has created and last updated fields (when and by whom). With additional configuration, you can generate an activity for additional levels of auditing. This is best used when there are limited requirements for auditing, for example, just a few areas to track.
- Siebel Business 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. It is also possible to maintain an audit trail of when the business component fields have been viewed or exported and who viewed or exported fields. Audit Trail is a configurable feature that allows users to choose business components and fields to audit, and to determine the scope of the audit.

  Siebel customers can choose to audit all activity, or to limit the scope of auditing to those operations performed by certain responsibilities, positions, or employees. Siebel Business Applications also allow customers to audit specific data fields or objects.

- 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.)

- Using Siebel Workflow, you can 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.

For more information, see "Auditing for Data Continuity" on page 57.

Secure Physical Deployment to Prevent Intrusion

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

In Siebel Business Applications deployments, the Web server resides in the *demilitarized zone* (DMZ). Clients outside the firewall access the Web server and the Siebel Server through a secure connection.

- In employee application deployment, clients as well as servers often reside behind a firewall.
- In customer or partner application deployment, or in employee application deployment where employees accessing the application are outside of the firewall, the Siebel Server is deployed behind an additional firewall.

Siebel Business Applications also support reverse proxy configuration to further enhance the DMZ security. Increasingly, firewall vendors offer virtual private network (VPN) capabilities. VPNs provide a protected means of connecting to Siebel Business Applications for users (such as employees) who require remote access.

Siebel Business Applications work with leading third-party vendors to provide additional physical security measures, such as attack prevention, data back-up, and disaster recovery. For example, HTTP load balancing protects against denial-of-service attacks by handling TCP connections and catching incoming attacks before they reach the Siebel Server. Furthermore, only one IP address and one port have to be opened on the firewall between the Web server and the Siebel Server.

The architecture of Siebel Business Applications takes advantage of high availability technologies, such as Microsoft Cluster Services, which allow multiple computers to function as one by spreading the load across multiple systems. High availability technologies address the requirement for failover and catastrophic recovery management. For more information, see *Siebel Deployment Planning Guide*.

For more information, see Chapter 4, "Physical Deployment and Auditing."

Security for Mobile Solutions

Oracle provides a suite of mobile solutions that allow remote access to data within Siebel Business Applications. These solutions support a variety of mobile platforms, including wireless phones, handhelds, and laptop computers (running Siebel Mobile Web Client).

Oracle provides security for customers using these devices to access Siebel Business Applications, and works with alliance partners for other types of mobile devices.

- For information about security issues for Siebel Wireless applications, see *Siebel Wireless Administration Guide*.
- For information about security issues for Siebel Handheld applications, see documentation for particular Siebel Business Applications that use the Siebel Handheld client on *Siebel Bookshelf*.
- For information about security issues for Siebel Mobile Web Client, which can be installed on mobile devices such as laptop computers, see "Configuring Encryption for Mobile Web Client Synchronization" on page 82 and "Authentication for Mobile Web Client Synchronization" on page 176.

  See *Siebel Remote and Replication Manager Administration Guide* for additional Mobile Web Client security issues.

Secure Real-Time Wireless Communications

Siebel Wireless provides real-time wireless access to Siebel Business Applications through browser-enabled mobile devices. Siebel Wireless views rendered in XML or HTML are sent through the Web server on which the Siebel Web Server Extension (SWSE) is installed to a wireless network, and ultimately to the requestor's browser-enabled, wireless device.

In this enterprise solution, the Web server and the Siebel Server reside within the firewall of the Siebel customer, thereby protecting data security. Standard protocols are used to secure browser-based data transmissions across the wireless network.

Multiple methods of securing the data are available, including the Wireless Transport Security Layer, the equivalent of Secure Sockets Layer (SSL) for wireless devices and third-party products.

Mobile Device User Authentication

Mobile devices themselves must be secure. If a wireless or handheld device falls into the wrong hands, organizations must be assured that sensitive data will not be compromised. Siebel Business 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.

Security Settings for the Web Browser

Certain features and functions in Siebel Business Applications work in conjunction with security or other settings on the Web browser.

Some of the security features provided by Microsoft Internet Explorer, Windows XP, and Vista are not supported when used with Siebel Business Applications. For information on the features currently supported, see the following:

- For information on Internet Explorer 8 support, see 796015.1 (Article ID) on My Oracle Support.
- For information on Internet Explorer 7 support, see 475275.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Alert 1251.

- For information on Microsoft Vista support, see 780814.1 (Article ID) on My Oracle Support.
- For information on Web client deployment options, see 476952.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Technical Note 418.

Detailed information about the browser settings used in deploying Siebel clients is provided in *Siebel System Administration Guide*. For more information about settings in your Web browser, see the documentation that came with your browser, and *Siebel System Requirements and Supported Platforms* on Oracle Technology Network.

Web Sites With Security Information

The following Web sites provide information about managing security on your network and about industry trends in security:

- Oracle Application Security and Compliance page at

  http://www.oracle.com/security/security-solutions.html

- RSA Laboratories home page at

  http://www.rsa.com/rsalabs/

- RSA Laboratories Crypto FAQ at

  http://www.rsa.com/rsalabs/node.asp?id=2152

- CERT Coordination Center, Carnegie Mellon University at

  http://www.cert.org

- Microsoft Security & Privacy home page at

  http://www.microsoft.com/security/

NOTE: Web sites are subject to change. If a URL listed previously is no longer active, try using a Web search engine to find the new location.

Roadmap for Configuring Security

This topic provides a general overview of tasks you can perform to take advantage of security resources for Siebel Business Applications. Use the information in this topic as a checklist for setting up security for your Siebel environment.

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

1. During Siebel Business Applications installation, plan your Siebel Server and third-party HTTP load balancer TCP port usage for firewall access. See Chapter 4, “Physical Deployment and Auditing.” See also the *Siebel Installation Guide* for the operating system you are using.
2. After you install your Siebel site, change the default passwords for Siebel accounts. For more information, see Chapter 3, “Changing or Adding Passwords.”

   - Change the password for the Siebel administrator account.

- Add a password for updating Web server images.

3. Make sure communications and important data is encrypted. See Chapter 5, "Communications and Data Encryption."

4. Implement security adapter authentication or Web Single Sign-On to validate users. For more information, see Chapter 6, "Security Adapter Authentication," and Chapter 7, "Web Single Sign-On Authentication."

5. Set up an access control system to control user visibility of data records and Siebel Business Applications views. For more information, see Chapter 10, "Configuring Access Control."

6. Enable audit trail functionality to monitor database updates and changes. See "Auditing for Data Continuity" on page 57. See also *Siebel Applications Administration Guide*.

7. Make sure communications between Mobile Web Clients and your Siebel site are secure.

   Enable encryption for Mobile Web Clients. See "Configuring Encryption for Mobile Web Client Synchronization" on page 82.

   For other Mobile Web Client security issues, such as changing passwords on the local database, and encrypting the local database, see *Siebel Remote and Replication Manager Administration Guide*.

3 Changing or Adding Passwords

This chapter provides guidelines on how to change passwords. It includes the following topics:

For information about configuring and using hashed user passwords and database credentials passwords through your security adapter, see "About Password Hashing" on page 157.

Changing Passwords

The Siebel Database Configuration Wizard and the seed data provided with Siebel Business Applications create several 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.

NOTE: For information about changing the local DBA password on Mobile Web Clients, see *Siebel Remote and Replication Manager Administration Guide*.

The topics that follow include procedures for changing account passwords. Before you change default passwords, review the following points:

- For Siebel end users, the availability of the Password and Verify Password fields (User Preferences screen, User Profile view) depends on several factors:
  - For an environment using LDAP or ADSI authentication, the underlying security mechanism must allow this functionality. See also "Requirements for the LDAP or ADSI Directory" on page 118.

    In addition, the Propagate Change parameter (alias PropagateChange) must be TRUE for the LDAP or ADSI security adapter (default is TRUE). For Siebel Developer Web Client, the system preference SecThickClientExtAuthent must also be TRUE. For more information, see Chapter 6, "Security Adapter Authentication."

    - For an environment using database authentication, the Propagate Change parameter (alias DBSecAdpt_PropagateChange) must be TRUE for the database security adapter. The default is FALSE for the parameter defined in the Siebel Gateway Name Server, FALSE for the same parameter defined in application configuration files for the Developer Web Client. For more information, see Chapter 6, “Security Adapter Authentication.”

- The procedures in this topic describe changing parameters at the Enterprise level that specify passwords. If you set and change passwords at this level, the changes are inherited at the component level.

  However, if you set a password parameter at the component level, from that point forward, this password can be changed only for this component. Changing it at the Enterprise level will not cause the new password to be inherited at the component level, unless the override is deleted at the component level. For more information, see *Siebel System Administration Guide*.

- If you are using a third-party load balancer for Siebel Server load balancing, make sure load-balancer administration passwords are set. Also make sure that the administrative user interfaces for your load-balancer products are securely protected. See the following topics for more information about changing passwords:

- “Changing System Administrator Passwords on Microsoft Windows” on page 34

- “Changing the Siebel Administrator Password on UNIX” on page 36

- “Changing the Table Owner (DBO) Password” on page 38

- “Troubleshooting Password Changes By Checking for Failed Server Tasks” on page 39

Changing System Administrator Passwords on Microsoft Windows

Before you run the Database Configuration Wizard to configure the Siebel database on the RDBMS, you must create the table owner and administrator accounts, either manually (on IBM DB2) or using the grantusr.sql script. The default user ID and password for the administrator account is SADMIN and SADMIN (case-sensitive). It is recommended that you change the password for this account before running the grantusr.sql script. You can change the password for the Siebel administrator account using the procedures provided in this topic. For additional information on creating the Siebel administrator account, see *Siebel Installation Guide* for the operating system you are using and *Implementing Siebel Business Applications on DB2 for z/OS*.

You might also want to change the password for the Siebel service owner account, which is the Windows user account that starts the Siebel Server system service.

Separate procedures are provided for changing the password for the Siebel service owner account and for changing the password for the Siebel administrator database account.

NOTE: Do not use ' or " (single or double quotation marks) as part of a password. Because quotation marks are used as special characters in some contexts, using them within a password can cause the password to be truncated. For example, the password abcde"f might be truncated to abcde.

Changing the Password for the Siebel Service Owner Account

Use the procedure below to modify the password for the Siebel service owner; this is the Windows user account that starts the Siebel Server system service.

To change the password for the Siebel service owner account

1. Change the Windows domain login password for the Siebel service owner account.

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

2. Change the password for the Siebel Server system service.

   a. From the Start menu, choose Settings, Control Panel, Administrative Tools, and then the Services option.

   b. Right-click on the Siebel Server System Service, and select Properties.

   c. In the Properties dialog box for this service, click the Log On tab.

   d. Enter the password in the Password and Confirm Password fields, and click OK.

   The password specified here must correspond to the Windows domain login password you modified in Step 1.

3. Stop and restart the Siebel Server system service.

   For details, see *Siebel System Administration Guide*.

Changing the Password for the Siebel Administrator Account

Use the following procedure to modify the password for the Siebel administrator account. You must change the Siebel administrator database account, change the corresponding password parameter for the Siebel Enterprise, then delete the Siebel Server system service and re-create it using the new password.

To change the password for the Siebel administrator account

1. Change the Siebel administrator's database account password using either the Server Manager command or the Siebel user interface.

   The following steps describe how to change the password using the Siebel user interface.

   a. Log into a Siebel employee application, such as Siebel Call Center.

   b. Navigate to the Administration - Server Configuration screen, and then the Enterprises view.

   c. Click the Parameters tab.

   d. In the Enterprise Parameters list, select the Password parameter.

   e. In the Value field, enter the new password, then commit the record.

2. Log out of the Siebel Business Applications (all users must log out).

3. Change the Siebel administrator's password in the database.

4 For more information, see your RDBMS documentation on changing passwords.On each Siebel Server in your Siebel Enterprise, delete the existing Siebel Server system service, then re-create it with the new administrator password as follows:

a Delete the Siebel Server system service using the following command:

```
siebctl -d -S siebsrvr -i “EnterpriseName_SiebelServerName"
```

where *EnterpriseName* is the name of your Siebel Enterprise and *SiebelServerName* is the name of the Siebel Server. For example:

```
siebctl -d -S siebsrvr -i “sia80_app01"
```

b Re-create the Siebel Server system service using the following command:

```
siebctl -h SIEBEL_ROOT -S siebsrvr -i "EnterpriseName_SiebelServerName" -a
-g "-g GatewayServerHostname:port -e EnterpriseName -s SiebelServerName -u
sadmin" -e NewPassword -u NTAccount -p NTPassword
```

where:

- *SIEBEL_ROOT* is the installation directory of the Siebel Server
- *EnterpriseName* is the name of your Siebel Enterprise
- *SiebelServerName* is the name of the Siebel Server
- *GatewayServerHostname* is the name of the Gateway Name Server host
- *port* is the port number of the Gateway Name Server
- *sadmin* is the administrator user ID
- *NewPassword* is the new Siebel administrator password in clear (unencrypted) text. The siebctl utility encrypts the password.
- *NTAccount* is the Siebel service owner account name
- *NTPassword* is is the Siebel service owner account password

For example:

```
D:\sia80\siebsrvr\BIN>siebctl -h "d:\sia80\siebsrvr" -S siebsrvr -i
"sia80_app01" -a -g "-g localhost:2320 -e sia80 -s app01 -u sadmin"
-e admin6! -u .\SADMIN -p admin6!
```

5 Start the Siebel Server system service.

For information on how to start the Siebel Server system service, see *Siebel System Administration Guide*.

Changing the Siebel Administrator Password on UNIX

The Siebel Database Configuration Wizard installation task 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). Change the password for this account.

Do not use single or double quotation marks as part of a password. Because quotation marks are used as special characters in some contexts, using them within a password can cause the password to be truncated. For example, the password abcde"f might be truncated to abcde. For more information about setting up this account for initial use, see *Siebel Installation Guide for UNIX*.

To change the password for the Siebel administrator database account

1 End all client sessions and shut down the Siebel Server using the following command:

```
SIEBSRVR_ROOT/bin/stop_server all
```

To stop all Siebel Servers in the Siebel Enterprise, you must run this command on all Siebel Server computers.

2 Change the Siebel administrator's database account password using either the Server Manager command or the Siebel user interface.

The following steps describe how to change the password using the Server Manager command:

a Log in at the Enterprise level.

```
srvrmgr -g SiebelGatewayName -e EnterpriseServerName -u UserName -p Password
```

b At the Server Manager prompt, enter the following command:

```
change enterprise param Password=NewPassword
```

3 Change the password in the database.

For more information on changing passwords, see your RDBMS documentation.

4 Change the password in the service (svc) file on each Siebel Server in your Siebel Enterprise.

CAUTION: Do not edit the svc file manually; doing so can corrupt the file. Instead, make a backup copy of the existing svc file, then re-create the svc file with the new password using the siebctl utility.

The following procedure describes how to re-create the svc file with a new administrator database account password:

a Navigate to the $siebsrvr/sys directory and rename the existing svc file. The svc file name is in a format similar to the following:

```
svc.siebsrvr.siebel:siebsrvrname
```

where *siebsrvrname* is the name of the Siebel Server.

b In the $siebsrvr/bin directory, run the following command to re-create the svc file with the new Siebel administrator password:

```
siebctl -r ''$Siebsrvr'' -S siebsrvr -i EnterpriseName:SiebsrvrName -a -g "-
g GatewayServerHostName:gtwyport -e EnterpriseName -s SiebsrvrName -u sadmin"
- e NewPassword -L ENU
```

where:

- ''*$Siebsrvr*'' is the installation directory of the Siebel Server

- *EnterpriseName* is the name of your Siebel Enterprise
- *SiebsrvrName* is the name of the Siebel Server
- *GatewayServerHostName* is the name of the Gateway Name Server host
- *gtwyport* is the port number of the Gateway Name Server
- *sadmin* is the administrator user ID
- *NewPassword* is the new Siebel administrator password in clear (unencrypted) text. The siebctl utility encrypts the password.

For example:

```
siebctl -r "/data/siebel/sia80/siebsrvr" -S siebsrvr -i TRN_ENTP:TRSIEBSRV2-
a -g "-g HBGNOVOAS04:2320 -e TRN_ENTP -s TRSIEBSRV2 -u sadmin" -e admin6!
-L ENU
```

The siebctl utility re-creates the svc file with the new encrypted password value.

5 Stop and restart the Siebel Gateway Name Server using the following commands:

```
$SIEBEL_ROOT/SiebelGatewayName/bin/stop_ns
$SIEBEL_ROOT/SiebelGatewayName/bin/start_ns
```

6 Restart all Siebel Servers using the following command:

```
$SIEBEL_ROOT/ServerName/bin/start_server all
```

Perform this step for each applicable Siebel Server.

7 Connect to the Server Manager and verify the password change:

```
srvrmgr -g SiebelGatewayName -e EnterpriseServerName -s SiebelServerName -u
SADMIN -p NewPassword
```

You can now log in as SADMIN with the new password.

Changing the Table Owner (DBO) Password

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

The Table Owner is used to reference table names in SQL statements that are generated by Siebel Business Applications (for example, SELECT * FROM SIEBEL.S_APP_VER).

A corresponding parameter is configured for the Siebel Enterprise, named Table Owner (alias TableOwner). Siebel Business Applications modules, such as Siebel Application Object Managers (AOMs), use this parameter value to provide the Table Owner name when generating SQL for database operations. You specify the Table Owner name during Siebel Enterprise Server configuration, which provides a value for this parameter.

A related parameter is Table Owner Password (alias TableOwnPass). For most database operations performed for Siebel Business Applications, the Table Owner password does not have to be provided. For this reason, this parameter is not configured during Siebel Enterprise Server configuration. However, if the Table Owner Password parameter is not defined, then the Table Owner password might sometimes have to be provided manually.

Note the following requirements for changing the Table Owner password:

- If you have not defined the Table Owner Password parameter, then the Table Owner password only has to be changed in the Siebel database. (The changed password might also have to be provided manually for certain operations.)
- If you have defined the Table Owner Password parameter, then you must also update the value for this parameter when you change the password in the Siebel database.

To change the password for the Table Owner account

1. Change the Table Owner password for the Enterprise, using Server Manager.
   a. Log into a Siebel employee application, such as Siebel Call Center.
   b. Navigate to the Administration - Server Configuration screen, then the Enterprises view.
   c. Click the Parameters tab.
   d. In the Enterprise Parameters list, locate the Table Owner Password parameter (alias TableOwnPass).
   e. In the Value field, type in the new value, then commit the record.
2. Change the password in the database.

   For more information on changing passwords, see your RDBMS documentation.
3. Restart the Siebel Server.

Troubleshooting Password Changes By Checking for Failed Server Tasks

After you have changed the Siebel administrator (SADMIN) password and the Table Owner password, make sure that all server tasks are still running.

To check for failed server tasks

1. After the Siebel Server restarts:
   a. Log into a Siebel employee application, such as Siebel Call Center.
   b. Navigate to the Administration - Server Management screen, then the Servers view.
   c. In the Siebel Servers list, select the applicable Siebel Server.

   d. Click the Tasks tab and check to see if any server tasks have an error.

      For example, if you are running the Call Center Application Object Manager, check if there is a task for this component that has an error.

2. For each Server Task that displays an error, update passwords for both the Siebel administrator account and the Table Owner for that task.

   a. Navigate to the Administration - Server Configuration screen, then the Enterprises view.

   b. Click the Component Definitions tab.

   c. Select the component that initiated the failed task.

      For example, if Call Center Application Object Manager had a failed task, display the record for the Call Center Object Manager component definition.

   d. Click the Parameters view tab to display parameters for this component definition.

   e. Respecify password values for the applicable parameters for this component definition.

      For example, if the Password or Table Owner Password parameters are not set correctly for the Call Center Application Object Manager component definition, that might be the reason for the failed tasks. If so, reentering the correct values will solve the problem.

3. Restart the Siebel Server computer, and check again if any tasks failed.

Changing Passwords in the Siebel Management Framework

The Siebel Management Framework is an optional deployment in your Siebel environment that provides the underlying infrastructure components to support the Siebel Diagnostic Tool and the Application Deployment Manager (ADM). This topic describes how you can change passwords for the following users in the Siebel Management Framework:

- Siebel Diagnostic Tool user

  During the installation and configuration of the Siebel Management Server with Diagnostic Tool, you specify a Siebel user who accesses the Siebel Diagnostic Tool. For information on how to change the Siebel Diagnostic Tool user’s password in the Siebel Management Framework, see “Changing the Siebel Diagnostic Tool User’s Password” on page 41.

- Siebel user for Siebel Management Server or Management Agent

  During the installation and configuration of the Siebel Management Server with Diagnostic Tool or the Siebel Management Agent, you specify a Siebel user who accesses the Siebel Management Server or Siebel Management Agent. For information on how to change the password for this Siebel user in the Siebel Management Framework, see “Changing a Siebel User Account Password in the Siebel Management Framework” on page 41.

Changing the Siebel Diagnostic Tool User’s Password

This topic describes how you change the password of a Siebel Diagnostic Tool user in the Siebel Management Framework. The Siebel Diagnostic Tool is installed with the Siebel Management Server. During the installation and configuration of the Siebel Management Server with Diagnostic Tool, you specify a user name and password for a Siebel user who accesses the Siebel Diagnostic Tool. For details, see *Siebel Installation Guide* for the operating system you are using. For information about using the Siebel Diagnostic Tool, see *Siebel System Monitoring and Diagnostics Guide*.

The following procedure describes how you change the password of the Siebel user who accesses the Siebel Diagnostic Tool. Before you carry out the procedure, you first change this Siebel user’s password in the Siebel Enterprise.

To change the Siebel Diagnostic Tool user’s password

1 Stop the Siebel Management Server.

  For details, see *Siebel System Administration Guide*.

2 Navigate to the *MGTINSTALL_ROOT*\tomcat\conf directory, where *MGTINSTALL_ROOT* is the installation directory of the Siebel Management Server.

3 Open the tomcat-users.xml file and change the value of the password parameter for the Siebel Diagnostic Tool user whose password you want to change.

  The following example shows a Siebel Diagnostic Tool user, SiebelDiagTool, with an existing password, SiebDiagToolPassword:

```
user username="SiebelDiagTool" password="SiebDiagToolPassword"
roles="configurator" /
```

  In the above example, you replace SiebDiagToolPassword with the new password.

4 Save and close the tomcat-users.xml file.

5 Restart the Siebel Management Server.

  For details, see *Siebel System Administration Guide*.

  The Siebel Diagnostic Tool user whose password you changed in this procedure must now log in to the Siebel Diagnostic Tool using the new password.

Changing a Siebel User Account Password in the Siebel Management Framework

This topic describes additional steps that you must take if you change the password of a Siebel user account that accesses the Siebel Management Server or the Siebel Management Agent. These entities authenticate the Siebel user account when a Siebel user attempts to execute the Siebel Management Server or Siebel Management Agent.

If you change the password of a Siebel user as described elsewhere in *Siebel Bookshelf*, or if you change the Siebel administrator password as described in "Changing System Administrator Passwords on Microsoft Windows" on page 34 or "Changing the Siebel Administrator Password on UNIX" on page 36, then this password change takes effect in the Siebel Enterprise only. In order for the Siebel Management Framework to authenticate the new password, you must replicate the password change in the Siebel Management Framework.

The following procedures describe how you replicate the password change in the Siebel Management Framework. Use the appropriate procedure:

- If, during the configuration of the Siebel Management Server or Siebel Management Agent, you selected RC2 encryption to encrypt the Siebel user's password, use the procedure that describes how to change RC2-encrypted passwords.
- If you did not select RC2 encryption to encrypt the Siebel user's password during configuration of the Siebel Management Server or Siebel Management Agent, use the procedure that describes how to change non-encrypted passwords.

  NOTE: If you did not select RC2 encryption, the password that you specified during configuration of the Siebel Management Server or Siebel Management Agent was encoded using Base64 Content-Transfer-Encoding. For this reason, you must convert the plaintext of the new password to Base64 Content-Transfer-Encoding before you change it in the Siebel Management Framework.

See the *Siebel Installation Guide* for the operating system you are using for information about installing and configuring the Siebel Management Server or Siebel Management Agent.

To change an RC2-encrypted password in the Siebel Management Framework

1. Change the Siebel user account password. If you are changing the Siebel administrator password, see "Changing System Administrator Passwords on Microsoft Windows" on page 34 or "Changing the Siebel Administrator Password on UNIX" on page 36.
2. Stop the Siebel Management Server or Siebel Management Agent for which you are going to change the password.
3. Open a command window and execute the following command:

   ```
   JRE_HOME\bin\java -cp MGTINSTALL_ROOT\lib\siebelmgr.jar
   com.siebel.management.util.Decoder MGTINSTALL_ROOT\security rc2_key_file_name
   new_password -write-properties
   ```

   where:

   - *JRE_HOME* is the location of the JRE home directory
   - *MGTINSTALL_ROOT* is the installation directory for the Siebel Management Server or the Siebel Management Agent
   - *rc2_key_file_name* is the location of the RC2 key file

- *new_password* is the new password that you specified in Step 1

This updates the Siebel user account password that is used to access the Siebel Management Server or the Siebel Management Agent.

NOTE: Siebel Management Server runs only on Microsoft Windows but Siebel Management Agent can run on either Microsoft Windows or supported UNIX operating systems.

4 Repeat Step 2 and Step 3 for all installed instances of the Siebel Management Server or Siebel Management Agents.

5 Restart the Siebel Management Server or Siebel Management Agent.

For details, see *Siebel System Administration Guide*.

To change a non-encrypted password in the Siebel Management Framework

1 Change the Siebel user account password. If you are changing the Siebel administrator password, see "Changing System Administrator Passwords on Microsoft Windows" on page 34 or "Changing the Siebel Administrator Password on UNIX" on page 36.

2 Stop the Siebel Management Server or Siebel Management Agent for which you are going to change the password.

3 Open a command window and execute the following command:

```
JRE_HOME\bin\java -cp MGTINSTALL_ROOT\lib\siebelmgr.jar
com.siebel.management.util.Base64 newPassword
```

where:

- *JRE_HOME* is the location of the JRE home directory
- *MGTINSTALL_ROOT* is the installation directory for the Siebel Management Server or the Siebel Management Agent
- *newPassword* is the plaintext of the password that you created in Step 1.

This command converts the plaintext of the password to Base64 encoding.

NOTE: Siebel Management Server runs only on Microsoft Windows but Siebel Management Agent can run on either Microsoft Windows or supported UNIX operating systems.

4 Save the output of Step 3.

5 Stop the Siebel Management Server or Siebel Management Agent for which you are going to change the password.

For details, see *Siebel System Administration Guide*.

6 Navigate to the *MGTINSTALL_ROOT*\security directory where *MGTINSTALL_ROOT* is the installation directory of the Siebel Management Server or Siebel Management Agent.

7 Open the security.properties file and change the value of the com.siebel.management.security.password parameter to the value that you saved in Step 4.

8 Save and close security.properties file.

9. Repeat Step 5 to Step 8 for all installed instances of the Siebel Management Server or Siebel Management Agents.

10. Restart the Siebel Management Server or Siebel Management Agent.

    For details, see *Siebel System Administration Guide*.

Changing the Siebel Enterprise Security Token

The Siebel Enterprise security token is a value that you specify when you create a Siebel Web Server Extension (SWSE) logical profile. This token serves as a password that authenticates the following:

- A Siebel administrator refreshing application images (and other static content) from the Siebel Server to the Web server without requiring a restart of the Web server.

- Requests from Siebel Management Agents during their installation.

After you apply the SWSE logical profile, the parameter SiebEntSecToken in the application sections of the eapps.cfg file stores the value you specified for the Siebel Enterprise security token. The SiebEntSecToken parameter stores the value in encrypted form if password encryption for the eapps.cfg file is in effect (EncryptedPassword = TRUE). If you manually edit the eapps.cfg file, then you must use the encryptstring utility to generate an encrypted version of the new password to store in the file. Enter the output from the encryptstring utility.

If EncryptedPassword = FALSE, passwords are not stored as encrypted values. In this case, passwords must not be entered as encrypted values.

For more information about password encryption for the eapps.cfg file, and about the encryptstring utility, see "Managing Encrypted Passwords in the eapps.cfg File" on page 45.

NOTE: The SiebEntSecToken parameter provides Web server security, but does not correspond to a database account and is stored only in the eapps.cfg file.

For more information about managing Web images and other files for your Siebel Business Applications, see *Configuring Siebel Business Applications*.

To edit the eapps.cfg file to configure the Siebel Enterprise security token

1. The Web public root directory (the location of Web file caching for Siebel Business Applications) is set automatically when you apply the SWSE logical profile by running the Siebel Configuration Wizard for SWSE. Or, you can specify it by adding a line in each application section of the eapps.cfg file. For example, to specify the Web public root directory for Siebel eService (for a Web server on a Windows computer), add a parameter like this:

```
[/eservice_enu]
WebPublicRootDir = SWEAPP_ROOT\public\LANGUAGE
```

where *SWEAPP_ROOT* is the SWSE installation directory, such as `D:\sba80\SWEApp`, and *LANGUAGE* is the application language, such as ENU for U.S. English. Files will be copied to this location from all of the language-specific subdirectories of the directory *SIEBSRVR_ROOT*`\webmaster`, where *SIEBSRVR_ROOT* is the Siebel Server installation directory.

The directory structure on the Web server is parallel to that on the Siebel Server, except that the files are moved up from their original language-specific subdirectories. For example, files would be copied from *SIEBSRVR_ROOT*`\webmaster\files\enu` and *SIEBSRVR_ROOT*`\webmaster\images\enu` to *SWEAPP_ROOT*`\public\enu\files` and *SWEAPP_ROOT*`\public\enu\images`.

It is recommended to set `WebPublicRootDir` the same for all applications for a given language, in order to conserve disk resources on the Web server.

2 The Siebel Enterprise security token can be set by applying a SWSE logical profile using the Siebel Configuration Wizard for SWSE. Or, you can specify it by adding a line in each application section of the eapps.cfg file. For example, to specify a Siebel Enterprise token for Siebel eService, add a parameter like this:

```
[/eservice_enu]
SiebEntSecToken = abcdef
```

Typically, password encryption is in effect for the eapps.cfg file, as described in "Managing Encrypted Passwords in the eapps.cfg File" on page 45. If encryption is in effect and if you edit the file manually, then you must use the encryptstring utility to generate an encrypted version of the new password to store in the file.

Siebel administrators can then use this password to update cached static files from a browser, without restarting the Web server. For example, specify a URL like the following. (Specify the password in clear text form, whether or not encryption is used.)

```
http://hostname/eservice/start.swe?SWECmd=UpdateWebImages&SWEPassword=abcdef
```

Managing Encrypted Passwords in the eapps.cfg File

The RC2 algorithm encrypts passwords stored in the eapps.cfg file with a 56-bit encryption key. Passwords are written to the file in encrypted form when you configure the SWSE. (Optionally, you can turn off encryption and use clear-text passwords in this file.)

Values for the AnonPassword parameter are subject to encryption, whether this parameter appears only in the [defaults] section or also in the application-specific sections of the eapps.cfg file. The values for the SiebEntSecToken (Siebel Enterprise security token) and TrustToken parameters are also encrypted.

For more information about the SiebEntSecToken parameter, see "Changing the Siebel Enterprise Security Token" on page 44.

After you initially configured SWSE, encryption behavior is subject to the status of the EncryptedPassword parameter. This parameter is added to the eapps.cfg file, with a value of TRUE, when you configure the SWSE.

The status of the EncryptedPassword parameter and the encryption status of the passwords themselves must match. That is, if the parameter is TRUE, then the password parameter values must be encrypted, and, if the parameter is FALSE, the passwords must not be encrypted.

If the EncryptedPassword parameter does not exist in the eapps.cfg file, the default behavior is the same as if EncryptedPassword = FALSE. It is strongly recommended to keep EncryptedPassword = TRUE in eapps.cfg.

When an anonymous user password is used (during application login or anonymous browsing sessions), the encrypted password is decrypted and compared to the value stored for the database account (specified using the AnonUserName parameter).

The account and password are created using the standard Siebel database scripts, and must already exist in the Siebel database when you configure the SWSE. If you change the password for this account after setting up your system, you must update the password stored in the eapps.cfg file.

For more information about parameters in the eapps.cfg file, see “Parameters in the eapps.cfg File” on page 335.

Encrypting Passwords Using the encryptstring Utility

Using the Siebel Configuration Wizard to change an anonymous user password, or the Siebel Enterprise security token, automatically saves the password in encrypted form. If, however, you have to manually add an encrypted value for the corresponding parameters in the eapps.cfg file (AnonPassword or SiebEntSecToken), use the encryptstring.exe utility to generate the encrypted value to provide as the parameter value.

NOTE: If you want to use different database accounts for the anonymous user for different applications, you must manually update the eapps.cfg file.

The encryptstring utility is installed with both the Siebel Server and the SWSE. It is located in the *SIEBSRVR_ROOT*\bin and *SWEAPP_ROOT*\bin directories, where *SIEBSRVR_ROOT* is the Siebel Server installation directory, and *SWEAPP_ROOT* is the SWSE installation directory.

To generate as output an encrypted value for a password, enter the following command:

```
encryptstring clear_text_password
```

For example, if you want to store the encrypted version of GUESTCST, a password you might initially specify for the anonymous user account, you would enter:

```
encryptstring GUESTCST
```

The command output in this case might be something like fhYt8T9N4e8se4X3VavTjQXwAEqm. (The specific value that is output changes each time you use the encryptstring utility.)

NOTE: Although the anonymous user has limited privileges, it is generally recommended to use more secure passwords for production deployments of your Siebel Business Applications. The topic "Changing Passwords" on page 33 describes changing passwords for database accounts and also for corresponding values in parameters stored on the Siebel Gateway Name Server. For anonymous user accounts, changing passwords involves changing passwords for database accounts and changing passwords in the eapps.cfg file.

About Password Encryption

The encryptor that you use in your Siebel deployment writes encrypted passwords to the siebns.dat file. The passwords are encrypted using the RC4 algorithm with a 56-bit encryption key. If you install the Siebel Strong Encryption Pack, you can increase the encryption key length used to encrypt passwords to 128-bits.

For more information about the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97.

The encryptor generates the encrypted password using an encryption key that is unique to each parameter. The encryption key itself is generated based on repository information.

4 Physical Deployment and Auditing

This chapter describes security issues related to physical deployment of Siebel components on the network. It includes the following topics:

For more information on some of these topics, see *Siebel Deployment Planning Guide* and the *Siebel Installation Guide* for the operating system you are using.

About the Siebel Network

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

Figure 3 on page 50 shows the basic components included in Oracle's Siebel Business Applications network.

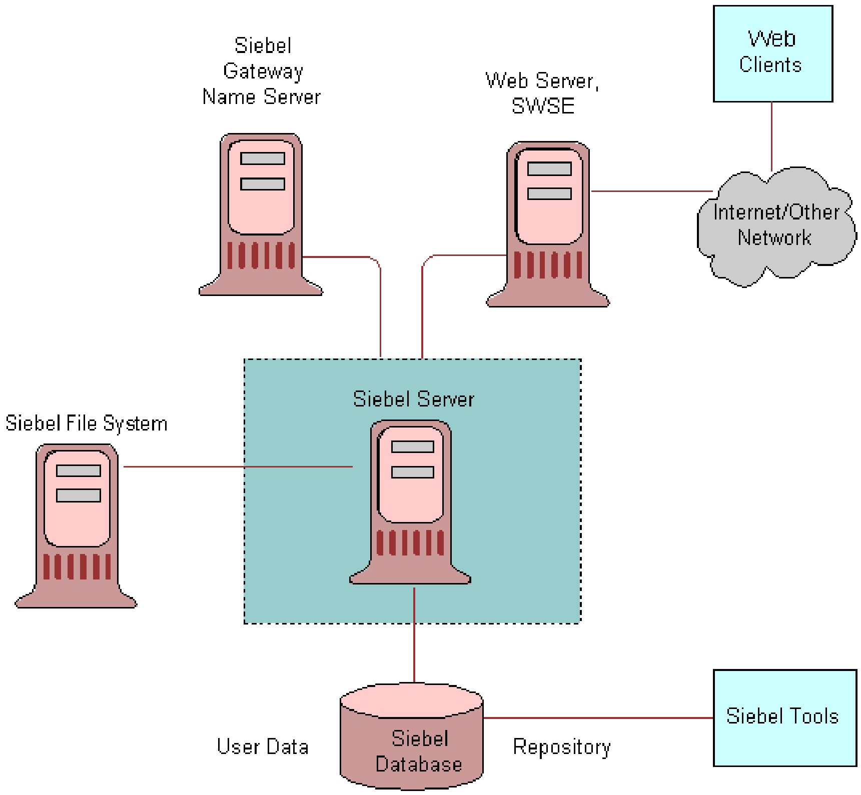


Figure 3. Siebel Network Components

Firewall and Proxy Server Support

A firewall separates a company's external Siebel Web Clients (those accessing applications over the Internet) 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 often include one or more of the following capabilities:

- **Proxy server.** A *proxy server* is a Web server that acts as an intermediary to prevent direct connection to your local corporate network from the Internet. It shields internal IP addresses from the Internet. Siebel Business Applications support both forward and reverse proxy servers within a deployment.

- **Reverse proxy server.** A reverse proxy server acts as an intermediary to prevent direct connections from clients to Web servers. A reverse proxy server shields internal IP addresses from users by rewriting IP addresses of the Web servers so that they are not revealed to the user. Additionally, the reverse proxy server can cache data closer to end users, thereby improving performance.

  You do not have to perform any configuration within your Siebel environment to enable reverse proxy servers.

  Customer applications, which use standard interactivity, commonly are deployed with reverse proxy servers. Employee applications, which use high interactivity, can also be deployed with reverse proxy servers. If you deploy applications that use high interactivity with a reverse proxy server or a Web server load balancer, note the following considerations:

  - Siebel Business Applications do not support the translation of port numbers or protocol switching. An example of protocol switching is changing from HTTP to HTTPS.

    Protocol switching from HTTPS to HTTP is supported if you have enabled the SSL acceleration feature for communications between Siebel Web clients and the Web server. For information on using SSL acceleration, see "Enabling SSL Acceleration for Web Server and Web Client Communications" on page 80.

  - Siebel Business Applications support rewriting of the host name and of the IP addresses of the Web servers.

    For example, you can rewrite the following URL:

    ```
    http ://ServerInternal/callcenter_enu/start.swe
    ```

    to:

    ```
    http ://ServerExternal/callcenter_enu/start.swe
    ```

    However, you cannot rewrite it to:

    ```
    http ://ServerExternal/portal1/start.swe
    ```

  - The reverse proxy server and Web server must run on the same port.

    Port switching from 443 to 80 is supported if you have enabled the SSL acceleration feature for communications between Siebel Web clients and the Web server. For information on using SSL acceleration, see "Enabling SSL Acceleration for Web Server and Web Client Communications" on page 80.

  - If you deploy SSL between the client and the reverse proxy server, then you must deploy SSL between the reverse proxy server and the Web server on which the Siebel Web Server Extension (SWSE) is installed. Similarly, if you deploy SSL between the reverse proxy server and the Web server, then you must deploy it between the client and the reverse proxy server.

    NOTE: If the SSL acceleration feature is enabled, you can deploy SSL between Siebel Web Clients and the reverse proxy server, but do not have to deploy SSL between the reverse proxy server and the Web server; you can use the HTTP protocol for communications between the reverse proxy server and the Web server. For information on enabling SSL acceleration, see "Enabling SSL Acceleration for Web Server and Web Client Communications" on page 80.

- **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).** Siebel Business Applications also support the use of Virtual Private Networks. 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 intranet resources (for example, email servers, file shares, and so on) which otherwise would not be sufficiently secured to be placed outside the firewall.

Recommended Placement for Firewalls

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

- **Internet.** Where external Siebel Web Clients reside.
- **Web server zone.** Where Siebel Web servers and Web server load balancers reside. The Siebel Web Server Extension (SWSE) is installed on the Web server computer. Sometimes called the DMZ (demilitarized zone), this zone is where the external network first interacts with the Siebel environment.

  To handle traffic between the external Siebel Web Clients and the Web server that contains the SWSE, installing a reverse proxy server is recommended. If you deploy a reverse proxy, locate it in the DMZ. The Web server and SWSE can then be moved behind a firewall into its own zone, or into the Siebel Server zone.
- **Siebel Server zone.** (This is sometimes called the application server zone.) Components that reside inside this zone include Siebel Servers, the Siebel Gateway Name Server, a third-party HTTP load balancer (if deployed) for Siebel Servers, and the authentication server (such as an LDAP or ADS directory server).
- **Data Server zone.** Where the Siebel database, Siebel File System, and Database Server reside. Typically, this is where the most critical corporate assets reside. Limit access to this zone to authorized system administrators and database administrators only.

Siebel network architecture allows you to install firewalls between each of these zones. For optimum performance, however, do not install a firewall between the Siebel Server zone and the Data Server zone. Figure 4 on page 53 shows the recommended placement for firewalls in Siebel networks.

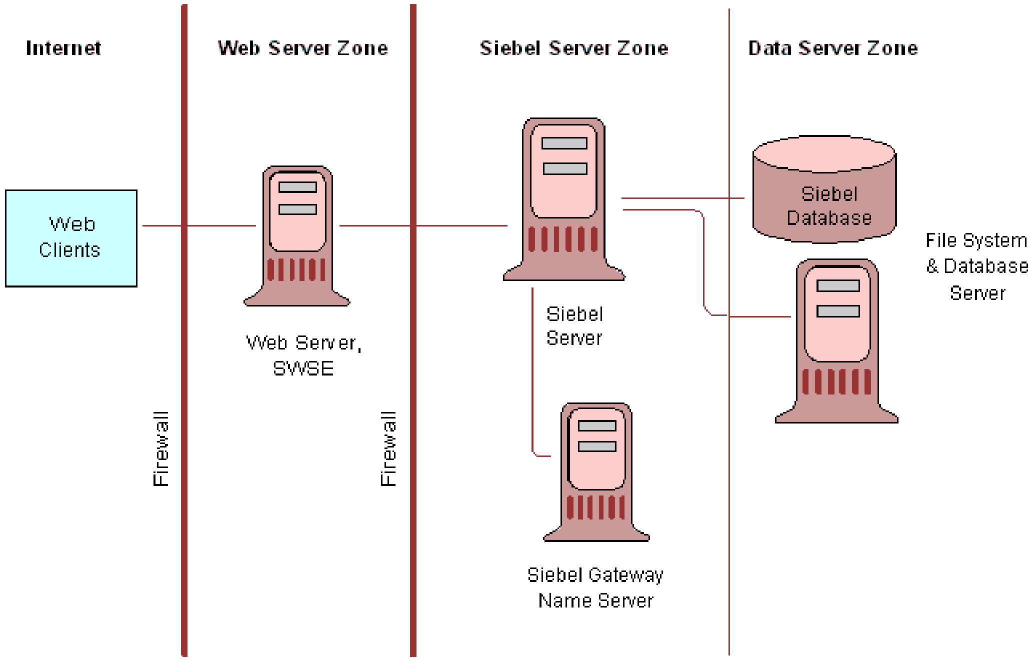


Figure 4. Firewalls in Siebel Networks

Deploying Siebel Business Applications Accessed Through a Firewall

When deploying Siebel Business Applications across a firewall, verify that your firewall and proxy servers support the HTTP 1.1 protocol. This protocol enables functionality such as inline data compression to improve performance for bandwidth-constrained environments, cookies, and other features.

If your firewall does not support HTTP 1.1, and you use HTTP 1.0 instead, lower performance will result. The following requirements apply if you do not use HTTP 1.1:

- Web server compression for SWSE must be disabled. In the eapps.cfg file, set the value of the DoCompression parameter to FALSE. (Use other settings where compression is known to be supported, or might be supported.) For more information, see *Siebel System Administration Guide*.
- Make sure that the firewall can handle cookie-wrapping or other proxy-specific features that enable forwarding of cookie. Or, reduce or remove the use of cookies in your Siebel Business Applications. For more information, see "About Using Cookies with Siebel Business Applications" on page 204.
- Make sure that your proxy server does not pass to the SWSE any header content that uses HTTP 1.1 protocol. The proxy must strip any header content that is not compliant with HTTP 1.0.

Role of Siebel Server Load Balancing in Network Security

You can load-balance your Siebel Servers, using either Siebel load balancing or a third-party HTTP load balancer.

A third-party load balancer typically can provide additional security features, such as limiting TCP port exposure to a single port for multiple Siebel Servers. 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 security features provided by most third-party load balancers include:

- **Denial of Service (DoS) Attack prevention.** In a DoS attack, a third-party HTTP load balancer helps handle the TCP connections. Incoming attacks can be caught at the load balancer before they ever reach the Siebel Server. A third-party HTTP load balancer typically has a built-in mechanism to stop DoS attacks at the point of entry.
- **Virtual IP (VIP) addressing.** A third-party HTTP load balancer uses VIP addressing to shield hackers from accessing Siebel Servers directly. Because a VIP is an IP alias, no physical addresses are ever exposed. Web servers in the DMZ communicate with the VIP only.
- **TCP handshake protection.** The TCP handshake is replayed from the third-party HTTP load balancer to the Siebel Server rather than directly from the Web server to the Siebel Server.

For information on configuring load balancing for your Siebel deployment, see *Siebel System Administration Guide* and the *Siebel Installation Guide* for the operating system you are using.

About Selecting Port Numbers

Network traffic going to Siebel Application Object Managers (AOMs) on Siebel Servers go through static, configurable TCP ports. Each Siebel Server listens on one TCP port only.

For more information on configuring ports for use with Siebel Business Applications, see *Siebel Deployment Planning Guide*. See also the *Siebel Installation Guide* for the operating system you are using.

If you use Siebel load balancing, the AOM listens on one TCP port on each Siebel Server for traffic from the Web Server to the Siebel Server. If you use a third-party HTTP load balancer, then you can also use a single VIP address and port for all such communications from the Web Server to the Siebel Server. You can also use multiple VIP addresses and ports, if different VIPs or ports are used for different applications.

By default, Siebel Server configuration assumes that each Web server communicates to one VIP address and port for all AOMs. You can change this manually, to support multiple VIP addresses or ports.

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

- To secure communications between the Web browser and the Web server, using SSL, specify the HTTPS port (default is 443) when you install the SWSE.

- If you are setting up an LDAP or ADSI directory to use with Siebel Business Applications, use port 636 for secure transmission instead of port 389 for standard transmission.
- If you are using TCP/IP filtering, make sure that none of the ports you require, including the ServerMgr port, are blocked. If any required ports are blocked, the status of the Siebel Server will be Connect Failed. Note that the dynamic port numbers used range from 49152 to 65535.
- To allow users to access Siebel Business Applications across a firewall, make sure the Web server is accessible externally and that it can communicate with the Siebel Server using the SCBroker port (Siebel load balancing) or the virtual port of a third-party HTTP load balancer for TCP traffic. The default port used by SCBroker is 2321.
  - If you are using Siebel load balancing, make sure the Web server can access the SCBroker port on each Siebel Server.
  - If you are using a third-party HTTP load balancer, make sure the Web server can communicate with the VIP addresses and ports specified in the load balancer. Typically, the load balancer resides inside your corporate firewall, but as long as firewall access is set up properly, the customer can choose where the load balancer resides.

  Once firewall access is available, users can be authenticated using any Siebel-supported authentication method.
- Siebel Web Client users outside the firewall, such as authorized vendors (partners) or customers 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 must support HTTP over SSL, you can open port 443.
- The COM data control and the Java DataBean both communicate using SISNAPI. COM data control supports RSA and Microsoft Crypto, but not SSL. Java DataBean supports RSA, but not Microsoft Crypto or SSL.
- Port numbers for communications between the Siebel Server and the Siebel database are database-specific. Default TCP port numbers available for this purpose are as follows:
  - Oracle: 1521
  - Microsoft SQL Server: 1433
  - IBM DB2 UDB for Windows and UNIX: 5000 (Siebel default)
  - IBM DB2 UDB for z/OS: no default
- Port numbers for communications between the 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 User Datagram Protocol (UDP) port numbers are 137 and 138. UDP is a network protocol on the same level as TCP. Both TCP and UDP run on top of IP.
- Siebel Mobile Client users who have to connect to a Siebel Server in order to synchronize using Siebel Remote connect directly to the Siebel Server that serves as the Siebel Remote server. Telnet connections for mobile users can be configured in the Siebel environment. However, because of possible security risks, using such connections is not recommended.

Restricting Access to Siebel Components

This topic 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 Siebel Business Applications. You can use utilities that provide computer-level security by either enforcing computer passwords or encrypting the computer hard drive.

Most leading handheld devices have user-enabled passwords. Oracle works closely with a number of third-party partners who enable additional security layers on handheld devices, ranging from biometric authentication to wireless device management.

Database Server Access

Define stringent policies for database access both at the account login level and at the network visibility level. Only give authorized users (for example, approved database administrators (DBAs) system accounts (for root usage) and remote access to the server. On UNIX, it is recommended that you define netgroups to control access to database servers.

Siebel Server Access

To restrict privileges to Siebel Server processes, assign an operating system account specific to the Siebel Server. Assign this account access to only those files, processes, and executables required by Siebel Business Applications. Do not assign the Siebel Server account root administrator rights or privileges.

On UNIX systems, the .rhosts file allows remote, root administrators to access other computers. To provide the appropriate level of access and control to the Siebel Server, it is recommended that you minimize the usage of .rhosts files.

Siebel File System Access

The Siebel File System consists of a shared directory that is network-accessible to the Siebel Server and contains physical files used by Siebel Business Applications. The File System stores documents, images, and other types of file attachments.

Requests for access by Siebel user accounts are processed by Siebel Servers, which then use the File System Manager (FSM) server component to access the Siebel File System. FSM processes these requests by interacting with the File System directory. Siebel Remote components also access the File System directly. Other server components access the File System through FSM.

To prevent direct access to Siebel files from outside the Siebel Business Applications environment, restrict access rights to the Siebel File System directory to the Siebel Service owner. The Siebel Server processes and components use the Siebel Service owner account to operate.

A Siebel proprietary algorithm that compresses files in the File System also prevents direct access to files from outside the Siebel Business Applications environment in addition to providing a means of encrypting files. This algorithm is used at the Siebel Server level and appends the extension .saf to compressed files. These compressed files are decompressed before users or applications access them. Users access decompressed files through the Web client. You cannot disable use of this algorithm. For more information about the Siebel File System, see *Siebel System Administration Guide*.

NOTE: For Siebel Developer Web Client, access to the Siebel File System can be achieved either through FSM or through direct connection from each individual client. For more information, see *Siebel Installation Guide* for the operating system you are using.

Auditing for Data Continuity

To maintain data continuity and monitor activity on a Siebel site, Siebel Business Applications can maintain an audit trail of the following types of information:

- Date and time when a business component field has been changed
- Who made changes to a business component field
- What changes have been made to a business component field
- When a business component field was viewed or exported
- Who viewed or exported a business component field

NOTE: If Siebel Enterprise Application Integration (EAI) implements anonymous logins, Audit Trail cannot relate a change to the specific user who made the change.

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

By using Audit Trail, users can track which employee modified a certain field and what data has been changed. A call center user can track the status change of a service request or calculate the time it takes to solve it. For example, a user can activate the Audit Trail functionality on a status field in the Service Requests screen. An audit trail record is created for each status change, along with a time stamp and the ID of the user who made the change.

A more advanced use of Audit Trail involves a user who reconstructs records that existed at a certain point in time by doing complex queries. 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.

Audit Trail is applicable for every Siebel Web deployment and configuration option, including synchronization with Mobile Web Clients and replication to or from regional databases supported by Siebel Replication Manager. 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 configuring and using Audit Trail, see *Siebel Applications Administration Guide*.

Securing Siebel Reports Server

The Siebel Reports Server consists of the following components:

- Actuate iServer and Management Console for Siebel (Actuate iServer)
- Actuate Active Portal JSP and Reports View Adapter for Siebel (Actuate Active Portal)
- Actuate e.Report Designer Professional (optional)
- Actuate e.Report Designer (optional)

This topic describes how to secure communication between the Siebel Reports Server, the AOM, and the Siebel Web Client in the following topics:

- "Securing Communications Between the Siebel Web Client and Actuate Active Portal" on page 58
- "Securing Communications Between the AOM and Actuate iServer" on page 60

Note the following considerations when configuring Siebel Reports Server for security:

- Siebel Reports does not support the use of LDAP or ADSI for user authentication. Users must be synchronized between the Siebel Business Applications and Actuate in order for Siebel Reports to function correctly.
- Communication among Actuate components is outside the scope of the Siebel Business Applications environment. For more information, consult the Actuate product documentation in *Siebel Business Applications Third-Party Bookshelf*.

For information about deploying and installing the Siebel Reports Server in your Siebel environment, see *Siebel Deployment Planning Guide* and the *Siebel Installation Guide* for the operating system you are using. For information about Siebel Reports, see *Siebel Reports Administration Guide*.

Securing Communications Between the Siebel Web Client and Actuate Active Portal

You can use SSL to secure communication between the Siebel Web Client and the Actuate Active Portal. To make sure that communications occur between the Siebel Web Client and Actuate Active Portal using SSL, you must:

- Configure the Actuate HTTP Service for Active Portal to communicate over SSL. For information on how to configure SSL for the Actuate HTTP Service, see your Web server documentation.

  After you complete this task, note the port number that you configured for SSL communication on the Actuate HTTP Service (default port number = 8443). You require this number when you configure the Siebel application that communicates with the Actuate Active Portal.

- Configure Siebel Business Applications to communicate with Actuate Active Portal using SSL.

  The following procedure describes how to configure Siebel Business Applications to communicate with Actuate Active Portal using SSL.

CAUTION: If you enable SSL for communication between the Siebel Server and the Web server, and between the Siebel Web Client and the Web server, then you must enable SSL for communication between the Siebel Web Client and the Actuate Active Portal. If you do not, you cannot run Actuate reports.

To configure Siebel Business Applications to use SSL

1. Log in as an administrator.
2. Navigate to the Administration - Integration screen, then the WI Symbolic URL List view.
3. From the visibility filter, select Host Administration.
4. In the Virtual Name field, query for rshost.

   This query retrieves the record for the Siebel Reports Server.

5. In the Name field enter the host name of the Actuate Active Portal and the Actuate Active Portal port number.

   For example, enter sdc4500i076:8443 where sdc4500i076 equals the host name of the Actuate Active Portal and 8443 equals the Actuate Active Portal port number.

   The Actuate Active Portal port number is the number that you configured for SSL communication on the Actuate HTTP Service. For information on how to configure SSL for the Actuate HTTP Service, see your Web server documentation.

6. Step off the record to save changes.
7. From the visibility filter, select Symbolic URL Administration.
8. In the Name field, query for *Reports*. *Reports* is case sensitive.

   The query retrieves records for the symbolic URLs.

9. In the URL field of each record, change the protocol from http to https.

   For example, change

   ```
   http://rshost/acweb/newrequest/do_executereport.jsp
   ```

   to

   ```
   https://rshost/acweb/newrequest/do_executereport.jsp.
   ```

   NOTE: If you use symbolic URLs to specify how HTTP requests to external applications are to be constructed, it is recommended that you use SSL to ensure the communication is secure.

10. Log out of Siebel Business Applications.

Securing Communications Between the AOM and Actuate iServer

During report generation, Actuate iServer establishes a separate session to the AOM to obtain data for report generation. This communication can be encrypted by setting the desired encryption type (RSA or MSCRYTPO) for the Actuate Server Connect String parameter in the configuration file for the AOM. The following example specifies RSA as the encryption type to use:

```
Actuate Server Connect String = siebel.TCPIP.RSA.none://SiebelServerHost:SCBPort/
EnterpriseServerName/XXXObjMgr_language
```

For details on setting this parameter, see the postinstallation tasks described in the *Siebel Installation Guide* for the operating system you are using.

Using the Siebel Strong Encryption Pack with Siebel Reports Server

If you choose to encrypt communications between the AOM and the Actuate iServer, and if you have installed the Siebel Strong Encryption Pack (SSEP), you must perform the steps in the following procedure to enable the SSEP for the Siebel Reports Server. For information on the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97.

To use the Siebel Strong Encryption Pack with Siebel Reports Server

1. After installing the SSEP, copy one of the following SSEP library files from the Siebel Server directory to the Reports Server installation directory (for example, on Windows the default directory is `sba_thirdparty_800\Actuate8\Server`):

   - sslcrsaxxx.dll file (Windows)
   - libsslcrsaxxx.so file (UNIX)

2. Restart all Actuate process services.

   For information on starting Actuate services, see *Siebel Reports Administration Guide*.

3. Resynchronize accounts for Siebel report users.

   For information on this task, see *Siebel Reports Administration Guide*.

Securing Siebel Document Server

This topic describes issues in securing communication between the Siebel Document Server and the Siebel Server.

For more information about Siebel Document Server, see *Siebel Correspondence, Proposals, and Presentations Guide*.

- All document templates come in through the Siebel Server. As such, the Siebel Server controls security and represents the only client or user that interacts directly with the Siebel Document Server. Restrict access to the file system and restrict execute permissions on the Siebel Document Server to the user that authenticates as the Siebel Server service.

- Microsoft provides some standard utilities in the Resource kit to lock down security on a generic Microsoft Windows computer. It is recommended that tools such as C2.exe be implemented to secure such an environment. These tools are readily available from Microsoft.
- Microsoft Word does support macro security options. Set macro security to high so that untrusted macros cannot be executed by the document server. This should not be an issue because macros are not required in proposals.
- Make sure that templates used by the Siebel Document Server or by end users are secured, and that there is a virus policy in place for any computer that supplies templates to the Siebel Document Server.

5 Communications and Data Encryption

This chapter provides an overview of communications paths between Siebel Enterprise components and of how to configure components for secure communications. It also describes encryption technologies available for transmitting and storing Siebel Business Applications data and describes issues applicable to Unicode environments. It includes the following topics:

Types of Encryption

Encryption is a method of encoding data for security purposes. Siebel Business Applications support industry standards for secure Web communications and encryption of sensitive data such as passwords.

To facilitate compliance with U.S. export restrictions on encryption technology, Siebel Business Applications limit the encryption key length to 56-bit in its products. Customers who want to use encryption keys longer than 56-bit for transport layer encryption and data encryption can do so by using the Siebel Strong Encryption Pack. For more information, see "About the Siebel Strong Encryption Pack" on page 97.

To make sure that information remains private, Siebel Business Applications support the use of the following encryption technologies for transmitting and storing data:

- **SSL encryption for Web client connections.** For data security over the Internet, Siebel Business Applications use the Secure Sockets Layer, version 3.0 (SSL) capabilities of supported Web servers to secure transmission of data between the Web browser and the Web server.

  Siebel Business Applications can be configured to run completely under HTTPS, have specific pages run under HTTPS (for standard interactivity only), or simply handle login requests under HTTPS. For more information, see "Configuring a Siebel Web Client to Use SSL" on page 199 and "Login Security Features" on page 200.

- **Encryption for SISNAPI connections (SSL, Microsoft Crypto, or RSA).** For communications between Siebel components, Siebel administrators can enable encryption for SISNAPI (Siebel Internet Session API). 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 Secure Sockets Layer, version 3.0 (SSL) or on Microsoft Crypto API or RSA algorithms. SSL and RSA are supported across multiple operating systems. By default, SISNAPI encryption based on SSL uses the DES algorithm with a 56-bit key that performs both encryption and decryption. To upgrade to the AES algorithm with 256-bit encryption keys, you have to install the Siebel Strong Encryption Pack. For more information on the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97.

  SSL also supports certificate authentication between the Web server and the Siebel Server, or between Siebel Servers.

- **SSL encryption for connection to LDAP or ADSI directories.** Secure Sockets Layer (SSL) can be used for connection to certified LDAP or ADSI directories.

- **SSL encryption for connections to email servers.** SSL encryption is supported for connections to email servers, using Siebel Communications Server components. For more information, see *Siebel Communications Server Administration Guide*.

- **AES and RC2 database encryption.** Siebel Business Applications allow customers to encrypt sensitive information stored in the Siebel database (for example, credit card numbers, Social Security numbers, birth dates, and so on) so that it cannot be viewed without access to Siebel Business Applications.

  Customers can configure Siebel Business Applications to encrypt a column's data before it is written to the database and decrypt the same data when it is retrieved. This encryption prevents attempts to view sensitive data directly from the database.

  Sensitive data can be encrypted by using AES (Advanced Encryption Standard) or RC2 encryption, at various key lengths. Encryption can be enabled using Siebel Tools. For more information, see "About Data Encryption" on page 83.

- **RC4 encryption**. Siebel Business Applications use RC4 encryption to encrypt passwords stored in the siebns.dat file and to encrypt the Auto-Login Credential Cookie. The siebns.dat file stores information required by the Siebel Gateway Name Server. For more information about encrypted passwords in the siebns.dat file, see "About Password Encryption" on page 47. For more information about the Auto-Login Credential Cookie, see "Auto-Login Credential Cookie" on page 207.
- **RSA SHA-1 password hashing.** Siebel administrators can enable password hashing. Hashing uses a one-way hashing algorithm. The default password hashing method is RSA SHA-1. (The previous mangle algorithm is still available for existing customers.)

  Password hashing invalidates the password to unauthorized external applications and prevents direct SQL access to the data by anything other than Siebel Business Applications. For more information, see "About Password Hashing" on page 157.

This chapter does not describe how to encrypt communications between the Siebel Server and the Database Server because this will depend on the encryption methods supported by your RDBMS vendor. For information on how to configure communications encryption between the Siebel Server and your Database Server, contact your third-party RDBMS vendor.

Figure 5 on page 66 shows some of the types of encryption available in a Siebel Business Applications environment.

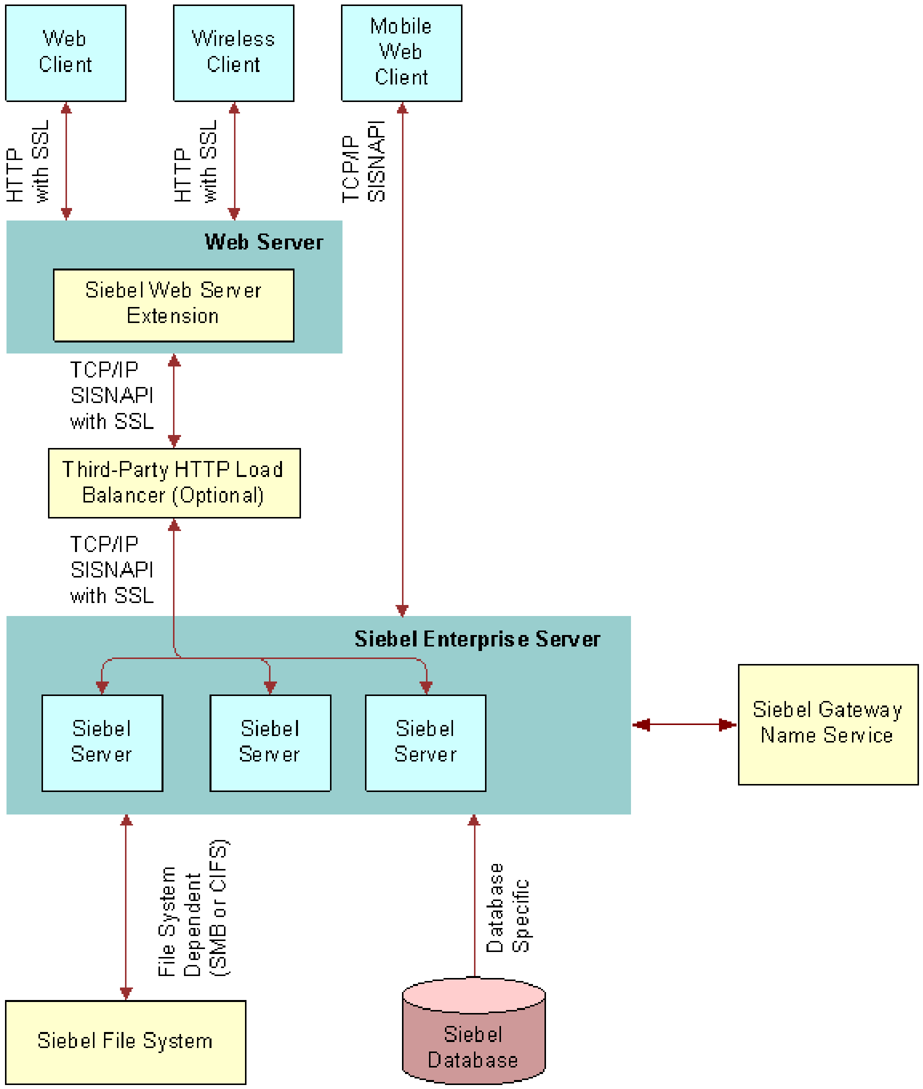


Figure 5. Communications Encryption in a Siebel Business Applications Environment

Process of Configuring Secure Communications

This topic describes how to set up encryption for communication between components in the Siebel environment. Encryption can be configured for data traffic between the Web server, Siebel Server, and Siebel Web Client.

To configure secure communications in your Siebel environment, perform the following tasks, as appropriate for your environment:

- "Installing Certificate Files" on page 69
- "Configuring SSL Mutual Authentication" on page 72
- "Configuring SSL Encryption for the Siebel Enterprise or a Siebel Server" on page 75
- "Configuring SSL Encryption for SWSE" on page 78
- Review "About Configuring SSL for the Siebel Management Framework" on page 80
- "Enabling SSL Acceleration for Web Server and Web Client Communications" on page 80
- Review "About Configuring Encryption for Web Clients" on page 81
- "Configuring Encryption for Mobile Web Client Synchronization" on page 82
- "Configuring a Siebel Web Client to Use SSL" on page 199

The encryption options described in these topics are not used to encrypt data in the database; this is described in "About Data Encryption" on page 83. Also, these encryption options are not used for communications with the database—for this type of encryption, check with your database vendor.

About Certificates and Key Files Used for SSL Authentication

When you configure SSL authentication for a Siebel Enterprise, Siebel Server, or SWSE, you specify parameter values that indicate the names of certificate files, certificate authority files, and private key files on the computers that host these components. The certificate files you use for this purpose can be issued by and obtained from third-party certificate authorities. Certificate authority files identify the third-party certificate authority who issued the certificate.

Certificate files must adhere to the following requirements:

- Use a supported certificate file format:
  - On Microsoft Windows environments, certificate authority files can use either ASN (Abstract Syntax Notation) or PEM (Privacy Enhanced Mail) format.

    The ASN.1 format is also referred to as the Distinguished Encoding Rules (DER) format. Rename certificate files in DER format to have the file extension .asn.
  - On UNIX environments, certificate authority files must use the PEM (Base 64 encoded X.509) format. Certificate files in ASN format cannot be used in UNIX environments.
  - Private key files must use the PEM format.

  The certificate file must use the file extension that corresponds to the certificate file format in use: .pem for the PEM format, and .asn for the ASN format.

  NOTE: You can convert PEM-based certificate files to the ASN-based format.
- Certificate files on each computer must be unique and belong to that computer if PeerAuth is set to TRUE on the remote computer.

- If an intermediate certification authority is used, both the intermediate and the root certificate authority certificates must be in the same file. You specify the name of this file for the CACertFileName parameter when you configure SSL for communication between Siebel components.

Certificate files and private key files are typically installed on each computer that hosts a component or module for which you configure SSL, such as a Siebel Server or SWSE. You do not have to authenticate or encrypt communications between components on the same computer. For information on installing certificate files, see "Installing Certificate Files" on page 69.

About Supported Values for SSL Certificate Encryption Keys

A certificate authority certifies ownership of the public and private key pairs that are used to encrypt and decrypt SSL communications. Messages are encrypted with the public key and decrypted with the private key. The certificate key size refers to the size, in bits, of the encryption key provided with the certificate.

In general, for SSL authentication for a Siebel Enterprise, Siebel Server, or SWSE, Siebel Business Applications support certificates that use an encryption key size of 1024 bits. If you require a higher encryption key size, you must install the Siebel Strong Encryption Pack. However, the size of the certificate key supported depends on the components for which you are configuring SSL communications.

Table 5 shows the certificate key sizes supported for SSL communications between different components in a Siebel Business Applications deployment.

Table 5. Encryption Key Sizes Supported For SSL Certificates

SSL Communication Type	Supported Key Size
SSL communications using SISNAPI. Communications between the Siebel Server and the Web server (SWSE), and between Siebel Servers.	1024-bit certificate keys only are supported if you do not install the Siebel Strong Encryption Pack (SSEP). To use certificate key sizes larger than 1024 bits, install the Siebel Strong Encryption Pack and follow the instructions in "Increasing the Certificate Key Sizes Supported For SISNAPI Communications" on page 69.
SSL communications between Web clients and the Web server.	The acceptable SSL protocols and key sizes are determined by the underlying operating system and Web server software. In most cases, these systems support larger private key sizes.
SSL communications between dedicated clients (including Siebel Tools) and components in the Siebel environment.	1024-bit certificate keys only are supported.
SSL communications between the Siebel Server and the Siebel database.	The key size supported is determined by the third-party database used and database client software.

Table 5. Encryption Key Sizes Supported For SSL Certificates

SSL Communication Type	Supported Key Size
SSL communications between Siebel security adapters and external directory servers.	These connections can support larger bit sizes for SSL certificate keys.
SSL communications for Web services.	1024-bit certificate keys only are supported.

Increasing the Certificate Key Sizes Supported For SISNAPI Communications

In general, for SSL authentication for Siebel Enterprise, Siebel Server, or SWSE communications, Siebel Business Applications support certificates that use an encryption key size of 1024 bits. If you want to use certificates with encryption key sizes larger than 1024 bits, perform the steps in the following procedure.

To increase the certificate key sizes supported for SISNAPI communications

1. Install the Siebel Strong Encryption Pack (SSEP) on the Siebel Server and the Web server.

   For information on installing the SSEP, see "Installing the Siebel Strong Encryption Pack" on page 98.

2. Replace the sslcnapi file on the Siebel Server and the Web server with the sslcnapi128 file that is included with the Siebel Strong Encryption Pack. The sslcnapi files are located as follows:

   - Web server
     - Windows: `\SWEAPP\bin\sslcnapi.dll`
     - UNIX: `/sweapp/bin/sslcnapi.so`
   - Siebel Server
     - Windows: `\siebsrvr\bin\sslcnapi.dll`
     - UNIX: `/siebsrvr/lib/libsslcnapi.so`

If your version of the Siebel Strong Encryption Pack does not include the sslcnapi128 file, create a service request (SR) on My Oracle Support. Alternatively, you can phone Oracle Global Customer Support directly to create a service request or get a status update on your current SR. Support phone numbers are listed on My Oracle Support.

Installing Certificate Files

This topic describes how to install certificate files on Microsoft Windows and on Unix. For information on using certificate files and SSL authentication, see "About Certificates and Key Files Used for SSL Authentication" on page 67.

This task is a step in "Process of Configuring Secure Communications" on page 66.

About Installing Certificate Files on Windows

You import certificate authority files and certificate files using Microsoft Internet Explorer's Certificate Import Wizard. For information on how to use this wizard, see the Microsoft documentation.

About Installing Certificate Files on UNIX

If you are using a UNIX operating system, refer to the following for information on obtaining certificate authority files and certificate files:

- **SSL encryption for Web client connections to the Web server.** Refer to your Web server documentation for information on encrypting data transmission and on certificate requirements.
- **Encryption for SISNAPI connections.** Obtain the required certificate files and locate them on a local volume; they do not have to be installed.
- **SSL encryption for connection to LDAP or ADSI directories.** The LDAP security adapter uses the IBM GSKit to handle the installation of certificates. For information on the IBM GSKit, see "Generating a CMS Key Database Using IBM GSKit" on page 131.
- **Communications encryption between the Siebel Server and the Database Server.** Refer to your third-party RDBMS vendor for information on configuring communications encryption and certificate requirements.

Installing Certificate Files on UNIX for Client Authentication

When using the EAI HTTP Transport business service with the SSL protocol, you might have to install certificate files, for example, if you want to enable client authentication. If you are using a UNIX-based operating system, Siebel Business Applications provide a utility (mwcontrol utility) that enables you to install on your Siebel Server and SWSE computers the certificate authority and certificate files required when using EAI HTTP Transport with SSL. For information on client authentication, see "Configuring SSL Mutual Authentication" on page 72.

The mwcontrol utility invokes a wizard that is similar to Microsoft Internet Explorer's Certificate Import Wizard. The following procedure describes how to use the mwcontrol utility to install certificate files. Execute the mwcontrol utility on each Siebel Server and SWSE computer where you want to install client authentication certificate files.

NOTE: When you use the mwcontrol utility to install a certificate file, the certificate file must be located on a local volume. You cannot use the mwcontrol utility to install certificate files that are located on a network-attached storage (NAS) device or other remote volume.

To invoke the mwcontrol utility and install certificate files

1. Depending on the type of UNIX operating system you use, enter the following commands:
   - For Bourne shell or Korn shell:

     ```
     . ./siebenv.sh
     ```

   - For C shell:

     ```
     source siebenv.csh
     ```

2 Set your DISPLAY environment variable to the IP address of the computer that hosts the mwcontrol utility:

- For Bourne shell or Korn shell:

  ```
  export DISPLAY=ipaddress of the computer that hosts the mwcontrol utility:0.0
  ```

- For C shell:

  ```
  setenv DISPLAY ipaddress of the computer that hosts the mwcontrol utility:0.0
  ```

If you are using an X-Windows client, *00* is the connection identifier.

3 To invoke the mwcontrol utility, execute the following command:

```
mwcontrol $SIEBSRVR_ROOT/mw/lib/inetcpl.cpl
```

where:

$SIEBSRVR_ROOT is the Siebel Server installation directory.

Alternatively, if you are running this procedure on your SWSE computer, replace *$SIEBSRVR_ROOT* with the location of the SWSE installation directory.

The wizard appears.

4 Select the Content tab, then click the Certificates button.

The Certificate Manager appears.

5 Select the tab that corresponds to the type of certificate you want to install.

For example to install a certifying authority certificate, select Trusted Root Certification Authorities tab.

6 Click Import to display the Certificate Manager Import Wizard, then click Next to navigate to the location where you stored the certificate file you want to install.

7 Select the certificate, and click Next.

8 Select the check box, Automatically select the certificate store based on the type of certificate, then click Next.

9 Click Next, then Finish to complete the installation, and terminate the execution of the mwcontrol utility.

Note the following points about your application's configuration file before you modify it in Step 10:

- The configuration files for a client are stored in the client's bin\LANGUAGE directory, where *LANGUAGE* represents an installed language pack, such as ENU for U.S. English.
- When synchronization is performed within Siebel Business Applications (from the File menu, select the Synchronize Database option), configuration is read from the configuration file associated with the application (for example, siebel.cfg for Siebel Sales).

  For more information about working with the Siebel Business Applications configuration files, see *Siebel System Administration Guide*.

10 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 element in the DockConnString parameter. This element indicates the type of encryption used during synchronization.

   An example of a DockConnString parameter value is as follows:

   ```
   APPSRV:TCPIP:40400:SMI:RSA
   ```

11 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, use one of the following:

   - `APPSRV:TCPIP:40400:DOCK:RSA`
   - `APPSRV::RSA`

12 Save your changes and exit the file.

   For more information about editing configuration files for Siebel Remote and Mobile Web Clients, see *Siebel Remote and Replication Manager Administration Guide* and *Siebel System Administration Guide*.

13 Restart the Siebel Server or SWSE computer on which you installed the certificate file.

For additional information on certificate files, see "About Certificates and Key Files Used for SSL Authentication" on page 67.

Configuring SSL Mutual Authentication

Mutual authentication is a process in which a connection between two parties is established only after each party has authenticated the other. In SSL mutual authentication, the client is authenticated to the server and the server is authenticated to the client during the SSL handshake, using digital certificates issued by certificate authorities.

Siebel Business Applications support server authentication and, in the current release, client authentication is also supported for SSL-based communications using the EAI HTTP Transport business service, and for workflows or outbound Web service calls that call the EAI HTTP Transport business service.

If you choose to enable client authentication, the Siebel Server presents a client certificate to an external Web server by supplying values for the HTTPCertSerialNo and HTTPCertAuthority EAI HTTP Transport parameters.

This task is a step in "Process of Configuring Secure Communications" on page 66.

The following procedure describes how to configure client authentication using the EAI HTTP Transport business service.

To configure client authentication using EAI HTTP Transport

1. Obtain the following files and install them on the Siebel Server:

   - A certificate authority file
   - A client certificate file

     Client certificate files must be in PKCS#12 format.

   For information on installing certificate files, see "About Installing Certificate Files on Windows" on page 70 and "Installing Certificate Files on UNIX for Client Authentication" on page 70.

2. Configure the Web server for client authentication.

   For information on configuring client authentication on the Web server, see your Web server vendor documentation.

3. Provide client authentication information by specifying values for the following EAI HTTP Transport parameters:

   - **HTTPCertSerialNo.** Specify the client certificate serial number. This is a hexadecimal string which cannot contain spaces.
   - **HTTPCertAuthority.** Specify the name of the authority that issued the client certificate. The issuing authority name must be in FQDN format and is case sensitive.

   The certificate authority and serial number details are displayed on the certificate, which you can view using Internet Explorer (Windows) or the mwcontrol utility (UNIX).

   The EAI HTTP Transport business service can be called directly or indirectly.

   - If the EAI HTTP Transport business service is invoked directly by an eScript script or workflow, you can specify the HTTPCertSerialNo and HTTPCertAuthority parameters using the Set Property method of the business service call. For additional information, see *Transports and Interfaces: Siebel Enterprise Application Integration*.
   - If the EAI HTTP Transport business service is invoked indirectly by an outbound Web service, you can specify the HTTPCertSerialNo and HTTPCertAuthority parameters as input arguments for the outbound Web Service Dispatcher. For additional information, see *Integration Platform Technologies: Siebel Enterprise Application Integration*.

Using Null Ciphers on UNIX

If you configure your Web server for client authentication using SSL 3.0, and if your Siebel Server is on a UNIX operating system, you can encounter an error (Error 12157) during the SSL handshake procedure if you have enabled the NULL encryption cipher.

To use the NULL cipher on the Web server, you must disable all other ciphers. For information on disabling ciphers in the Mainsoft MainWin registry using the X-Windows regedit utility, and for general information on resolving errors that can occur when using the EAI HTTP Transport business service with SSL, see 762002.1 (Article ID) on My Oracle Support.

About Configuring Communications Encryption for Siebel Enterprise and SWSE

When you configure your Siebel Enterprise or a Siebel Web Server Extension (SWSE) logical profile after installation, you specify which encryption type to use for communications between the Siebel Server and the Web server (SWSE), and between Siebel Servers. Communications between these modules use the SISNAPI protocol.

The encryption type setting determines how encryption is defined within generated connect strings for Siebel Business Applications. It also corresponds to the value of the Siebel Enterprise parameter Encryption Type (alias Crypt). You can specify Secure Sockets Layer (SSL), Microsoft Crypto, or RSA encryption.

You can use both SSL and RSA or Microsoft Crypto for SISNAPI encryption in a single Siebel Enterprise. This flexibility is because SSL is enabled at the Siebel Server level while RSA or Microsoft Crypto are enabled at the server component level. For example, because the remote synchronization SISNAPI channel does not currently support SSL, RSA or Microsoft Crypto are the only encryption options for this channel. To encrypt this channel with RSA or Microsoft Crypto, run the remote component on a Siebel Server separate from the Siebel Servers that are configured for SSL. Then, enable RSA or Microsoft Crypto for the remote component.

Use SSL or RSA or Microsoft Crypto to encrypt different communication channels; it does not make sense to encrypt the same communication channel with both SSL and RSA or Microsoft Crypto.

When configuring the Siebel Enterprise using the Siebel Configuration Wizard, the Security Encryption Level or Type screen displays the options for configuring the encryption type. You can choose one of the following options:

- None
- SISNAPI Without Encryption
- SISNAPI Using RSA Encryption Algorithm
- SISNAPI Using SSL 3.0
- SISNAPI Using Enhanced SSL 3.0 (requires hardware proxy)
- SISNAPI Using Microsoft Crypto API Encryption (Windows Only)

NOTE: For Siebel CRM installations that use both UNIX and Microsoft Windows operating systems, it is recommended to use an encryption method supported by both, such as SSL or RSA.

When using the Siebel Configuration Wizard to configure a SWSE logical profile that you subsequently deploy to Web Servers in your Siebel environment, you are presented with an option allowing you to enable SSL communication between the Web server and Siebel Server. For information about running the Siebel Configuration Wizard, see *Siebel Installation Guide* for the operating system you are using. For more information on configuring SSL, see the following topics:

- "Configuring SSL Encryption for the Siebel Enterprise or a Siebel Server" on page 75
- "Configuring SSL Encryption for SWSE" on page 78

Key Exchange for Microsoft Crypto or RSA Encryption

If you are using Microsoft Crypto or RSA encryption, the following steps explain how Siebel encryption keys are exchanged between the client (for example, the Web server) and the server (for example, Siebel Server).

1. The client 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.

NOTE: If you are using SSL encryption between the Web server and Siebel Server or between Siebel Servers, the key exchange is handled through a standard SSL handshake.

Configuring SSL Encryption for the Siebel Enterprise or a Siebel Server

This topic describes how you configure your Siebel Enterprise or Siebel Server to use Secure Sockets Layer (SSL) encryption and authentication for SISNAPI communications between Siebel Servers and the Web server (SWSE), and between Siebel Servers. Configuring SSL for SISNAPI communications is optional.

This task is a step in "Process of Configuring Secure Communications" on page 66.

Configuring SSL communications between Siebel Servers and the Web server also requires that you configure the SWSE to use SSL, as described in "Configuring SSL Encryption for SWSE" on page 78.

When configuring SSL for Siebel Server and the SWSE, you can also configure connection authentication for the relevant modules. In other words, when a module connects to another module, modules might be required to authenticate themselves against the other using third-party certificates.

Connection authentication scenarios are:

- Siebel Server authenticates against the Web server.
- Web server authenticates against the Siebel Server.
- Siebel Server authenticates against another Siebel Server.

A peer authentication option requires that mutual authentication be done.

The following procedure describes running the Siebel Configuration Wizard to deploy SSL for a Siebel Server or a Siebel Enterprise. Performing this procedure adds parameters to the Siebel Gateway Name Server; these parameters can also be set using Siebel Server Manager.

NOTE: If you configure SSL for the Siebel Enterprise, all Siebel Servers in the Enterprise inherit all settings. These settings include the key file name and password and certificate file names. You can run the Siebel Configuration Wizard again later to separately configure individual Siebel Servers, at which time you can specify unique key filenames or passwords or unique certificate file names. In order to completely configure SSL for your Siebel Servers, you must run this utility multiple times.

On Windows, SSL configuration of the Enterprise or SWSE always uses GUI mode. On UNIX, initial SSL configuration of the Enterprise or SWSE uses GUI mode. However, if you configure SSL separately later on a UNIX operating system, SSL runs in console mode.

To enable SSL encryption for the Siebel Enterprise or for a Siebel Server

1. Before you begin, obtain and install the necessary certificate files that you require if you are configuring SSL authentication.

2. (Siebel Enterprise) If you are running the Siebel Configuration Wizard to configure the Siebel Enterprise, do the following:

   a. Start the Siebel Configuration Wizard and configure values for the Enterprise, as described in *Siebel Installation Guide* for the operating system you are using.

   b. When the Additional Tasks for Configuring the Enterprise screen appears, select the Enterprise Network Security Encryption Type option.

   c. Specify that you want to deploy SSL for the Enterprise.

   d. Proceed to Step 4 on page 76.

3. (Siebel Server) If you are running the Siebel Configuration Wizard directly on a Siebel Server computer, do the following:

   a. Start the Siebel Server Configuration Wizard directly and configure values for the Siebel Server, as described in *Siebel Installation Guide* for the operating system you are using.

   b. When the Additional Tasks for Configuring the Siebel Server screen is displayed, select the Server-Specific Security Encryption Settings option.

   c. Proceed to Step 4.

4. Specify the name and location of the certificate file and of the certificate authority file.

   The equivalent parameters in the Siebel Gateway Name Server are CertFileName (display name is Certificate file name) and CACertFileName (display name is CA certificate file name).

5. Specify the name of the private key file, and the password for the private key file, then confirm the password.

   The password you specify is stored in encrypted form. The equivalent parameters in the Siebel Gateway Name Server are KeyFileName (display name Private key file name) and KeyFilePassword (display name Private key file password).

6. Specify whether you require peer authentication.

   Peer authentication means that this Siebel Server authenticates the client (that is, SWSE or another Siebel Server) that initiates a connection. Peer authentication is false by default.

   The peer authentication parameter is ignored if SSL is not deployed between the Siebel Server and the client (that is, SWSE or another Siebel Server). If peer authentication is set to TRUE on the Siebel Server, a certificate from the client is authenticated provided that the Siebel Server has the certifying authority's certificate to authenticate the client's certificate. The client must also have a certificate. If SSL is deployed and the SWSE has a certificate, then it is recommended that you set PeerAuth to TRUE on both the Siebel Server and the SWSE to obtain maximum security.

   The equivalent parameter in the Siebel Gateway Name Server is PeerAuth (display name Peer Authentication).

7. Specify whether you require peer certificate validation.

   Peer certificate validation performs reverse-DNS lookup to independently verify that the hostname of the Siebel Server computer matches the hostname presented in the certificate. Peer certificate validation is false by default.

   The equivalent parameter in the Siebel Gateway Name Server is PeerCertValidation (display name Validate peer certificate).

8. (Siebel Enterprise) If you are running the Siebel Configuration Wizard to configure the Siebel Enterprise, you return to that process, as described in the *Siebel Installation Guide* for the operating system you are using.

9. (Siebel Server) If you are running the Siebel Server Configuration Wizard, select the appropriate option to specify whether or not you want to enable clustering of the Siebel Servers and, if you do, the type of clustering you want to use.

10. Select the check box if you want the Siebel Server system service to start automatically.

11. Select the check box if you want the Siebel Server system service to start at the end of the profile configuration.

12. Review the settings, finish configuration, and restart the server.

13. Perform the tasks in "Setting Additional SSL Parameters for Siebel Server" on page 78.

14. Repeat this procedure for each Siebel Server in your environment, as necessary.

    Make sure you also configure each SWSE in your environment, as described in "Configuring SSL Encryption for SWSE" on page 78.

Setting Additional SSL Parameters for Siebel Server

After configuring SSL for a Siebel Server, you must set additional SSL parameters for the Siebel Server, as described in the following procedure.

To set additional SSL parameters for Siebel Server

- Using Siebel Server Manager, set the Communication Transport parameter (alias CommType) to SSL for each AOM that is to use SSL. (TCP/IP is used by default.)
- If you previously used Microsoft Crypto or RSA encryption, then, using Siebel Server Manager, set the Encryption Type parameter (alias Crypt) to `NONE` (instead of `MSCRYPTO` or `RSA`) for the Siebel Enterprise.

For information on using Siebel Server Manager, see *Siebel System Administration Guide*.

Configuring SSL Encryption for SWSE

This topic describes how to configure your SWSE to use Secure Sockets Layer (SSL) encryption and, optionally, authentication for SISNAPI communications with Siebel Servers using the Siebel Configuration Wizard. Configuring SSL communications between Siebel Servers and the Web server also requires that you configure a Siebel Enterprise or Siebel Server to use SSL, as described in "Configuring SSL Encryption for the Siebel Enterprise or a Siebel Server" on page 75.

This task is a step in "Process of Configuring Secure Communications" on page 66.

The information in this topic describes how to implement SSL for communications between the SWSE and Siebel Servers. For information on implementing SSL for communications between a Siebel Web client and the SWSE, see "Configuring a Siebel Web Client to Use SSL" on page 199.

About Configuring SSL Encryption for SWSE

When you configure your SWSE to use SSL, a parameter is added to the eapps.cfg file in a new section called [connmgmt]. The [connmgmt] section looks similar to the following:

```
[connmgmt]
CACertFileName = c:\security\cacertfile.pem
CertFileName = c:\security\certfile.pem
KeyFileName = c:\sba80\admin\keyfile.txt
KeyFilePassword = ^s*)Jh!#7
PeerAuth = TRUE
PeerCertValidation = FALSE
```

Names for the eapps.cfg file parameters mentioned in this procedure correspond to the Siebel Gateway Name Server parameters for the Siebel Server. For descriptions of the SSL-related parameters listed in the previous example, see "Parameters in the eapps.cfg File" on page 335.

After configuring SSL encryption for the SWSE, for any AOM that will connect to the SWSE using SSL, you must modify the ConnectString parameter to specify SSL as the communications type (TCP/IP is used by default), and none as the encryption type. For example, for Siebel Sales using U.S. English, modify the parameter in the [/sales_enu] section of eapps.cfg to resemble the following:

```
siebel.ssl.None.None://gtwyname/siebel/SSEObjMgr_enu
```

Deploying SSL for SWSE

To deploy SSL for SWSE, you first configure a SWSE logical profile using the Siebel Configuration Wizard (Siebel Enterprise Configuration Wizard). During this stage, you specify the values for deployment of SSL on the SWSE. You then apply the SWSE logical profile to the installed instance of the SWSE using the SWSE Configuration Wizard. The following procedure describes both of these steps.

To enable SSL encryption for the SWSE

1. Before you begin, obtain and install the necessary certificate files you require if you are configuring SSL authentication.
2. Launch the Siebel Configuration Wizard, as described in *Siebel Installation Guide* for the operating system you are using.
3. Specify whether you want to configure the product in live mode or offline mode.
4. Select Create New Configuration.
5. Select the option Configure a New Siebel Web Server Extension Logical Profile.
6. Configure other values for the SWSE logical profile, as described in *Siebel Installation Guide* for the operating system you are using, until the Deploy SSL in the Enterprise screen appears.
7. Select the check box, Deploy Secure Socket Layer (SSL) in the Enterprise, to enable SSL communications between the Web server and the Siebel Server.
8. Specify the names of the certificate file and of the certificate authority file.

   The equivalent parameters in the eapps.cfg file are CertFileName and CACertFileName.
9. Specify the name of the private key file, and the password for the private key file, then confirm the password. The password you specify is stored in encrypted form.

   The equivalent parameters in the eapps.cfg file that the SWSE logical profile applies to the installed SWSE are KeyFileName and KeyFilePassword.
10. Specify whether you require peer authentication.

    Peer authentication means that the SWSE authenticates the Siebel Server whenever a connection is initiated. Peer authentication is false by default.

    NOTE: If peer authentication is set to TRUE on the SWSE, the Siebel Server is authenticated, provided that the SWSE has the certifying authority's certificate to authenticate the Siebel Server's certificate. If you deploy SSL, it is recommended that you set PeerAuth to TRUE to obtain maximum security.

    The equivalent parameter in the eapps.cfg file that the SWSE logical profile applies to the installed SWSE is PeerAuth.

11 Specify whether you require peer certificate validation.

Peer certificate validation performs reverse-DNS lookup to independently verify that the hostname of the Siebel Server computer matches the hostname presented in the certificate. Peer certificate validation is false by default.

The equivalent parameter in the eapps.cfg file that the SWSE logical profile applies to the installed SWSE is PeerCertValidation.

12 Review the settings. If the settings are correct, execute the configuration and proceed to Step 13.

13 Using the SWSE Configuration Wizard, apply the SWSE logical profile to each SWSE in your Siebel environment for which you want to secure communication using SSL.

For information on applying the SWSE logical profile, see the *Siebel Installation Guide* for the operating system you are using.

14 For each AOM that will connect to the SWSE using SSL, modify the ConnectString parameter.

For information on modifying the ConnectString parameter, see "About Configuring SSL Encryption for SWSE" on page 78.

Make sure you also configure each Siebel Server in your environment, as described in "Configuring SSL Encryption for the Siebel Enterprise or a Siebel Server" on page 75.

About Configuring SSL for the Siebel Management Framework

You can deploy SSL to secure communication between the Siebel Diagnostic Tool, the Siebel Management Server, and Siebel Management Agent(s). For details, see 475465.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Alert 1268.

Enabling SSL Acceleration for Web Server and Web Client Communications

This topic describes how to configure the deployment of SSL in your Siebel Enterprise to use SSL acceleration for communications between the Siebel Web server and Siebel Web Clients.

This task is a step in "Process of Configuring Secure Communications" on page 66.

Use of SSL acceleration moves computationally intensive SSL processing away from the Web server to a reverse proxy server, or third-party load balancer, which improves application performance. For information on using reverse proxy servers with Siebel Business Applications, see "Firewall and Proxy Server Support" on page 50. For information on configuring Siebel Web Clients to use SSL, see "Configuring a Siebel Web Client to Use SSL" on page 199.

To enable SSL acceleration

- To enable SSL acceleration, set the Siebel Application Object Manager parameter, EnforceSSL, to True.

  The default value of the EnforceSSL parameter is False. For detailed information on changing the EnforceSSL parameter value, see *Siebel System Administration Guide*.

About Configuring Encryption for Web Clients

This topic describes the encryption options available for Web client communications. To use encryption, both the server and the client must enforce encryption in their connection parameters. If these parameters do not match, connection errors occur.

Siebel Business Applications support the following types of clients:

- **Siebel Web Client.** This client runs in a standard browser from the client computer and does not require any additional persistent software installed on the client. Encryption settings you make to the SWSE or Siebel Server are automatically recognized by this Web Client.

  For more information about securing communication using SSL, see "Configuring a Siebel Web Client to Use SSL" on page 199

- **Siebel Mobile Web Client.** This client is designed for local data access, without having 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 a Mobile Web Client and the Siebel Remote server, see "Configuring Encryption for Mobile Web Client Synchronization" on page 82. See also *Siebel Remote and Replication Manager Administration Guide*.

- **Siebel Developer Web Client.** This client connects directly to the Siebel database for all data access. It does not store any Siebel data locally. With the exception of the database, all layers of the Siebel Business Applications architecture reside on the user's personal computer.

- **Siebel Handheld Client.** A streamlined version of the Siebel Mobile Web Client. Documentation for particular Siebel Business Applications using the Siebel Handheld client can be found on *Siebel Bookshelf*.

For more information about some of the Siebel client types described above, see also *Siebel Deployment Planning Guide*.

About Session Cookies

The AOM 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 Business Applications use session cookies to track the session state.

These session 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 that started at the login page.

Instead of storing the session ID in clear text in the client's browser, Siebel Business Applications create an encrypted session ID and attach an encryption key index to the encrypted session ID. Session cookie encryption uses a 56-bit key default.

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

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

For more information about session cookies, see "About Using Cookies with Siebel Business Applications" on page 204.

Configuring Encryption for Mobile Web Client Synchronization

This topic describes how to enable encryption for Mobile Web Client synchronization. During this synchronization, DX files are transferred between the Siebel Server and Mobile Web Clients. DX files use SISNAPI messages to transfer information between the Siebel Server and Mobile Web Clients.

This task is a step in "Process of Configuring Secure Communications" on page 66.

The Siebel Mobile Web Client reads configuration parameters in the Siebel application configuration file (for example siebel.cfg, used by Siebel Sales) to determine the type of encryption to use during synchronization. Encryption options are defined as one of the elements in the DockConnString parameter.

NOTE: Secure Sockets Layer (SSL) is not a supported encryption method for the Siebel Developer Web Client or for synchronization of the local database on the Siebel Mobile Web Client.

For information about authentication for Siebel Mobile Web Client and Siebel Remote, see "Authentication for Mobile Web Client Synchronization" on page 176.

For information about other security issues for Siebel Mobile Web Client, including encrypting the local database, see *Siebel Remote and Replication Manager Administration Guide*.

To enable encryption of synchronization on the Mobile Web Client

1. Open the Siebel application configuration file you want to edit. You can use any plain text editor to make changes to the file.

   - Configuration files for a client are stored in the client's bin\LANGUAGE directory, where *LANGUAGE* represents an installed language pack—such as ENU for U.S. English.

   - When synchronization is performed within Siebel Business Applications by selecting the Synchronize Database option from the File menu, configuration is read from the configuration file associated with the application (for example, siebel.cfg for Siebel Sales).

     For more information about working with Siebel Business Applications configuration files, see *Siebel System Administration Guide*.

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 element in the DockConnString parameter. This element indicates the type of encryption used during synchronization.

   An example of a DockConnString parameter value would be:

   ```
   APPSRV: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 one of the following:

   - `APPSRV:TCPIP:40400:DOCK:RSA`
   - `APPSRV::RSA`

4. Save your changes and exit the file.

   For more information about editing configuration files for Siebel Remote and Mobile Web Clients, see *Siebel Remote and Replication Manager Administration Guide* and *Siebel System Administration Guide*.

About Data Encryption

You can encrypt sensitive data in the Siebel database, such as customer credit card numbers, using various encryption alternatives (RC2 or AES encryption) provided by Siebel Business Applications.

Standard Siebel Business Applications provide the option for 56-bit RC2 encryption capabilities for data in the Siebel database. If you require stronger encryption capabilities, you must have the Siebel Strong Encryption Pack. For further information, see “About the Siebel Strong Encryption Pack” on page 97.

See the following topics for additional information about data encryption:

- “How Data Encryption Works” on page 84
- “Requirements for Data Encryption” on page 84
- “Configuring Encryption and Search on Encrypted Data” on page 86
- “Managing the Key File Using the Key Database Manager” on page 89
- “About Upgrading Data to a Higher Encryption Level” on page 92

How Data Encryption Works

When encryption is enabled for a column in a database table, unencrypted data from all the fields in this column is sent through the specified encryptor (that is, the AES Encryptor or RC2 Encryptor). The encryptor encrypts the data using an encryption key stored in the key file.

After the data is encrypted, it is sent back to the database. When a user accesses this data, the encrypted data is sent through the encryptor again to be decrypted. The data is decrypted using the same encryption key from the key file that was used for encryption. The decrypted data is then sent to the business component field to be displayed in the application. For information on configuring encryption for a database column, see "Configuring Encryption and Search on Encrypted Data" on page 86.

The key file stores a number of encryption keys that encrypt and decrypt data. The key file is named keyfile.bin and is located in the admin subdirectory of the Siebel Server directory. Additional encryption keys can be added to the key file. For security, this file is encrypted with the key file password. For information on using the Key Database Manager utility to add encryption keys and change the key file password, see "Managing the Key File Using the Key Database Manager" on page 89.

NOTE: The loss of the key file's password is irrecoverable.

Requirements for Data Encryption

Encrypting data is subject to the following restrictions and requirements:

CAUTION: Do not attempt to change the encryption key length after a Siebel environment has been set up and running. To do so requires the regeneration of all keys (including the key file), as well as the reencryption of all the applicable data. Rather, set the key length once during installation. You can, however, use the supported mechanisms to explicitly upgrade the encryption key lengths.

- Because encryption and decryption have performance implications, encrypt only column data that is truly sensitive, such as credit card numbers and social security numbers.
- Siebel Assignment Manager does not decrypt data before making assignments. Assignment rules must take this limitation into consideration.
- When creating a link object to define a one-to-many relationship between a master business component and a detail business component, the source and destination fields specified in the link object definition must not be encrypted fields. If encrypted fields are specified, Siebel Business Applications cannot create the association between the two business components. For detailed information on configuring links, see *Configuring Siebel Business Applications*.
- Data that is moved into or out of the Siebel database using Siebel EIM will not be encrypted or decrypted by EIM.
- To configure 128-bit RC2 encryption (RC2 Encryptor) or any AES encryption option (AES Encryptor), you must have first installed the Siebel Strong Encryption Pack. 56-bit RC2 encryption is available for Siebel Business Applications without the Strong Encryption Pack.

- Encrypted data is retrieved, decrypted, and displayed from the fields in the encrypted column when records are selected. Users can perform exact-match queries on the unencrypted values for these fields if you create a hash column to store the hash values as described in "Configuring Encryption and Search on Encrypted Data" on page 86.
- You can only apply RC2 or AES encryption to data in database columns that are at least 32 bytes long. You cannot encrypt database columns of type VarChar that are less than 30 bytes long.
- Encrypted data requires more storage space in the database than unencrypted data. You must specify appropriate data length for the affected columns. Use the following formulae when you allocate storage space for encrypted data:
  - For ASCII characters, the column size must be: (number of characters * [multiplied by] 2) + [plus] 10.
  - For non-English characters, the column size must be: (number of characters * [multiplied by] 4) + [plus] 10.
  - If you create a Hash Column (to enable search on encrypted data), specify VarChar as the physical type of the column. The column size must be at least 30 characters; this is a requirement for use of the RSA SHA-1 algorithm.
- Field-level AES or RC2 encryption is not supported for Developer Web Clients.
- Encryption is not supported for List of Values (LOV) columns or multilingual LOV (MLOV) columns.
- Encryption for a Mobile Web Client.

  Rather than encrypt data using AES or RC2 encryption, the local database is encrypted. For information about encrypting the local database, see *Siebel Remote and Replication Manager Administration Guide*. For information about configuring encryption when the Mobile Web Client's local database is synchronized, see "Configuring Encryption for Mobile Web Client Synchronization" on page 82.

Related Topic

"About Data Encryption" on page 83

Encrypted Database Columns

Siebel Business Applications provide a number of database columns that are encrypted by default. Table 6 lists the database table columns encrypted by default in the Siebel database. For information on how to encrypt a database column, see "Configuring Encryption and Search on Encrypted Data" on page 86.

Table 6. Encrypted Database Table Columns

Table	Table Column
S_ORDER	ACCNT_ORDER_NUM
	CC_NUMBER

Table 6. Encrypted Database Table Columns

Table	Table Column
S_PTY_PAY_PRFL	PAY_ACCNT_NUM
	VERIFICATION_NUM
S_SRC_PAYMENT	CC_NUM
S_SSO_SYS_USER	SSO_PASSWORD

Related Topic

"About Data Encryption" on page 83

Upgrade Issues for Data Encryption

This topic describes upgrade issues for data encryption to consider when upgrading from a previous release of Siebel Business Applications to the 8.0 release.

Prior to release 8.0, application developers enabled data encryption by specifying values for business component field user properties. As of release 8.0, application developers enable data encryption by encrypting columns in database tables. All fields in the encrypted columns are encrypted.

The upgrade process automatically migrates business component field user properties to database table column properties so that all fields in the encrypted column are encrypted.

NOTE: A requirement for data encryption to work in release 8.0 is that the encrypted column and the key index column reside in the same database table.

For information on upgrading data encrypted using the standard encryptor, which is no longer supported, to 56-bit RC2 encryption, see "About Upgrading Data to a Higher Encryption Level" on page 92.

Related Topic

"About Data Encryption" on page 83

Configuring Encryption and Search on Encrypted Data

This topic describes how to use Siebel Tools to enable encryption for a column in a database table. In addition, it describes how you can enable search on the encrypted column.

NOTE: Do not encrypt columns in database tables without the assistance of Oracle's Application Expert Services. For help with encrypting a column in a database table, you must contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance from Oracle's Application Expert Services.

You encrypt a column and its data by specifying values for certain parameters of the column in the database table. You can also enable search on the encrypted data by creating an additional column (hash column) that stores the result of applying the RSA SHA-1 algorithm to the plaintext value of the encrypted data. Search can be case-sensitive or case-insensitive depending on how you configure search.

The following procedure describes how to encrypt data and, optionally, how to enable search on this data. Before carrying out the procedure, note the following points:

- The encrypted column, hash column, and the column that stores the index number to the key file must come from the same database table.
- You cannot encrypt a column that has a denormalized column, because this feature is not supported. For example, column NAME of account table S_ORG_EXT has a denormalized column in: S_ACCNT_POSTN.ACCOUNT_NAME.
- The encrypted column and the hash column must be of type String (VARCHAR), while the column that stores the index number to the key file must be of type Integer. For more information on requirements for data encryption, see "About Data Encryption" on page 83.

To encrypt a column and enable search on the encrypted column in a database table

1. Start Siebel Tools.
2. Select the column in the database table that contains the data you want to encrypt.
3. Add values to the following parameters of the column you selected in Step 2:
   - Computation Expression

     Specify the algorithm to encrypt data in the column. Valid values are SiebelEncrypt.RC2 ([ColumnName]) or SiebelEncrypt.AES ([ColumnName]). To use AES, you require the Siebel Strong Encryption Pack. For more information, see "About the Siebel Strong Encryption Pack" on page 97.
   - Encrypt Key Specifier

     Specify the column that stores the index number to the key file.
4. If you want to allow search on encrypted data, create another column with a name of your choice or with the following name format:

```
C_HASH_NAME
```

where *Name* is the name of the column you selected in Step 2.

C_HASH_*NAME* stores the value that results from applying the RSA SHA-1 algorithm to the plain text values of the column you selected in Step 2.

The following table lists the syntax for a number of encryption and search scenarios.

Scenario	Enter these values

Encrypt data in column C_SSI using the RC2 algorithm	■ For Computation Expression, enter:
	`SiebelEncrypt.RC2 ([C_SSI])`
	■ For Encrypt Key Specifier, specify the column that stores the index key for the key file. For example:
	`C_KeyIndex`

Encrypt data in column C_SSI using the AES algorithm	■ For Computation Expression, enter:
	`SiebelEncrypt.AES ([C_SSI])`
	■ For Encrypt Key Specifier, specify the column that stores the index key for the key file. For example:
	`C_KeyIndex`

To enable case-sensitive search on the data that you encrypt in column C_SSI, you create an additional column C_HASH_SSI	Enter the following syntax in the field for the Computation Expression of column C_HASH_SSI: `SiebelHash.SHA1 ([C_SSI])`
To enable case-insensitive search on the data that you encrypt in column C_SSI, you create an additional column C_HASH_SSI	Enter the following syntax in the field for the Computation Expression of column C_HASH_SSI: `SiebelHash.SHA1CI ([C_SSI])`

Now do one of the following:

- If the column that you have enabled for encryption does not yet contain data, there are no further steps to perform.
- If the column that you have enabled for encryption does contain data, proceed to Step 5 on page 89.

5. If the database column that you have enabled for encryption previously contained data, run the Encryption Upgrade utility (encryptupg.exe) to encrypt the existing data and, if applicable, to create searchable hash values for the preexisting data.

   Encrypt existing data immediately after you configure a column for encryption. You can create searchable hash values for the column at a later time if you choose. For information on using the encryptupg.exe utility, see "Running the Encryption Upgrade Utility" on page 95.

Managing the Key File Using the Key Database Manager

This topic describes how to run the Key Database Manager utility to add new encryption keys to the key file and to change the key file password. The AES Encryptor and RC2 Encryptor use the key in the key file to encrypt new data. The Key Database Manager automatically determines which encryptor to use (RC2 Encryptor or AES Encryptor).

The Key Database Manager utility is named keydbmgr.exe on Microsoft Windows and keydbmgr on UNIX operating systems. It is located in the bin subdirectory of the Siebel Server directory.

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

The following procedure describes how to run the Key Database Manager.

To run the Key Database Manager

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

   For information on shutting down server components, see *Siebel System Administration Guide*.

2. From the bin subdirectory in the Siebel Server directory, run Key Database Manager using the following syntax:

   On Windows:

   ```
   keydbmgr.exe \u db_username \p db_password \l language \c config_file
   ```

   On UNIX:

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

   For descriptions of the flags and parameters, see Table 7 on page 90.

3. When prompted, enter the key file password:

   - To add a new encryption key, see "Adding New Encryption Keys" on page 90.
   - To change the key file password, see "Changing the Key File Password" on page 91.

4. To exit the utility, enter *3*.

5. Restart any server components that were shut down in Step 1 on page 89.

   For information on starting server components, see *Siebel System Administration Guide*.

Table 7 on page 90 lists the flags and parameters for the Key Database Manager utility.

Table 7. Key Database Manager Flags and Parameters

Flag	Parameter	Description
/u	*db_username*	Username for the database user
/p	*db_password*	Password for the database user
/l	*language*	Language type
/c	*config_file*	Full path to the application configuration file, such as siebel.cfg for Siebel Sales.

The following topics provide information on adding new encryption keys to the key file and changing the key file password:

- "Adding New Encryption Keys" on page 90
- "Changing the Key File Password" on page 91

Adding New Encryption Keys

You can add new encryption keys to the key file. The AES Encryptor or RC2 Encryptor uses the latest key in the key file to encrypt new data; existing data is 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 key file.

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

To add new encryption keys

1. Shut down any server components that are configured to use encryption.
2. From the bin subdirectory in the Siebel Server directory, run Key Database Manager.

   For details, see "Managing the Key File Using the Key Database Manager" on page 89.
3. To add an encryption key to the key file, enter *2*.
4. Enter some seed data to provide random data for generating the new encryption key.

   The key must be at least seven characters and no more than 255 characters in length.
5. Exit the utility by entering *3*.

   When exiting the Key Database Manager utility, monitor any error messages that are generated. If an error occurs, you might have to restore the backup version of the key file.

6 Distribute the new key file to all Siebel Servers by copying the file to the admin subdirectory in the Siebel Server directory.

CAUTION: When copying the keyfile.bin file to Siebel Servers, take care that the file does not become damaged. If the key file is damaged, it might not be possible to recover encrypted data without a backup key file.

7 Restart any server components that were shut down in Step 1 on page 90.

For information on starting server components, see *Siebel System Administration Guide*.

Related Topic

"Managing the Key File Using the Key Database Manager" on page 89

Changing the Key File Password

The key file is encrypted by the key file password. To prevent unauthorized access, you can change the key file password using the Key Database Manager utility. The key file will be reencrypted using a new encryption key generated from the new key file password.

Before using AES or RC2 encryption for the first time, change the key file password, because all versions of the Key Database Manager utility are shipped with the same default password. The default key file password is kdbpass. Consider changing the key file password regularly to make sure the file is secured.

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

To change the key file password

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

2 Run the Key Database Manager utility from the bin subdirectory in the Siebel Server directory.

For more information, see "Managing the Key File Using the Key Database Manager" on page 89.

3 To change the key file password, enter *1*.

4 Enter the new password.

5 Confirm the new password.

6 Exit the utility by entering *3*.

When exiting the Key Database Manager utility, monitor any error messages that are generated. If an error occurred, you might have to restore the backup version of the key file.

7 Distribute the new key file to all Siebel Servers by copying the file to the admin subdirectory in the Siebel Server root directory.

8 Restart any server components that were shut down in Step 1 on page 91.

For information on starting server components, see *Siebel System Administration Guide*.

Related Topic

"Managing the Key File Using the Key Database Manager" on page 89

About Upgrading Data to a Higher Encryption Level

The Encryption Upgrade utility (encryptupg.exe), located in the bin subdirectory of the Siebel Server directory, allows you to do the following:

- Upgrade unencrypted data to the RC2 encryption method.
- Upgrade encrypted data to a higher encryption level, for example, from RC2 (56 bits) to RC2 (128 bits), provided you have installed the Siebel Strong Encryption Pack.

  For information on the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97.
- Upgrade data that was encrypted using the standard encryptor to the RC2 encryption method.

You must upgrade data that was encrypted using the standard encryptor (based on the mangle algorithm) to RC2 encryption before you upgrade to a Siebel version 8 release. For additional information, see "Requirements for Upgrading to a Higher Encryption Level" on page 93.

About the Standard Encryptor

In Siebel CRM releases earlier than 7.5.x, data was encrypted using the standard encryptor. As of Siebel CRM 7.5.x, Siebel Business Applications use the AES and the RC2 encryption algorithms to encrypt data, and the standard encryptor is supported for backwards-compatibility purposes only.

If you want to upgrade encrypted data from Siebel CRM 6.x or 7.0.x to Siebel CRM 7.5.3, 7.7, or 7.8, it is recommended that you upgrade the encrypted data to the RC2 or AES standard to ensure that the data can be read accurately by the later release. If you want to upgrade encrypted data from Siebel CRM 6.x or 7.0.x to any Siebel CRM 8 release, you must upgrade the encrypted data to the RC2 or AES standard. For information on the specific tasks you must perform to upgrade your data to a higher encryption level, see "Process of Upgrading Encrypted Data to a Higher Encryption Level" on page 92.

NOTE: You cannot upgrade directly from a Siebel CRM release earlier than 7.5.x to release 8.0. If you want to upgrade from release 6.x, you must first upgrade to release 7.7 even if you want to upgrade to a release later than 7.7.

Process of Upgrading Encrypted Data to a Higher Encryption Level

To upgrade your data to a higher encryption level, perform the following tasks:

- Verify that all requirements are met.

  For information, see "Requirements for Upgrading to a Higher Encryption Level" on page 93.

- Make sure that the input file includes every column that you want to upgrade.

  For information, see "Modifying the Input File" on page 94.

- Run the Key Database Manager utility to change the password or add a new key to the database.

  For information, see "Managing the Key File Using the Key Database Manager" on page 89.

- Upgrade the data to a higher level of encryption.

  For information, see "Running the Encryption Upgrade Utility" on page 95.

Requirements for Upgrading to a Higher Encryption Level

This topic lists the tasks you must complete before you upgrade your data to a higher encryption level.

This task is a step in "Process of Upgrading Encrypted Data to a Higher Encryption Level" on page 92.

To upgrade to a higher encryption level, the following requirements must be fulfilled:

- The Siebel Gateway Name Server and Siebel Server are installed.
- The Siebel repository has been upgraded to the schema for the current release, so that a new column has been created to store the key index for the encrypted column.
- If you created or customized columns to use the standard encryptor, for each encrypted column that you want to upgrade, you have to create a new column to store the key index.
- If, in Siebel CRM releases prior to 8.0, you customized business component fields to use the standard encryptor, verify that you define the correct properties for the columns in the database table that holds encrypted data. For further information, see "Configuring Encryption and Search on Encrypted Data" on page 86.
- Verify that column sizes for custom extension columns are large enough to hold the new RC2 values.
- The key database (keyfile.bin) must already exist. (A default key file was created in the *SIEBEL_ROOT*/siebsrvr/admin directory when you installed the Siebel Server.)
- If you require an encryption level greater than 56-bit RC2 encryption, you must install the Siebel Strong Encryption Pack and upgrade the key database file to use a higher level of encryption. For more information on these tasks, see the following topics:
  - "Installing the Siebel Strong Encryption Pack" on page 98
  - "Increasing the Encryption Level" on page 99

Modifying the Input File

Before upgrading to a higher encryption level, you must modify the encrypt_colums.inp input file to list every table and column that you want to upgrade. The input file, encrypt_colums.inp, indicates the table and column that store the encrypted data, and the table and column that store the key index.

This task is a step in "Process of Upgrading Encrypted Data to a Higher Encryption Level" on page 92.

The following procedure describes how to modify the input file.

To modify the encrypt_columns.inp file

1. Navigate to the `*SIEBEL_ROOT*/dbsrvr/bin` directory where the input file is located.

   If you want to execute the Encryption Upgrade Utility from the command line, place this file in the `*SIEBEL_ROOT*/siebsrvr/bin` directory.

2. Using a text editor, edit the input file to include every column that you want to upgrade.

   The first line of the input file indicates a table name with brackets around it. On subsequent lines following the table name, list all the columns to be upgraded for that table.

   Each column that stores encrypted data requires a table column to store the key index, which is specified after the column name; for example:

   ```
   [TABLE_NAME]
   COLUMN_NAME TABLE_NAME_FOR_KEY COLUMN_NAME_FOR_KEY
   WHERE clause
   ```

3. After each table, skip a line, and continue to list the columns for subsequent tables, as shown in the following example:

   ```
   [S_ORDER]
   CC_NUMBER S_ORDER CCNUM_ENCRPKEY_REF
   WHERE S.CC_NUMBER='1234567890'

   [S_DOC_ORDER]
   CC_NUMBER S_DOC_ORDER CCNUM_ENCRPKEY_REF
   WHERE S.CC_NUMBER='1231231231'

   [S_PER_PAY_PRFL]
   PAY_ACCNT_NUM S_PER_PAY_PRFL CCNUM_ENCRPKEY_REF
   WHERE S.CC_NUMBER='1231231231'
   ```

4. When you have added information for every table column that you want to upgrade, save the input file.

About Using the Where Clause and Flags in the Input File

On the line following the name of each column to be upgraded, you can optionally specify the WHERE clause, the N flag, and the H flag for the column:

- Use the WHERE clause if you want to partition the data to encrypt. Every column name that you specify for the WHERE clause must have the letter S added to the start of the column name. If you do not want to partition data, omit the WHERE clause, as in the following example:

  ```
  [S_ORDER]
  CC_NUMBER S_ORDER CCNUM_ENCRPKEY_REF
  WHERE
  ```

- To support upgrade of non-encrypted fields to use encryption, add the letter *N* to the end of the column; for example:

  ```
  [S_NEW_TABLE]
  COLUMN_NAME S_NEW_TABLE NAME_KEY_INDEX
  N
  ```

- If you want to enable search on the upgraded encrypted column, add the letter `H` to the end of the column; for example:

  ```
  [S_NEW_TABLE]
  COLUMN_NAME S_NEW_TABLE NAME_KEY_INDEX
  H
  ```

  This creates a hash column that stores the output, which results from applying the RSA SHA-1 algorithm to the plain text values of the encrypted column.

  If you want to enable search on an existing encrypted column, add the following entry in the input file to create a column which stores the hash value of the plain text in the encrypted column:

  ```
  [S_TABLE_NAME]
  COLUMN_NAME S_TABLE_NAME COLUMN_NAME_ENCRPKEY_REF
  H
  WHERE S.ROW_ID='123123'
  ```

  This creates a hash column that stores the output, which results from applying the RSA SHA-1 algorithm to the plaintext values of the encrypted column.

For more information about search on encrypted data, see "Configuring Encryption and Search on Encrypted Data" on page 86.

Running the Encryption Upgrade Utility

This topic describes how to run the Encryption Upgrade utility. You must run the utility if you want to perform either of the following tasks:

- Encrypt data that is not encrypted
- Increase the encryption level of data that is already encrypted

This task is a step in "Process of Upgrading Encrypted Data to a Higher Encryption Level" on page 92.

The Encryption Upgrade utility writes output to its own log file which is located in the log subdirectory of your Siebel Server directory. The default filename for the log file is encryptupg.log. You can specify another filename for the log file as described by the following procedure.

To run the encryption upgrade utility

1. Verify that the input file encrypt_colums.inp includes all the columns that you want to upgrade. If necessary, review "Modifying the Input File" on page 94.

2. Run encryptupg.exe by navigating to the *SIEBEL_ROOT*\siebsrvr\bin directory and entering the following command:

```
encryptupg.exe /f FromEncrytionStrength /t ToEncryptionStrength /j InputFileName
/l Language /u UserName /p Password /c ConfigurationFile /L LogFile
```

where:

- *FromEncrytionStrength* is the encryption strength that you want to upgrade from. The following table describes valid parameters to enter in this command.

Parameter	Description
NONE	Unencrypted data.
STAND	Data encrypted by the Siebel Standard Encryptor. This type of encryption is no longer supported.
RC2	Data encrypted using the RC2 encryption method.

CAUTION: When you run the Encryption Upgrade utility on unencrypted data and specify the NONE parameter, the utility will encrypt the data. Be careful that you do not run the utility in this mode on the same data twice. If you do, you will encrypt data that is already encrypted, leading to a permanent loss of data.

- *ToEncryptionStrength* is the encryption strength that you want to upgrade to. The following table describes valid parameters to enter in this command.

Parameter	Description
RC2	Data encrypted using the RC2 encryption method.
AES	Data encrypted using the AES encryption method.

- *InputFileName* is the filename of your input file (the default is encrypt_columns.inp).
- *Language* is the language code. To specify U.S. English, enter ENU.
- *UserName* is the user name for the database.
- *Password* is the password for the database.
- *ConfigurationFile* is the application configuration file where you specify the data source for the Encryption Upgrade utility to retrieve data from.
- *LogFile* is the log file that the Encryption Upgrade utility writes to. By default it is encryptupg.log.

For example, the following command allows a Siebel administrator to upgrade data encrypted using RC2 encryption to AES encryption:

```
encryptupg /f RC2 /t AES /j d:\sba80\siebsrvr\bin\encryptupg.inp /l ENU /u sadmin
p dbpw /c d:\sba80\siebsrvr\bin\enu\siebel.cfg
```

3. After the upgrade is complete, make sure that the encrypted database columns specify the value for the encryption method used in the Computation Expression parameter. For more information, see "Configuring Encryption and Search on Encrypted Data" on page 86.

4. Compile a new Siebel repository file (.SRF). For more information on how to compile a.SRF file, see *Siebel Database Upgrade Guide*.

About the Siebel Strong Encryption Pack

If you require an encryption level greater than 56-bit RC2 encryption, you must install the Siebel Strong Encryption Pack, which provides more secure encryption alternatives for your Siebel Enterprise. Installing the Siebel Strong Encryption Pack provides the following:

- AES encryption (128, 192, and 256 bits), using AES Encryptor
- RC2 encryption (128 bits), using RC2 Encryptor

  The RC2 Encryptor supports 56-bit encryption without requiring you to install the Siebel Strong Encryption Pack.

- Key Database Upgrade utility

  This utility decrypts the key file (if previously encrypted with a 56-bit or 128-bit RC2 encryption key) and then reencrypts the key file with a longer key and a more secure algorithm.

AES encryption and RC2 encryption for data are provided as Siebel business services and are configured using Siebel Tools.

Obtaining the Strong Encryption Pack

Due to restrictions imposed by the United States Department of Commerce on the export of encryption technologies, Oracle delivers the Siebel Strong Encryption Pack on separate distribution media which require a separate installation into your existing Siebel environment. For information on the export restrictions, see

http://www.bis.doc.gov/Encryption/Default.htm

To request the Siebel Strong Encryption Pack, log in to the Oracle E-Delivery Web site at the following URL and select the Siebel CRM product pack

http://edelivery.oracle.com

The Siebel Strong Encryption Pack is a media pack within the Siebel CRM product pack. Install the base Siebel Strong Encryption Pack product for your release, then install the appropriate Fix Pack release. The Fix Pack release can be obtained from My Oracle Support. For further information on the Siebel Strong Encryption Pack, see the following topics:

- "Installing the Siebel Strong Encryption Pack" on page 98
- "Increasing the Encryption Level" on page 99

Installing the Siebel Strong Encryption Pack

This topic describes how to install the Siebel Strong Encryption Pack.

For an overview of the contents of the Siebel Strong Encryption Pack and for details on how to obtain it, see "About the Siebel Strong Encryption Pack" on page 97.

Before you install the Siebel Strong Encryption Pack, carry out the following tasks:

- Install and configure a Siebel Enterprise.

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

- Read "About Upgrading Data to a Higher Encryption Level" on page 92

- Use the Siebel Image Creator utility to create a network image from which you install the Siebel Strong Encryption Pack.

  For more information on using the Siebel Image Creator utility, see *Siebel Installation Guide* for the operating system you are using.

- Change the key file password.

  For more information, see "Managing the Key File Using the Key Database Manager" on page 89.

To install the Siebel Strong Encryption Pack

1. Navigate to the location that contains the installer for the Siebel Strong Encryption Pack:

   Siebel_Image\OperatingSystem\Server\Siebel_Strong_Encryption\encryption

   where:

   - *Siebel_Image* is the directory for your Siebel network image.
   - *OperatingSystem* is the operating system where you install the Siebel Strong Encryption Pack. For example, Windows for Microsoft Windows.

   NOTE: Siebel Strong Encryption Pack is only available in U.S. English (enu) and can be installed in a Siebel environment that uses other languages.

2. Run the install executable as described in the following list:

Windows	setup.exe
Oracle Solaris	setupsol
HP-UX	setuphp
AIX	setupaix
Linux	setuplinux

   The installation starts.

3. Specify the following directory as appropriate:

   - *SIEBEL_ROOT*\siebsrvr (Windows) or *SIEBEL_ROOT/*siebsrvr (UNIX) to install the Siebel Strong Encryption Pack on the Siebel Server

- *SIEBEL_ROOT*\SWEApp (Windows) or *SIEBEL_ROOT/*SWEApp (UNIX) to install the Siebel Strong Encryption Pack on the SWSE

where *SIEBEL_ROOT* is the installation directory for your Siebel Enterprise.

4 Select the encryption algorithm to use, AES, or RC2.

For information about these algorithms, see "About the Siebel Strong Encryption Pack" on page 97.

5 Select the desired key lengths.

For information about available key lengths, see "About the Siebel Strong Encryption Pack" on page 97.

6 Complete the installation as directed by the command-line or GUI. On completion of the installation, the following files are created:

- keydbupgrade. This file is located in the BIN subdirectory of the location you specified in Step 3.

- (Windows only) sslcrsa*xxx*.dll

  where *xxx* refers to the key length that you selected in Step 5. This file is located in the BIN subdirectory of the location you specified in Step 3.

- (UNIX or LINUX only) libsslcrsa*xxx*.so

  where *xxx* refers to the key length that you selected in Step 5. This file is located in the LIB subdirectory of the location you specified in Step 3.

This completes the installation of the Siebel Strong Encryption Pack.

7 To verify that the encryption algorithm has been upgraded to the level you selected, navigate to the *SIEBEL_ROOT*\siebsrvr\bin directory (Windows) or the *$SIEBEL_ROOT*/siebsrvr/lib directory (UNIX) and identify the highest RSA DLL file that has been installed.

For example, if the highest RSA DLL file is 56, then 56-bit RC2 encryption is installed; if the highest RSA DLL file is 128, then 128-bit RC2 encryption is installed.

8 Reencrypt the Siebel administrator password using the new encryption algorithm provided by the Siebel Strong Encryption Pack. For information on this task, see one of the following topics:

- "Changing System Administrator Passwords on Microsoft Windows" on page 34
- "Changing the Siebel Administrator Password on UNIX" on page 36

9 If you are using the Siebel Strong Encryption Pack with the Siebel Reports Server, and if you have encrypted communications between the AOM and the Actuate iServer, perform the steps outlined in "Using the Siebel Strong Encryption Pack with Siebel Reports Server" on page 60.

Increasing the Encryption Level

This topic describes how to upgrade Siebel Business Applications to 128-bit, 192-bit, or 256-bit encryption.

You can upgrade the key database file to use a level of encryption greater than 56-bit RC2 encryption provided you have installed the Siebel Strong Encryption Pack. For information on the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97 and "Installing the Siebel Strong Encryption Pack" on page 98.

Table 8 on page 100 shows the supported data encryption upgrade scenarios.

Table 8. Supported Encryption Upgrade Scenarios

Encryption Level to Upgrade From	Upgrade To 128-bit RC2 encryption	Upgrade To 128-bit AES encryption	Upgrade To 192-bit AES encryption	Upgrade To 256-bit AES encryption
No encryption	Yes	Yes	Yes	Yes
Standard Encryptor encryption	Yes	Yes	Yes	Yes
56-bit RC2 encryption	Yes	Yes	Yes	Yes
128-bit RC2 encryption	NA	Yes	Yes	Yes
128-bit AES encryption	NA	NA	Yes	Yes
192-bit AES encryption	NA	NA	NA	Yes

The following procedure describes how you upgrade the key database file to use a higher level of encryption.

To upgrade the key database file to use a higher level of encryption

1 Install the Siebel Strong Encryption Pack.

2 For information on this task, see "Installing the Siebel Strong Encryption Pack" on page 98.

3 Make sure that the Siebel Gateway Name Server and Siebel Servers within the Siebel Enterprise are running.

   For more information, see *Siebel System Administration Guide*.

4 On the Siebel Server where you installed the Siebel Strong Encryption Pack, open a command-line window and navigate to the `SIEBEL_ROOT\siebsrvr\bin` directory.

5 Execute the appropriate command:

   On Windows:

```
keydbupgrade.exe \u db_username \p db_password \l language \c config_file
```

   On UNIX:

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

The following table describes the flags and parameters for the keydbupgrade command.

Flag	Parameter	Description
/u	*db_username*	Username for the database user
/p	*db_password*	Password for the database user
/l	*language*	Language type
/c	*config_file*	Full path to the application configuration file, such as siebel.cfg for Siebel Sales.

6 When prompted, enter the key length you are upgrading from. If you have not implemented encryption before, select 56-bit encryption.

7 Select the key length to upgrade to.

8 Enter the key database manager password.

For information about the key database manager password, see "Managing the Key File Using the Key Database Manager" on page 89.

The utility upgrades the encryption level to the level you specified in Step 7.

9 To verify that the encryption level has been upgraded, navigate to the following directory and note if the timestamp for keyfile.bin matches the time when you executed the keydbupgrade utility.

10 After you verify that the encryption level has been upgraded, perform the following tasks in the order listed:

- Add a new encryption key

  For information on this task, see "Adding New Encryption Keys" on page 90.

- Reset Masked Parameters

  For information on this task, see "Adding New Encryption Keys" on page 90.

11 Distribute the key file (keyfile.bin) that contains the increased encryption level to the other Siebel Servers in your Siebel Enterprise. Place it in the same directory on each Siebel Server, that is: `SIEBEL_ROOT\siebsrvr\admin\`

12 Upgrade existing encrypted data to use the new encryption level.

For more information, see "About Upgrading Data to a Higher Encryption Level" on page 92.

Reencrypting Masked Parameters

This topic provides information on how to reencrypt masked parameters after you have increased the level of encryption you use with Siebel Business Applications. Masked parameters are parameters that have their values encrypted. You must reencrypt masked parameters after increasing the encryption level, because if you do not, the Siebel Server attempts to decrypt the encrypted parameters using the original encryption key and to compare it to the password entered. If this happens, the Siebel Server writes an error to the keydbmgr.log log file.

Table 9 on page 103 lists the parameters that are encrypted when you enable encryption for Siebel Business Applications and that must be reencrypted when you increase the encryption level. Most, but not all, of the masked parameters are Siebel Server parameters that can be changed using the Server Manager program. The following procedure describes how to reset encrypted parameters to use a new encryption level using Server Manager.

To reset encrypted parameters to use a new encryption level using Server Manager

1. Log in to the Server Manager command-line interface (srvrmgr program).

   For more information on how to start and use the srvrmgr program, see *Siebel System Administration Guide*.

2. Change each of the masked parameters so that it uses the increased encryption level (see Table 9 on page 103 for a list of the masked parameters).

   For example, enter the following command to reset the Password parameter at the enterprise level:

   ```
   change ent param Password=NewPassword
   ```

Table 9 on page 103 lists the parameters that you must reencrypt if you increase the encryption level you use with Siebel Business Applications and indicates how you can reencrypt each parameter.

Table 9. Parameters That Must Be Reencrypted After Increasing the Encryption Level

Parameter	Description	To Reencrypt the Parameter
ApplicationPassword	This parameter is defined for named subsystems of type InfraSecAdpt_LDAP [the default names are LDAPSecAdpt and ADSISecAdpt]. This parameter is set if LDAP or ADSI security adapter authentication is used.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file.
CRC CustomSecAdpt_CRC DBSecAdpt_CRC	These parameter are defined for named subsystems of type InfraSecAdpt_DB, InfraSecAdpt_LDAP, or InfraSecAdpt_Custom. These parameters specify the checksum validation value for the security adapter DLL file and are set for LDAP, ADSI, database, and custom security adapters. For further information on checksum validation, see "Configuring Checksum Validation" on page 165.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file.
ClientDBAPwd	This parameter is specified for the Database Extract server component.	Use the Server Manager command.
DSPassword	This parameter is defined for named subsystems of type InfraDataSource (it can be set for the ServerDataSrc named subsystem, or another data source). It is specified for database security adapter authentication.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file.
DSPrivUserPass PrivUserPass	These parameters are specified for the Generate Triggers Siebel Server component.	Use the Server Manager command.
DbaPwd NewDbaPwd	These parameters are specified for the Generate New Database Siebel Server component used with Siebel Remote.	Use the Server Manager command. For information on changing these parameters, see *Siebel Remote and Replication Manager Administration Guide*

Table 9. Parameters That Must Be Reencrypted After Increasing the Encryption Level

Parameter	Description	To Reencrypt the Parameter
ExtDBPassword	This parameter provides credentials for the database specified in the external database subsystem.	Use the Server Manager command.
KeyFilePassword	The key file stores the encryption keys that encrypt and decrypt data. The file is encrypted with the key file password.	Using the Key Database Manager utility. For further information, see "Changing the Key File Password" on page 91. This parameter is also changed in the eapps.cfg file.
MailPassword	This parameter is set for the email account that Siebel Email Response uses to connect to the SMTP/POP3 server.	Use the Siebel user interface. Navigate to Administration - Communications, Communications Drivers and Profiles, and then the Internet SMTP/POP3 Server screen.
Password	This parameter, set at the Siebel Enterprise level, is the password for the system user (for example, SADMIN) specified by the Username parameter. It is recommended that you do not change the value for this parameter when you reencrypt it.	Use the Server Manager command.
SAPRfcPassword	This parameter specifies the SAP password used with Oracle's Siebel Connector for SAP R/3.	Edit the tools.cfg file. Edit the [SAPSubsys] section of the appropriate application configuration file if using a Siebel Mobile Web Client. See *Siebel Connector for SAP R/3* for additional information on changing this parameter.

Table 9. Parameters That Must Be Reencrypted After Increasing the Encryption Level

Parameter	Description	To Reencrypt the Parameter
TableOwnPass	This parameter specifies the password for the Database Table Owner (DBO) account, which is used to modify the Siebel database tables.	Siebel Web Clients can use the Server Manager command. Siebel Developer Web Clients must edit the appropriate application configuration file. Change the parameter in the Siebel database. See "Changing the Table Owner (DBO) Password" on page 38 for instructions.
TrustToken CustomSecAdpt_Trust Token	These parameters apply in a Web SSO environment only, and are defined for named subsystems of type InfraSecAdpt_LDAP and InfraSecAdpt_Custom. These parameters are also specified for the SWSE; the setting must be the same on both the SWSE and the security adapter.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file. Edit the eapps.cfg file for SWSE.

For information on how to increase the encryption level using the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97 and "Increasing the Encryption Level" on page 99.

Security Considerations for Unicode Support

Siebel Business Applications support Unicode. For comprehensive 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 can occur if you log into 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 SSO are Unicode-compliant.

Logging Into Siebel Business Applications

- If you use a form login mechanism for your Siebel Business 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 Business Applications, the characters used in the login form must be in ASCII.

Encrypted Data

Siebel Business Applications provide either AES and RC2 encryption to encrypt data for sensitive information such as credit card numbers. For encryption with Unicode, you *must* use either AES or RC2 encryption, rather than the Standard Encryptor, which is no longer supported.

For more information, see "About Data Encryption" on page 83.

6 Security Adapter Authentication

This chapter describes how to set up security adapter authentication for Siebel Business Applications. It includes the following topics:

About User Authentication

Authentication is the process of verifying the identity of a user. Siebel Business Applications support multiple approaches for authenticating users. You choose either security adapter authentication or Web SSO authentication for your Siebel Business Applications users:

- **Security adapter authentication.** Siebel Business Applications provide a security adapter framework to support several different user authentication scenarios:
  - **Database authentication.** Siebel Business Applications support authentication against the underlying database. In this architecture, the security adapter authenticates users against the Siebel database. Siebel Business Applications provide a database security adapter (it is configured as the default security adapter).
  - **Lightweight Directory Access Protocol (LDAP) or Active Directory Service**

  - **Interfaces (ADSI) authentication.** Siebel Business Applications support authentication against LDAP-compliant or Microsoft Active Directory (AD) directories. In this architecture, the security adapter authenticates users against the directory. Siebel Business Applications provide the following two security adapters to authenticate against directory servers:

    - ADSI Security Adapter

    - LDAP Security Adapter

    For more information, see “About LDAP or ADSI Security Adapter Authentication” on page 115.

  - **Custom.** You can use a custom adapter you provide, and configure the Siebel Business Applications to use this adapter. For more information, see “Security Adapter SDK” on page 24.

- **Web Single Sign-On (Web SSO).** This approach uses an external authentication service to authenticate users before they access Siebel Business Applications. In this architecture, a security adapter 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. For more information, see Chapter 7, “Web Single Sign-On Authentication.”

You can 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 Business Applications, because a consistent approach lowers the overall complexity of the deployment. Note that a Siebel Mobile Web Client can use only database authentication against the local database on a Mobile client. For more information about authentication for a Siebel Mobile Web Client, see *Siebel Remote and Replication Manager Administration Guide*.Referential and procedural information in the following topics relates to all major 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.

- **Configuration parameters related to authentication.** Configuration parameter values determine how your authentication architecture components interact. For information about the purpose of configuration parameters, see Appendix B, “Configuration Parameters Related to Authentication.”

- **Seed data.** When you install your Siebel Business Applications, you are provided seed data that is related to authentication, user registration, and user access to Siebel Business Applications. For detailed information on the seed data that is provided and for procedures for viewing and editing seed data, see Appendix C, “Seed Data.”

Comparison of Authentication Strategies

Table 10 on page 109 highlights the capabilities of each authentication approach to help guide your decision. Several options are available for each basic strategy.

NOTE: Comparisons do not apply for Siebel Mobile Web Client, for which only database authentication is available.

Table 10. Comparison of Authentication Approaches

Functionality	Database Security Adapter	LDAP or ADSI Security Adapter	Web SSO	Comments
Requires additional infrastructure components.	No	Yes	Yes	None
Centralizes storage of user credentials and roles.	No	Yes	Yes	None
Limits number of database accounts on the application database.	No	Yes	Yes	None
Supports dynamic user registration. Users are created in real-time through self-registration or administrative views.	No	Yes	Siebel Business Applications do not support the feature, but it might be supported by third-party components.	For Web SSO, user registration is the responsibility of the third-party authentication architecture. It is not logically handled by the Siebel architecture.

Table 10. Comparison of Authentication Approaches

Functionality	Database Security Adapter	LDAP or ADSI Security Adapter	Web SSO	Comments
Supports account policies. You can set policies such as password expiration, password syntax, and account lockout.	Yes	Yes	Siebel Business Applications do not support the feature, but it might be supported by third-party components.	Among supported RDBMS vendors for the Siebel database, account policy (password expiration only) is supported *only* for IBM DB2 UDB. 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.	No	No	Yes	None

About Siebel Security Adapters

When you install your Siebel Business Applications, these security adapters are provided for user authentication:

- Database security adapter (enabled by default)

  For more information, see "Configuring Database Authentication" on page 112.

- ADSI (Active Directory Services Interface) security adapter
- LDAP (Lightweight Directory Access Protocol) security adapter

The security adapter is a plug-in to the authentication manager. The security adapter uses the credentials entered by a user (or supplied by an authentication service) to authenticate the user, as necessary, and allow the user access to Siebel Business Applications.

You can implement a security adapter other than one of those provided by Siebel Business Applications provided the adapter you implement supports the Siebel Security Adapter Software Development Kit. For more information, see "Security Adapter SDK" on page 24.

Do not use the ADSI security adapter or LDAP security adapter to authenticate access to batch components such as, for example, the Communications Outbound Manager. Configure batch components to use the database security adapter instead. Batch components access the Siebel database directly and, as a result, must use the database security adapter. Note also that Siebel Server infrastructure and system management components such as Server Request Broker and Server Request Processor access the Siebel database directly. For this reason, these components cannot use the LDAP or ADSI security adapters.

Authentication Directories

An LDAP directory or Microsoft Active Directory is a store in which information that is required to allow users to connect to the Siebel database, such as database accounts, Siebel user IDs, or roles, is maintained external to the Siebel database, and is retrieved by the security adapter. For specific information about third-party directories supported by the security adapters provided with Siebel Business Applications, see *Siebel System Requirements and Supported Platforms* on Oracle Technology Network.

Security Adapter Authentication

In general, the process of security adapter authentication includes the following principal stages:

1. The user provides identification credentials.
2. The user’s identity is verified.
3. The user’s Siebel user ID and database account are retrieved from a directory (LDAP and ADSI security adapters), from the Siebel database, or from another external source (for Web Single Sign-On).
4. The user is granted access to Siebel Business Applications and the Siebel database.

Depending on how you configure your authentication architecture, the security adapter can function in one of the following modes, with respect to authentication:

- **With authentication (LDAP or ADSI security adapter authentication mode).** The security adapter uses credentials entered by the user to verify the user’s existence and access rights 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 Siebel Application Object Manager (AOM) to grant the user access to Siebel Business Applications and the database. This adapter functionality is typical in a security adapter authentication implementation.

- **Without authentication (Web SSO mode).** The security 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 AOM to grant the user access to Siebel Business Applications and the database. This adapter functionality is typical in a Web SSO implementation.

  NOTE: The security adapter does not provide authentication for Web SSO. Web SSO is the ability to authenticate a user one time for access to multiple applications, including Siebel Business Applications. However, when implementing Web SSO, you must also deploy a security adapter.

  For more information, see Chapter 7, “Web Single Sign-On Authentication.”

In an environment using external security adapter authentication (such as LDAP or ADSI), the security adapter can create a record in the directory when a user is created in the Siebel database.

For information on the most commonly reported error messages when implementing standard Siebel security adapters, see 477528.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Troubleshooting Steps 56.

Event Logging for Siebel Security Adapters

Siebel Business Applications provide the following event types to set log levels for security adapters:

- Security Adapter Log

  This event type traces security adapter events.

- Security Manager Log

  This event type traces security manager events.

Modify the values for these two event types to set the log levels that the Siebel Application Object Manager writes to the log file. For more information about how to set the log levels for event types, see *Siebel System Monitoring and Diagnostics Guide*.

Configuring Database Authentication

If you do not use LDAP or ADSI authentication, 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 into Siebel Business Applications.

Database Authentication Process

The stages in a database authentication process are:

1. The user enters a database account's username and password to a Siebel Business Applications login form.
2. The Siebel Web Server Extension (SWSE) passes the user credentials to the AOM, which in turn passes them to the authentication manager.
3. The authentication manager hashes the password, if DBHashUserPwd is TRUE for the data source specified for the database security adapter, and passes the user credentials to the database security adapter.
4. If the user credentials match a database account, the user is logged into the database and is identified with a user record whose user ID is the same as the database account's username.

   In other words, the database security adapter validates each user's credentials by trying to connect to the Siebel database.

Features Not Available for Database Authentication

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

- A single user-authentication method that is valid for Siebel Business Applications and other applications
- User self-registration (typically used with customer applications)
- External delegated administration of users (typically used with partner applications)
- Creation of users from the Administration - User screen in Siebel Business Applications

Implementing Database Authentication

If you implement database authentication, it will typically be for a Siebel employee application, such as Siebel Call Center or Siebel Sales. Database authentication is configured as the default, and is the easiest to implement of the authentication approaches presented in this book.

Although configuration might not be required, parameters for the database security adapter can be configured using Siebel Server Manager. To do this, you specify parameter values for a named subsystem (enterprise profile). For Developer Web Clients, parameters can be configured by editing the application configuration file directly.

The database security adapter is specified using the Security Adapter Mode (SecAdptMode) and Security Adapter Name (SecAdptName) parameters:

- Security Adapter Mode must be set to DB (the default value).
- Security Adapter Name must be set to DBSecAdpt (the default value), or to a security adapter (enterprise profile or named subsystem) with a different name.

The Security Adapter Mode and Security Adapter Name parameters can be set for the Siebel Enterprise Server, for a particular Siebel Server, for an individual AOM component, or for the Synchronization Manager component (for Siebel Remote).

CAUTION: If you want to configure a server component or a Siebel Server to use different database authentication settings than those already configured at a higher level (that is, configured for the Siebel Enterprise or Siebel Server), then create a new database security adapter. Otherwise, settings you make will reconfigure the existing security adapter wherever it is used.

You can implement user password hashing if you implement database authentication by specifying the Hash User Password parameter. User password hashing maintains an unexposed, hashed password to a database account, while an unhashed version of the password is provided to the user for logging in. When user password hashing is enabled, a hashing algorithm is applied to the user's password before it is compared to the hashed password stored in the database. For details, see "About Password Hashing" on page 157.

NOTE: For database authentication, password hashing parameters are specified for a data source referenced from the database security adapter, rather than specified directly for the security adapter.

For more information about parameters for the database security adapter, see Appendix B, "Configuration Parameters Related to Authentication."

An administrator must perform the following tasks to provide a new user with access to Siebel Business 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 Siebel user record in the Siebel database, in which the user ID matches the user name for the database account. You add users through an employee application such as Siebel Call Center.

  For information about adding users, see "Internal Administration of Users" on page 233.

Using Database Authentication with MS SQL Server

When you install the Siebel Server, an ODBC data source name (DSN) is created which the Siebel Server uses to connect to the Siebel database. If you implement database authentication and you are using Siebel Business Applications with a Microsoft SQL Server database, ensure that you select the correct ODBC DSN configuration settings; if you do not, Siebel Web clients can log in to Siebel Business Applications without providing a password.

When you configure the ODBC DSN settings for an MS SQL Server database, you can choose from the following authentication options:

- Windows NT authentication using the network login ID

  This option allows users to access applications on the server by entering a network login ID only. If you select this option, Siebel Web clients attempting to access Siebel Business Applications are not required to enter a password.

- SQL Server authentication using a login ID and password entered by the user.

  This option requires users attempting to access applications on the server to enter a valid user ID and password. Select this option to ensure that Siebel Web clients must enter both a Siebel user ID and a password to access Siebel Business Applications.

The following procedure describes how to set the MS SQL Server ODBC data source settings on your Siebel Server.

To set ODBC data source values for MS SQL Server

1. On the Siebel application server, from the Start menu, choose Settings, Control Panel, Administrative Tools, and then the Data Sources (ODBC) option.
2. On the ODBC Data Source Administrator dialog box, select the System DSN tab.
3. Select the Siebel data source name, and click Configure.

   The Microsoft SQL Server DSN Configuration screen appears. The default Siebel data source name (DSN) is *EnterpriseName*_DSN, where *EnterpriseName* is the name you assigned the Siebel Enterprise when you configured it.
4. Make any changes required and click Next.
5. Select an authentication option:

- Windows NT authentication using the network login ID.

  Do not select this option.

- SQL Server authentication using a login ID and password entered by the user.

  Select this option to ensure that Siebel Web clients must enter both a Siebel user ID and a password to access Siebel Business Applications.

6. Amend any other configuration options as required, then click Next.
7. Click Finish.

About LDAP or ADSI Security Adapter Authentication

Siebel Business Applications include security adapters that are based on the LDAP and ADSI standards, allowing customers to use LDAP directory products or Microsoft Active Directory (AD) for user authentication. LDAP or ADSI security adapter authentication can offer the following benefits:

- User authentication external to the database
- Automatic updating of the directory with new or modified user information entered through the Siebel Business Applications user interface by an internal administrator, a delegated administrator, or a self-registering user

Security adapter authentication provides a user with access to the Siebel application for which the security adapter is configured. Different Siebel Business Applications can be configured to use different security adapters.

The process of implementing security adapter authentication is similar for both the LDAP and ADSI security adapters although there are some differences, for example:

- You must install the IBM LDAP Client on the Siebel Server computer if you choose the LDAP security adapter. For more information, see "About Installing LDAP Client Software" on page 122.
- How you configure SSL between the Siebel security adapter and the directory server differs depending on the security adapter you use. For more information, see "Configuring Secure Communications for Security Adapters" on page 166.

For additional information about the LDAP and ADSI security adapters, see:

- "LDAP and ADSI Security Adapter Authentication Process" on page 115
- "Comparison of LDAP and ADSI Security Adapters" on page 116.

LDAP and ADSI Security Adapter Authentication Process

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

1 The user enters credentials to a Siebel Business Applications 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 are passed to the Siebel Web Server Extension (SWSE) and then to the AOM, which in turn passes them to the authentication manager.

2 The authentication manager determines how to process the user credentials and calls the security adapter to validate the credentials against the directory.

3 The security adapter returns the Siebel user ID and a database credential assigned to this user to the authentication manager. (If roles are used, they are also returned to the authentication manager.)

4 The AOM (or other module that requested authentication services) uses the returned credentials to connect the user to the database and to identify the user.

For additional information about LDAP and ADSI security adapter authentication, see "About LDAP or ADSI Security Adapter Authentication" on page 115.

Comparison of LDAP and ADSI Security Adapters

This topic outlines the differences in functionality provided by the LDAP and ADSI security adapters. The relative benefits of each type of security adapter are shown in Table 11 on page 116.

The LDAP security adapter can be used to authenticate against supported LDAP-compliant directories. The LDAP security adapter is also supported for integration to Active Directory and provides most of the functionality offered by the ADSI security adapter. The ADSI security adapter can authenticate against ADSI-compliant directories (Microsoft Active Directory).

For Siebel CRM release 8.0 and higher, it is recommended that you use the LDAP security adapter for authenticating against both Active Directory and LDAP-based external directories.

Table 11. Comparison of LDAP and ADSI Security Adapter Functionality

Functionality	LDAP Security Adapter	LDAP Security Adapter with AD Directory	ADSI Security Adapter
Shared database account credentials can be stored as security adapter profile parameters eliminating the necessity for a shared credentials user record in the external directory.	Yes	Yes	No
Password expiration warning	No	No	Yes

Table 11. Comparison of LDAP and ADSI Security Adapter Functionality

Functionality	LDAP Security Adapter	LDAP Security Adapter with AD Directory	ADSI Security Adapter
Administration of the directory through Siebel Business Applications (manage user passwords or create new users) **NOTE:** In large implementations, timeout issues can occur, particularly if using the ADSI security adapter.	Yes	Yes, provided that SSL is enabled between the LDAP security adapter and the Active Directory server.	Yes, provided that the Active Directory client can establish a secure connection to the Active Directory server. This can be achieved by: ■ Including all systems as part of a single Microsoft Windows domain forest ■ By configuring SSL
Communication with more than one directory server.	See "Communicating With More Than One Authentication Server" on page 117.		

For additional information about LDAP and ADSI security adapter authentication, see "About LDAP or ADSI Security Adapter Authentication" on page 115.

Using the LDAP Security Adapter With Active Directory: Setting the Base DN

If you use the LDAP security adapter with Active Directory, problems can occur if you set the base distinguished name (Base DN), which specifies the root directory under which users are stored, to the root level of the Active Directory.

When the LDAP security adapter searches the Active Directory, it searches everything under the Base DN. If the Base DN is set to the Active Directory root, the LDAP security adapter searches all directory entities, including configuration and schema entities to which the application user does not have access, resulting in problems occurring. To avoid these problems, do not set the base DN to the Active Directory root directory; this recommendation also applies to implementations in which the ADSI security adapter performs the authentication function.

Communicating With More Than One Authentication Server

This topic describes the specific circumstances in which the LDAP and ADSI security adapters can connect to more than one directory server, either to authenticate users in more than one directory, or for failover purposes.

ADSI Security Adapter

The ADSI security adapter does not support authentication of users in different domains or forests and does not support Microsoft Global Catalog functionality. However, the ADSI security adapter can connect to multiple AD servers for authentication or failover purposes provided that the following conditions are met:

- The Active Directory servers are all in the same domain
- The Siebel Enterprise is in the same domain as the Active Directory servers

To enable the ADSI security adapter to connect to multiple AD servers, specify the NetBIOS name of the domain containing the Active Directory servers, instead of the name of a specific Active Directory server, for the Server Name parameter of the ADSI security adapter profile.

LDAP Security Adapter

The LDAP security adapter provided with Siebel Business Applications currently does not support communication with more than one directory server. However, the following options are available:

- Failover functionality can be implemented to a limited degree for the LDAP security adapter. To implement failover functionality, specify the names of the primary and secondary servers for the Server Name parameter of the LDAP security adapter profile. For example:

  ```
  ServerName=ldap1 ldap2
  ```

  If communication cannot be established between the Siebel AOM and the primary LDAP server, failover to the secondary LDAP server occurs. If the AOM can communicate with the primary server, but LDAP functionality on the server is not available, failover to the secondary server does not occur.

- Oracle provides products, for example, Oracle Virtual Directory, that enable LDAP security adapters to communicate with multiple LDAP-compliant directories and Active Directory directories. For additional information on Oracle Virtual Directory, go to

  http://www.oracle.com/technetwork/testcontent/index-093158.html

Requirements for the LDAP or ADSI Directory

If you implement LDAP or ADSI security adapter authentication with Siebel Business Applications, you must provide a directory product that meets the requirements outlined in this topic.

The directory product you provide can be one of the directory servers supported by the security adapters provided with Siebel Business Applications, or another directory of your choice. The following options are available:

- If you provide one of the directory servers supported by Siebel Business Applications (that is, a supported LDAP directory or Microsoft Active Directory), then you can use a security adapter provided by Siebel Business Applications, or you can create your own security adapter that complies with Siebel Business Applications.

- If you provide a directory other than those supported by the security adapters provided with Siebel Business Applications, then you are responsible for implementing a security adapter that supports this directory.
- For specific information about third-party products supported by Siebel Business Applications, see *Siebel System Requirements and Supported Platforms* on Oracle Technology Network.

About Setting Up the LDAP or ADSI Directory

To provide user access to a Siebel application implementing an LDAP or ADSI security adapter, the Siebel application must be able to retrieve credentials to access the database and the user's Siebel user ID. Therefore you must set up a directory from which a database account and a Siebel user ID can be retrieved for each user.

Your LDAP or ADSI 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.** Specifies the attribute type that stores a database account. This attribute value must be of the form username=*U* password=*P*, where *U* and *P* are credentials for a database account. You can have any amount of white space between the two key-value pairs, but you cannot have any space within each pair. The keywords, username and password, must be lowercase.

  If you use an LDAP directory, you can specify the value for the username and password in a profile parameter for the LDAP Security Adapter profile (alias LDAPSecAdpt) instead of an attribute value for the directory entry. The profile parameters are SharedDBUsername and SharedDBPassword. For more information, see "Configuring the Shared Database Account" on page 167.

  NOTE: When storing database credentials in a directory attribute, both the username and password must be stored as plain text. To avoid having to store database credentials as plain text, it is recommended that you use an LDAP security adapter, and store username and password values as profile parameters.

- **Username.** This attribute value is the key passed to the directory that identifies the user. In a simple implementation, the username might be the Siebel user ID, and so it might not have to be a separate attribute.
- **Password.** The storage of a user's login password differs between LDAP and ADSI directories.
  - **LDAP.** Whether the password is stored in the directory depends on whether you are using Web SSO:
    - ❑ If the user authenticates through the LDAP directory, using the LDAP security adapter, then the login password must be stored in the UserPassword attribute of the LDAP directory.
    - ❑ If the user authenticates through the ADSI directory using the LDAP security adapter, then the login password must be stored in either the UserPassword or the unicodePWD attribute of the LDAP directory, depending on the code page used by the directory server.

  - If the user is authenticated by an authentication service, such as in a Web SSO implementation, a password attribute is not required.

  The Password Attribute Type parameter is used to specify the attribute type under which the user's login password is stored in the directory. For additional information on the Password Attribute Type parameter, see "Siebel Gateway Name Server Parameters" on page 341.

- **ADSI.** ADSI directories do not store the password as an attribute. The password can be entered at the directory level as a function of the client, or the ADSI security adapter can use ADSI methods to create or modify a password:

  - If the user authenticates through the ADSI directory, using the ADSI security adapter, then the login password must be provided.
  - If the user is authenticated by an authentication service, such as in a Web SSO implementation, a password is not required.

For more information about how to store the user's password, see "Configuring the Shared Database Account" on page 167.

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

If you create a new attribute object for your directory to store Siebel attributes (for example, Siebel User ID), you can use the Private Enterprise Number that Siebel Business Applications has registered with the Internet Assigned Numbers Authority (http://www.iana.org) to provide a unique X.500 Object ID. This number is 1.3.6.1.4.1.3856.*.

An additional type of data, *roles*, is supported, 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 Business Applications. For more information, see "Configuring Roles Defined in the Directory" on page 172.

About Creating the Application User in the Directory

Depending on your authentication and registration strategies and the options that you implement for your deployment, you must define a user, called the application user, in the directory.

The application user is the only user who can read or write user information in the directory. Therefore, it is critical that the application user has appropriate search and write privileges to the directory. For information on creating the application user, see "Configuring the Application User" on page 163.

For ADSI authentication, it is recommended that you use the Active Directory Delegation Control Wizard to define privileges for users in the directory.

NOTE: If you are configuring an ADSI security adapter, ensure that the application user is either a domain user or has access to the directory server. If the application user cannot access the directory server, the authentication process fails.

LDAP Security Adapter Requirements

If you are using LDAP authentication, you must install the IBM LDAP Client software that is provided by Siebel Business Applications. Siebel Business Applications uses DLL files provided by the IBM LDAP Client to communicate with the supported LDAP directory server product you have chosen to use. If the IBM LDAP Client is not yet installed, then you must manually install it.

For IBM LDAP Client installation instructions, see "About Installing LDAP Client Software" on page 122.

ADSI Security Adapter Requirements

If you are running the Siebel Server in supported Microsoft Windows environments, and you are using ADSI authentication, you must meet the requirements described in this topic. For more information about some of these requirements, see your Microsoft Active Directory documentation.

NOTE: Siebel Business Applications do not support Microsoft Global Catalog functionality.

These requirements are:

- To allow users to set or change passwords, the ADSI client software must be able to establish a secure connection to the Active Directory server. This requirement can be met in multiple ways:

  - Including all systems as part of a single Microsoft Windows domain forest

    It is recommended that all Siebel Servers and Active Directory servers are located in the same domain forest.

  - Configuring Secure Sockets Layer (SSL)

    To perform user management in the Active Directory through the Siebel client, you must configure the Active Directory server 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 Business Applications.

- DNS servers on your network must be properly configured with DNS entries for the Active Directory. Client computers using the ADSI security adapter must be configured to be able to retrieve these entries from the appropriate DNS servers.

- If you require ADSI security adapter functionality for Siebel Developer Web Client deployments, you must install the ADSI client software on each such client computer, where applicable.

  For more information about Active Directory client issues, search Microsoft's Web site for information about Active Directory Client Extensions.

Verifying the Active Directory Client Installation

The following procedure describes how to verify that the Active Directory client is successfully installed.

To verify an Active Directory client installation

1. Navigate to the system32 subdirectory of the installation location for the Microsoft Windows operating system (for example, `C:\WINDOWS\system32`).

2. Verify that the correct versions of each DLL required for the Active Directory client are present in the subdirectory (for example, the files adsiis.dll and adsiisex.dll). For more information, see Microsoft's documentation.
3. For each DLL, right-click on the file and choose Properties.
4. Click the Version tab to see the version number.

About Installing LDAP Client Software

You must install the IBM LDAP Client and IBM GSKit software if you implement LDAP security adapter authentication. The IBM LDAP Client allows Siebel Business Applications to authenticate against supported LDAP directory servers, when used with the LDAP security adapter. The IBM GSKit, optionally installed with IBM LDAP Client, enables Siebel Business Applications to communicate with supported LDAP directory servers over SSL.

Consider the following requirements for the IBM LDAP Client installation into a Siebel environment:

- The IBM LDAP Client must be installed on each Siebel Server computer for which LDAP authentication is to be supported using the LDAP security adapter. The IBM LDAP Client software can be installed either before or after you install the Siebel Server.
- For Siebel Developer Web Client deployments for which LDAP authentication is to be supported, the IBM LDAP Client must be installed on each local client computer. The IBM LDAP Client software can be installed either before or after you install the Siebel Developer Web Client.
- The IBM GSKit must be installed if you are supporting SSL. The IBM GSKit is a utility you use to generate Certificate Management Services (CMS) key databases which are required for Siebel Business Applications to communicate with LDAP directory servers over SSL. IBM GSKit can be installed on any computer using a supported operating system. If you require this module, you only have to install it once for each deployment.

The IBM LDAP Client and GSKit software are available from the Siebel network image directory. For information about creating a Siebel network image directory, see the *Siebel Installation Guide* for the operating system you are using. For information about supported version numbers for the IBM LDAP Client and GSKit software, see *Siebel System Requirements and Supported Platforms* on Oracle Technology Network. Also see your vendor documentation.

Process of Installing and Configuring LDAP Client Software

This topic outlines the steps involved in installing and configuring the IBM LDAP Client and IBM GSKit. To install the LDAP Client software, and to configure it for your environment, perform the following tasks:

- Review "Considerations for Secure LDAP Using SSL" on page 123
- Perform one of the following tasks, as appropriate:
  - "Installing the IBM LDAP Client and IBM GSKit on Windows" on page 123
  - "Installing the IBM LDAP Client and IBM GSKit on Oracle Solaris" on page 124

  - "Installing the IBM LDAP Client and IBM GSKit on AIX" on page 126
  - "Installing the IBM LDAP Client and IBM GSKit on HP-UX" on page 127
  - "Installing the IBM LDAP Client and IBM GSKit on Linux" on page 127
- (UNIX only) "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 128
- (Optional) "Configuring the IBM GSKit" on page 130
- (Optional) "Generating a CMS Key Database Using IBM GSKit" on page 131

Considerations for Secure LDAP Using SSL

This topic provides information on using LDAP authentication with SSL. The IBM LDAP Client requires that IBM GSKit be installed, if SSL must be supported. The LDAP libraries and utilities provided with the LDAP Client use the SSL libraries, if present. The SSL libraries are provided with IBM GSKit.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

NOTE: When you use the LDAP security adapter to authenticate users against Active Directory, you must configure SSL between the LDAP security adapter and Active Directory if you want to manage user passwords or create new users in the Active Directory.

- If IBM GSKit has been installed, the LDAP libraries dynamically load the SSL libraries and use them to enable support for SSL, when SSL is configured.
- If IBM GSKit has not been installed and the SSL libraries are not available, the LDAP library is fully functional, with the exception of SSL support.

By using SSL with server authentication, an LDAP application can use simple LDAP authentication (user ID and password) over a secure, encrypted communication connection. SSL provides for the establishment of a secure connection between the LDAP client application and the LDAP server. In addition, SSL provides data confidentiality (encryption) on connections protected by SSL. Authentication of servers to clients is accomplished with X.509 certificates.

These installation instructions assume that SSL capability is, or will be, required for Siebel LDAP authentication. Therefore, the LDAP client installation process includes IBM GSKit installation as an integral part. If you are absolutely sure that SSL will never be turned on for Siebel LDAP authentication, you do not have to install IBM GSKit.

Installing the IBM LDAP Client and IBM GSKit on Windows

This topic describes how to obtain the IBM LDAP Client and IBM GSKit installation files on Microsoft Windows.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

To obtain IBM LDAP Client and IBM GSKit installation files on Windows

1. Navigate within the Siebel network image to the following directory:

   Release\Windows\Server_Ancillary\IBM_LDAP_6.0_Client\enu

2. Unzip the file itds60-client-win-ia32-ismp.zip.
3. Install and configure the IBM LDAP Client and IBM GSKit as described in the IBM documentation.

   NOTE: The installer refers to the IBM LDAP Client as *Client SDK 6.0* and IBM GSKit as *GSKit*.

4. Stop and restart the Siebel Server.

Installing the IBM LDAP Client and IBM GSKit on Oracle Solaris

This topic describes how to install the IBM LDAP Client and IBM GSKit on Oracle Solaris. Before installing the IBM LDAP Client and GSKit, you must relocate any non-IBM LDAP files that exist on Oracle Solaris; this task is also described in this topic.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

Relocating Non-IBM LDAP Files on Your System

LDAP files are included in most Oracle Solaris installations and, if they exist, they must be moved from the /usr/bin/ directory before the IBM LDAP Client files can be installed. You can relocate the Oracle Solaris LDAP files either before or during the IBM Client and GSKit installation. Each method is described in this topic.

To relocate the Oracle Solaris LDAP files before you begin to install the IBM LDAP files, use the following procedure.

To relocate the Oracle Solaris LDAP files on your system

1. Locate the Oracle Solaris LDAP files by entering the following command:

   ```
   ls -al |grep ldap
   ```

2. Move the files you locate from `/usr/bin` to a directory of your choice, for example, `/usr/bin/ldapsparc`.
3. Proceed to install the IBM LDAP Client and GSKit.

If you do not relocate the Oracle Solaris LDAP files before you begin to install the LDAP Client and GSKit, you can relocate them during the LDAP Client installation, as described in the following procedure.

To relocate the Oracle Solaris LDAP files during the IBM LDAP Client and GSKit installation

1 If non-IBM LDAP files are detected during the IBM LDAP Client installation, the following message is displayed:

```
A non-IBM version of LDAP has been located on your system.
In order to use the command-line version of the IBM-supplied files, the existing
files (ldapadd, ldapdelete, ldaplist, ldapmodify, ldapmodrdn, ldapsearch) must be
relocated.

(/usr/bin/ldapsparc) [?,q]
```

Specify the name of the directory where you want to move the non-IBM LDAP files by doing one of the following:

- Press Enter to accept the default directory, /usr/bin/ldapsparc
- Type a different directory path name, and press Enter

  Alternatively, type q and press Enter to quit.

2 After relocating the files, a number of messages are displayed and then the following prompt appears:

```
Do you want to install these conflicting files [y,n,?,q]
```

Type y and press Enter to continue the installation of the IBM LDAP files.

The existing Oracle Solaris LDAP files are moved to the directory you specified in Step 1 on page 125 and the IBM LDAP Client files are installed in the /usr/bin directory.

Installing the IBM LDAP Client and GSKit Installation Files on Oracle Solaris

The following procedure describes how to install the IBM LDAP Client and GSKit.

To obtain IBM LDAP Client and IBM GSKit installation files on Oracle Solaris

1 Login as root.

2 Navigate within the Siebel network image to the directory Solaris/Server_Ancillary/IBM_LDAP_6.0_Client/enu.

This directory contains two files:

- itds60-client-sol-sparc-ismp.tar

  Choose this file if you want to use an installation wizard to install the IBM LDAP Client and IBM GSKit.

- itds60-client-sol-sparc-native.tar

  Choose this file if you want to install the IBM LDAP Client and IBM GSKit using the command line.

3 Copy one of the files described in Step 2 to an empty directory that has at least 50 MB of available space.

4 Enter the following command:

```
tar -xvf nameOfSelectedFile.tar
```

The directory *nameOfSelectedFile* is created at the current location and the IBM LDAP Client and IBM GSKit files are unpacked and installed into it.

5 Add the directory path of the IBM LDAP 6.0 libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) script file. For information on this task, see "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 128.

6 Stop and restart the Siebel Server.

Installing the IBM LDAP Client and IBM GSKit on AIX

This topic describes how to obtain the IBM LDAP Client and IBM GSKit installation files on AIX.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

To obtain IBM LDAP Client and IBM GSKit installation files on AIX

1 Log in as root.

2 Navigate to the directory that contains the folder AIX/Server_Ancillary/IBM_LDAP_6.0_Client/enu.

This directory contains two files:

- itds60-client-aix-ppc-ismp.tar

  Choose this file if you want to use an installation wizard to install the IBM LDAP Client and IBM GSKit.

- itds60-client-aix-ppc-native.tar

  Choose this file if you want to install the IBM LDAP Client and IBM GSKit using the command line.

3 Copy one of the files described in Step 2 to an empty directory that has at least 50 MB of available space.

4 Enter the following command:

```
tar -xvf nameOfSelectedFile.tar
```

The directory *nameOfSelectedFile* is created at the current location and the IBM LDAP Client and IBM GSKit files are unpacked and installed into it.

5 Add the directory path of the IBM LDAP 6.0 libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) script file. For information on this task, see "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 128.

6 Stop and restart the Siebel Server.

Installing the IBM LDAP Client and IBM GSKit on HP-UX

This topic describes how to obtain the IBM LDAP Client and IBM GSKit installation files on HP-UX.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

To obtain IBM LDAP Client and IBM GSKit installation files on HP-UX

1 Log in as root.

2 Navigate to the directory that contains the folder `HPUX/Server_Ancillary/IBM_LDAP_6.0_Client/enu`.

   This directory contains two files:

   - aus60ldap_051007_ia64_hpux_11_so.tar

     This file contains the installation files required to install the IBM LDAP Client.

   - gsk7bas32.tar

     This file contains the installation files required to install the IBM GSKit.

3 If you intend to deploy SSL, copy both of the files described in Step 2 to an empty directory that has at least 50 MB of available space. If you only require the IBM LDAP Client, copy aus60ldap_051007_ia64_hpux_11_so.tar to an empty directory.

4 For each file you copied, enter the following command:

```
tar -xvf nameOfSelectedFile.tar
```

   The directory *nameOfSelectedFile* is created at the current location and the IBM LDAP Client and IBM GSKit files are unpacked and installed into it.

5 Add the directory path of the IBM LDAP 6.0 libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) script file. For information on this task, see "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 128.

6 Stop and restart the Siebel Server.

Installing the IBM LDAP Client and IBM GSKit on Linux

This topic describes how to obtain the IBM LDAP Client and IBM GSKit installation files on Linux.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

To obtain IBM LDAP Client and IBM GSKit installation files on Linux

1. Log in as root.
2. Navigate to the directory that contains the folder Linux/Server_Ancillary/IBM_LDAP_6.0_Client/enu.

   This directory contains two files:

   - itds60-client-lin-ia32-ismp.tar

     Choose this file if you want to use an installation wizard to install the IBM LDAP Client and IBM GSKit.

   - itds60-client-lin-ia32-native.tar

     Choose this file if you want to install the IBM LDAP Client and IBM GSKit using the command line.

3. Copy one of the files described in Step 2 to an empty directory that has at least 50 MB of available space.
4. Enter the following command:

   ```
   tar -xvf nameOfSelectedFile.tar
   ```

   The directory *nameOfSelectedFile* is created at the current location and the IBM LDAP Client and IBM GSKit files are unpacked and installed into it.

5. When you have installed and configured the LDAP Client, add the directory path of the IBM LDAP 6.0 libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) script file. For information on this task, see "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 128.
6. Stop and restart the Siebel Server.

Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client

After you have installed the IBM LDAP Client on your UNIX operating system, you must add the directory path of the IBM LDAP 6.0 libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) shell scripts. When you source these scripts, they set the environment variables for your Siebel implementation.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

The siebenv.csh and siebenv.sh scripts are created in the $SIEBEL_ROOT directory during the Siebel Server installation and configuration process. Edit the siebenv.csh or siebenv.sh script, as described in the following topics, replacing the directory `/opt/ibm/ldap/v6.0/lib` with the installation path of your IBM LDAP Client libraries, if you installed into a different directory.

NOTE: Siebel supports only the IBM 32-bit LDAP Client so you can use only the 32-bit LDAP Client libraries with Siebel Business Applications.

Linux and Oracle Solaris Operating Systems

On Linux and Oracle Solaris operating systems, the name of the library path environment variable is LD_LIBRARY_PATH. Depending on whether you source the siebenv.csh or the siebenv.sh script, set the LD_LIBRARY_PATH variable as follows:

- siebenv.csh

```
if ($?LD_LIBRARY_PATH) then
setenv LD_LIBRARY_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${LD_LIBRARY_PATH}
else
setenv LD_LIBRARY_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
endif
```

- siebenv.sh

```
if [ a${LD_LIBRARY_PATH} = ${LD_LIBRARY_PATH}a ]
then
LD_LIBRARY_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/
v6.0/lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
else
LD_LIBRARY_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/
v6.0/lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${LD_LIBRARY_PATH}
fi
export LD_LIBRARY_PATH
```

AIX Operating System

On the AIX operating system, the name of the library path environment variable is LIBPATH. Depending on whether you source the siebenv.csh or the siebenv.sh script, set the LIBPATH variable as follows:

- siebenv.csh

```
if ($?LIBPATH) then
setenv LIBPATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${LIBPATH}
else
setenv LIBPATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
endif
```

- siebenv.sh

```
if [ a${LIBPATH} = ${LIBPATH}a ]
then
LIBPATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
else
LIBPATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
```

```
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${LIBPATH}
fi
export LIBPATH
```

HP-UX Operating System

On the HP-UX operating system, the name of the library path environment variable is SHLIB_PATH. Depending on whether you source the siebenv.csh or the siebenv.sh script, set the SHLIB_PATH variable as follows:

- siebenv.csh

```
if ($?SHLIB_PATH) then
setenv SHLIB_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${SHLIB_PATH}
else
setenv SHLIB_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
endif
```

- siebenv.sh

```
if [ a${SHLIB_PATH} = ${SHLIB_PATH}a ]
then
SHLIB_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
else
SHLIB_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/opt/ibm/ldap/v6.0/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${SHLIB_PATH}
fi
export SHLIB_PATH
```

Configuring the IBM GSKit

This topic provides information about configuration steps you must take to enable the Certificate Management Services (CMS) capability before you use the IBM GSKit.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

To set up IBM GSKit to support CMS key databases

1. Install the IBM JDK 1.4.1 or 1.4.2, or an equivalent JDK.
2. Set JAVA_HOME to point to the directory where the JDK is installed. For example:
   - (Windows) JAVA_HOME=C:\Program Files\IBM\Java14
   - (UNIX) export JAVA_HOME=/usr/opt/IBMJava14
3. Remove the ibmjsse.jar, gskikm.jar (if it exists) and ibmjcaprovider.jar files from your ${JAVA_HOME}/jre/lib/ext directory.

4 Be sure that ${JAVA_HOME}/jre/lib/ has the following jar files:

- ext/ibmjceprovider.jar
- ext/ibmpkcs.jar
- ibmjcefw.jar
- security/local_policy.jar
- security/US_export_policy.jar
- ibmpkcs11.jar

IBM GSKit includes the above jar files, and ibmjsse.jar, in the GSKit installation path. The files are located at *GSK_installation_directory*\classes\jre\lib\ext. Copy the GSKit jar files to ${JAVA_HOME}/jre/lib/ext.

JDK 1.4 requires the user to have jurisdiction policy files. Due to the import restrictions for some countries, the jurisdiction policy files distributed with the J2SDK version 1.4.1 software have built-in restrictions on the available cryptographic strength. The Oracle Solaris JDK and many other installations require jurisdiction policy files that contain no restrictions on cryptographic strength.

For more information about jurisdiction policy files, go to

http://www.oracle.com/technetwork/java/javase

5 Register IBM JCE and IBM CMS service providers.

Update the ${JAVA_HOME}/jre/lib/security/java.security file to add the IBM JCE provider and IBM CMS provider after the Sun provider. For example:

```
security.provider.1=sun.security.provider.Sun

security.provider.2=com.ibm.spi.IBMCMSProvider

security.provider.3=com.ibm.crypto.provider.IBMJCE
```

A sample java.security file for GSKit users is located in *GSK_installation_directory*\classes\gsk_java.security.

Generating a CMS Key Database Using IBM GSKit

This topic describes how to generate a Cryptographic Message Syntax (CMS) key database using the IBM GSKit. Before you attempt this task, make sure that you carry out the tasks described in "Configuring the IBM GSKit" on page 130.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 122.

By enabling SSL for the Siebel LDAP security adapter, a secure connection is established between the Siebel application and its LDAP server. For information on enabling SSL for an LDAP server, see your third-party LDAP server administration documentation. This topic assumes that the LDAP server is already SSL-enabled—that is, it accepts SSL connections.

To enable SSL for the Siebel LDAP security adapter, a certificate database file must be installed on the Siebel Server computer where AOMs or other components run that must support LDAP authentication through the LDAP security adapter. The LDAP security adapter must connect to the LDAP server using a port that accepts SSL connections.

The Siebel LDAP security adapter is built on top of the IBM LDAP Client. The IBM LDAP Client requires that the certificate database file uses the CMS key database format. You can generate a CMS key database using IBM GSKit.

The rest of this topic provides detailed instructions for generating a CMS key database and enabling SSL for the Siebel LDAP security adapter.

Generating a CMS Key Database

The CMS key database must contain CA certificates of those Certificate Authorities that have issued server certificates to LDAP servers.

For example, assume that the Siebel Server is configured to authenticate against LDAP server LDAPserver1:392. The server certificate for this LDAP server is issued by the certificate server evlab1. Therefore, the CMS key database only has to contain a CA certificate for CERTserver1. It does not have to contain a server certificate for LDAPserver1. If the Siebel Server is configured to authenticate against another LDAP server that gets its server certificate from CERTserver1, you do not have to update the CMS key database.

After installing and configuring the IBM GSKit on your computer, use the following procedure to configure IBM GSKit to support CMS key databases, and to generate a CMS key database.

To configure IBM GSKit to support CMS key databases

1. Determine which CA issued the server certificate for your LDAP server and obtain this CA certificate.
2. Copy the CA certificate to the computer where you have installed IBM GSKit.
3. Create a new CMS key database using iKeyMan.

   a. Navigate to *GSK_installation_directory*/bin, where *GSK_installation_directory* is the directory where you installed both IBM GSKit and IBM GSKit.

   b. Enter the following command:

   ```
   gsk7ikm
   ```

   c. To create a new CMS key database, select New from the Key Database File menu.

   d. In the dialog box, specify the key database type as CMS, and specify the file name (using file extension .kdb) and specify the location where you intend to store your CMS key database. Click OK.

   NOTE: The CMS key database must be located on a local drive, not on a network-attached storage device or other remote volume.

e. In the Password Prompt dialog box, enter and confirm the password, and check the option Stash the password to a file. Click OK.

   You must select the Stash password to a file option for the Siebel LDAP security adapter to work correctly with SSL.The stash password option creates a file with the same name as the CMS key database, but with the extension .sth. The file is created at the same location as the CMS key database. For example, ldapkey.sth is created if your CMS key database is named ldapkey.kdb.

f. Click OK to confirm the creation of the .sth file.

   The newly created CMS key database opens in the iKeyMan main window.

4. Add one or more CA certificates to the CMS key database created in the previous step.

   a. At the Signer Certificates prompt, click Add.

   b. In the dialog box named Add CA's certificate from a file, specify the data type, and specify the certificate file name and the location where you intend to store your file. Use the Browse button, as necessary, to specify the location of the CA certificate file. Click OK.

      - If the certificate was saved in Base64 format, specify the data type Base-64 encoded ASCII data.

      - If the certificate was saved in DER binary format, specify the data type DER binary data.

   c. Repeat the previous substep for each CA certificate you want to add into the CMS key database. Make sure that you select the correct data type.

NOTE: For LDAP servers that have their server certificate issued from a new CA, just add the CA certificate to the CMS key database, instead of creating a new CMS key database for every LDAP server.

Enabling SSL for Siebel LDAP Security Adapter

Use the procedure below to configure SSL for the Siebel LDAP security adapter. For more information about LDAP security adapter configuration, see "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

To enable SSL for the Siebel LDAP security adapter

1. Copy the ldapkey.kdb (the CMS key database) and ldapkey.sth files you just created in "Generating a CMS Key Database" on page 132 to the Siebel Server computer where you will run the AOM components that support LDAP authentication.

   For example, you might copy these files to the directory \ssldb.

2. Modify the LDAP security adapter configuration. Configure the following parameters:

   - port = 636

     The SSL port is configurable for the LDAP server. Verify the actual port number the LDAP server is using for SSL.

   - ssldatabase = *CMS_file_path*

     Specify the absolute path to the CMS key database, such as `d:\ssldb\ldapkey.kdb`.

3 Restart the Siebel Server (if you are configuring LDAP on a Siebel Server).

Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard

This topic describes how to configure the LDAP or ADSI security adapters provided with Siebel Business Applications using the Siebel Configuration Wizard. Alternatively, you can configure the security adapter settings by setting Gateway Name Server parameters directly using Server Manager. When you configure Siebel Gateway Name Server parameters, the Siebel Gateway Name Server must be running.

NOTE: When configuring a Siebel Developer Web Client, you configure authentication parameters stored in the Siebel application configuration file.

The Siebel Enterprise is configured to use database authentication by default. When you specify LDAP or ADSI as the security adapter type using the Configuration Wizard, the setting you make provides the value for the Security Adapter Mode (SecAdptMode) parameter, however, to enable LDAP or ADSI authentication, you must also manually change the SecAdptName and SecAdptMode parameters using Server Manager. When you specify LDAP or ADSI as the security adapter mode, additional configuration parameters are defined for the particular LDAP or ADSI security adapter. For example, the Security Adapter DLL Name (SecAdptDllName) parameter is automatically set when you specify LDAP or ADSI as the security adapter mode.

The Security Adapter Mode and Security Adapter Name parameters can be set for the Siebel Enterprise Server, for a particular Siebel Server, for an individual AOM component, or for the Synchronization Manager component (for Siebel Remote).

CAUTION: If you want to configure a server component or a Siebel Server to use different LDAP or ADSI authentication settings than those already configured at a higher level (that is, configured for the Siebel Enterprise or Siebel Server), you must create a new LDAP or ADSI security adapter. Otherwise, the settings you make reconfigure the existing security adapter wherever it is used.

The Siebel Configuration Wizard sets authentication-related configuration parameters for Siebel Business Applications authentication, but does not make changes to the LDAP or ADSI directory. Make sure the configuration information you enter is compatible with your directory server.

The following procedure describes how to run the Siebel Configuration Wizard to configure the LDAP or ADSI security adapters provided with Siebel Business Applications.

To configure your LDAP or ADSI security adapter

1 Launch the Siebel Configuration Wizard and navigate to the Enterprise Security Authentication Profile screen.

  For details about launching the wizard, see the *Siebel Installation Guide* for the operating system you are using.

2 Choose the authentication type that corresponds to the security adapter you want to implement, and click Next.

- Select LDAP Authentication to implement the LDAP security adapter.
- Select ADSI Authentication to implement the ADSI security adapter.

Enter values for the various parameters that the Configuration Wizard presents to you as described in the following steps. The screens that the Configuration Wizard presents depends on the authentication type you selected in Step 2.

3. Enter information pertaining to the security adapter and the use of checksum validation:

   - **Security Adapter Name (named subsystem).** Specify the name of the security adapter. The setting you make provides a value for the Security Adapter Name parameter. You can accept the default name, or specify a nondefault name. If an enterprise profile (named subsystem) does not already exist with the name you specify, the Siebel Configuration Wizard creates a new enterprise profile using that name. The default names are:

     - For LDAP, the default name is LDAPSecAdpt.
     - For ADSI, the deafly name is ADSISecAdpt.

   - **Security Authentication Library CRC Checksum.** Specify whether you want to use checksum validation for the security adapter DLL file. Corresponds to the CRC parameter.

     If you do not want to use checksum validation, enter 0. Otherwise, enter the value that you generate as described in "Configuring Checksum Validation" on page 165.

4. **Directory Server Domain Name.** Corresponds to the ServerName parameter.

   Specifies the name of the computer on which the LDAP or ADSI directory server runs. You must specify the fully qualified domain name of the LDAP directory server, not just the domain name. For example, specify `ldapserver.oracle.com`, not `oracle.com`.

   For ADSI, if SSL is configured between the Siebel Server and the directory server, you must specify the fully qualified domain name of the directory server. If the Siebel Server and directory server are in the same domain, you can specify the directory server's complete computer name or its IP address.

5. **Port Number** (*LDAP only*)**.** The port number used by the LDAP directory server. Use port 389 (the default) for standard transmission, or port 636 for secure transmission. Corresponds to the `Port` parameter.

   The ADSI directory server port is set as part of the directory installation, not as a configuration parameter.

6. Enter configuration information pertaining to attribute mapping:

   - **Siebel Username Attribute.** The Siebel user ID attribute used by the directory. An example entry for an LDAP directory is `uid`. An example entry for ADSI is `sAMAccountName` (maximum length 20 characters). If your directory uses a different attribute for the Siebel user ID, enter that attribute instead. Corresponds to the UsernameAttributeType parameter.
   - **Siebel Password Attribute** (*LDAP only*)**.** The password for the Siebel user ID attribute used by the directory. Corresponds to the PasswordAttributeType parameter.

7 Enter additional configuration information pertaining to attribute mapping:

- **Database Account Attribute.** The database credentials attribute type used by the directory. For LDAP and ADSI, an example entry is dbaccount. If your directory uses a different attribute for the database account, enter that attribute instead. Corresponds to the CredentialsAttributeType parameter. Configuring the shared database account requires you to have defined the database account attribute.

  If you use LDAP, you can choose to specify the database credentials as server parameters rather than as attributes of a directory entry. For more details on this option and on how to store database credentials as attributes of a directory entry, see "Configuring the Shared Database Account" on page 167.

- **LDAP Roles Attribute.** The attribute type for roles stored in the directory. This setting is required only if you use roles in your directory. Corresponds to the RolesAttributeType parameter.

  For more information, see "Configuring Roles Defined in the Directory" on page 172.

- **Shared Database Account Distinguished Name (DN).** Specify the full DN for the shared database account stored in the directory. Corresponds to the SharedCredentialsDN parameter.

  Configuring the shared database account also uses the database account attribute you defined in Database Account Attribute.

  If you use an LDAP directory server, you can, as an alternative, specify the database credentials as profile parameters. For more information on this option, see Step 8.

8 **Cache shared database user credentials.** Choose the appropriate action:

- Select the check box Cache shared database user credentials if you want to store the database credentials for the shared database account as profile parameters for the LDAP Security Adapter profile (alias LDAPSecAdpt) instead of directory attributes. Proceed to Step 9.

- Leave the check box clear if you want to store each user's database account credentials in an attribute of that user's record in the directory. Proceed to Step 10.

9 **Shared Database Account.** Specify the shared database account user name and password.

For more information on the shared database account, see "Configuring the Shared Database Account" on page 167.

10. Configure the application user:

    - **Application User Distinguished Name (DN).** The full DN (distinguished name) for the application user stored in the directory. Corresponds to the ApplicationUser parameter.

      In addition to defining the application user here, you must also create the application user in the LDAP or ADSI directory. For more information, see "Configuring the Application User" on page 163.

      NOTE: If you are configuring an ADSI security adapter, ensure that the application user is either a domain user or has access to the directory server. If the application user cannot access the directory server, the authentication process fails.

      In addition to defining the application user here, you must also create the application user in the LDAP or ADSI directory. For more information, see "Configuring the Application User" on page 163.

    - **Application Password.** The password for the application user stored in the directory. Corresponds to the ApplicationPassword parameter. Confirm the password.

11. **Configure Web Single Sign-On (Web SSO).** Specify whether you want to configure Web SSO. Corresponds to the SingleSignOn parameter.

    - If you check Yes, then you must specify the shared secret. Go to Step 12.
    - If you do not check Yes, go to Step 14.

    For more information about configuring Web SSO, see Chapter 7, "Web Single Sign-On Authentication."

12. Enter configuration information pertaining to Web SSO:

    - **Credentials Attribute.** The database credentials attribute type used by the directory. For LDAP and ADSI, an example entry is dbaccount.
    - **User Specification.** The Web server variable which stores the user's identity key.

    Proceed to Step 13.

13. **Shared Secret.** Specify the trust token to use for Web SSO. Corresponds to the TrustToken parameter. The value also corresponds to the TrustToken parameter in the eapps.cfg file on the SWSE.

    You also specify a value for the SSL Database as described in Step 16.

14. **Hash User Password.** Specify whether you want to use password hashing for user passwords. Corresponds to the HashUserPwd parameter.

15. **Hash Database Password.** Specify whether you want to use password hashing for the database credentials password. Corresponds to the HashDBPwd parameter.

    For more information, see "About Password Hashing" on page 157.

16. **SSL Database** (*LDAP only*)**.** To enable Secure Sockets Layer (SSL), provide the location of the ldapkey.kdb file. Corresponds to the SslDatabase parameter.

    For more information, see "Configuring Secure Communications for Security Adapters" on page 166.

17 **Implement Adapter-Defined User Name.** Specify whether you want to implement the adapter-defined user name. Corresponds to the UseAdapterUserName parameter. For more information, see "Configuring Adapter-Defined User Name" on page 169.

- If you check Yes, then you must specify the Siebel User ID attribute. Go to Step 18 on page 138.
- If you do not check Yes, go to Step 19 on page 138.

18 **Siebel User ID Attribute.** Specify the Siebel User ID attribute for the adapter-defined user name. Corresponds to the SiebelUsernameAttributeType parameter.

19 **Base Distinguished Name (DN).** Specify the base distinguished name (DN) in which you are storing your users. Corresponds to the BaseDN parameter.

20 **Propagate Change.** Specify whether you want to configure the ability to propagate changes to the LDAP or ADSI directory from a Siebel Developer Web Client or a Siebel Mobile Web Client. Corresponds to the PropagateChange parameter.

NOTE: If you specify this option, then you must also set the SecThickClientExtAuthent system preference to TRUE.

21 Review the settings and, if satisfied, execute the configuration to apply changes.

22 When the Siebel Configuration Wizard has executed successfully, enable LDAP or ADSI authentication and implement the security adapter settings you have just configured by using Siebel Server Manager to change the SecAdptName and SecAdptMode parameters to specify either LDAP or ADSI. For information on this task, see "Parameters for Enterprise, Siebel Servers, or Components" on page 148.

Process of Implementing LDAP or ADSI Security Adapter Authentication

This topic describes the tasks involved in implementing LDAP or ADSI security adapter authentication.

The process outlined in this topic provides instructions for implementing and testing security adapter authentication for a single Siebel application using either an LDAP or ADSI security adapter with one of the supported directories described in *Siebel System Requirements and Supported Platforms* on Oracle Technology Network. The security adapter authenticates a user's credentials against the directory and retrieves login credentials from the directory. A user is authenticated by the user's Siebel user ID and a password.

You can repeat the appropriate tasks listed in this topic to provide security adapter authentication for additional Siebel Business Applications. You can also implement components and options that are not included in this process. For additional information about security adapter authentication options, see "Security Adapter Deployment Options" on page 163. For information about special considerations in implementing user authentication, see "User Authentication Issues" on page 329.

Implement your authentication architecture in a development environment before deploying it in a production environment.

If you use a security adapter not provided by Siebel Business Applications, it must support the Siebel Security Adapter Software Developers Kit, which is described in "Security Adapter SDK" on page 24. You must adapt the applicable parts of the following task instructions to your security adapter.

You must perform the following tasks to set up and test a typical LDAP or ADSI security adapter authentication architecture:

1. Verify that all requirements are met.

   For information on the requirements, see "Requirements for Implementing an LDAP or ADSI Authentication Environment" on page 140.

2. Review "About Creating a Database Login" on page 140.
3. Set up the attributes for users in the directory. See "Setting Up the LDAP or ADSI Directory" on page 141.
4. Create users in the directory: a regular user, the anonymous user, and the application user. See "Creating Users in the LDAP or ADSI Directory" on page 141.
5. Add user records in the Siebel database corresponding to the users in the directory. See "Adding User Records in the Siebel Database" on page 144.
6. Edit security adapter parameters in the eapps.cfg file. See "Setting Security Adapter Parameters in the SWSE Configuration File (eapps.cfg)" on page 146.
7. Select the security adapter you want to use (LDAP, ADSI, Custom), and configure parameters for the selected security adapter, using one of the following methods:

   - Using the Siebel Configuration Wizard

     Configure values for the security adapter parameters by running the Siebel Configuration Wizard. Then select the security adapter you want to use (LDAP, ADSI, Custom) by specifying the appropriate values for the SecAdptName and SecAdptMode Siebel Gateway Name Server parameters using either Siebel Server Manager or by running the Siebel Configuration Wizard again.

     For information on running the Siebel Configuration Wizard, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 134.

   - Editing Siebel Gateway Name Server parameters directly

     You can select the security adapter you want to use, and configure Gateway Name Server parameters for the security adapter, by editing Siebel Gateway Name Server parameters directly using Siebel Server Manager. For further information, see "Configuring Security Adapter Gateway Name Server Parameters" on page 147.

   - (Developer Web Clients only) Editing the application configuration file

     For Developer Web Clients only, you configure parameters for the security adapter in the application configuration file. For additional information, see "Configuring LDAP or ADSI Authentication for Developer Web Clients" on page 152.

8. (Developer Web Clients only) "Setting a System Preference for Developer Web Clients" on page 153.
9. "Restarting Servers" on page 154.

10 "Testing the LDAP or ADSI Authentication System" on page 154.

Requirements for Implementing an LDAP or ADSI Authentication Environment

This topic describes the requirements for implementing an LDAP or ADSI authentication environment. The Siebel default authentication method is database authentication; if you want to implement LDAP or ADSI authentication instead, ensure that the requirements outlined in this topic are in place.

This task is step in"Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

You must complete the following tasks before you can configure an LDAP or ADSI security adapter for your environment:

- Install the Web server.
- Install the LDAP or ADSI directory.
- Install Siebel Business Applications, including the Siebel Gateway Name Server and the Siebel Server.
- Review "Requirements for the LDAP or ADSI Directory" on page 118.

  To implement LDAP or ADSI authentication, you must be experienced with administering the directory. That is, you must be able to perform tasks such as creating and modifying user storage subdirectories, creating attributes, creating users, and providing privileges to users.
- (LDAP only) Install the LDAP client software. For information on this task, see "About Installing LDAP Client Software" on page 122.
- Have available a URL or hyperlink with which users can access the login form for the Siebel application you are configuring.

For information on installing Siebel components, see *Siebel Installation Guide* for the operating system you are using.

About Creating a Database Login

A database login must exist for all users who are authenticated externally. The database login must not be assigned to any real person. A seed database login is provided for this purpose when you install your Siebel Business Applications, as described in Appendix C, "Seed Data." Its login name is LDAPUSER, and its default password is LDAPUSER. Change the default password. If this login name is not present, create it.

This task is step in"Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

Setting Up the LDAP or ADSI Directory

When you implement LDAP or ADSI authentication, users are authenticated through a directory. This topic describes how to setup the directory to do the following:

- Authenticate users through the directory.
- Allows self-registration.
- Uses the Siebel user ID as the username.

NOTE: For more information about setting up the directory, review "Requirements for the LDAP or ADSI Directory" on page 118.

This task is step in"Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

The following procedure describes how to setup the LDAP or ADSI directory.

To setup the LDAP or ADSI directory

1. Determine the Base Distinguished Name, that is, the location in the directory in which users will be stored. For details, see the BaseDN parameter description in "Siebel Gateway Name Server Parameters" on page 341.

   You cannot distribute the users of a single Siebel application in more than one base DN. However, you can store multiple Siebel Business Applications' users in one base DN or in substructures such as organization units (OU), which are used for LDAP.

   For this example, users are stored in the People base DN under the domain level for LDAP directories, or in the Users base DN under the domain level for ADSI directories.

2. Define the attributes to use for the following user data. Create new attributes if you do not want to use existing attributes. Suggested attributes to use are as follows:

   - **Siebel user ID.** Suggested attribute: uid for LDAP, or sAMAccountName for ADSI.
   - **Database account.** Suggested attribute: dbaccount.
   - **Password.** Suggested attribute (*for LDAP only*): userPassword. ADSI does not use an attribute to store a user's password.

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

Creating Users in the LDAP or ADSI Directory

This topic describes the users you have to create in the LDAP or ADSI directory to implement LDAP or ADSI security adapter authentication.

This task is step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

When you use LDAP or ADSI authentication, you must create the following users in the directory:

- Application user

  Make sure the application user has write privileges to the directory, because the security adapter uses application user credentials when using the self-registration component. The application user must also have search privileges for all user records. For additional information, see "Configuring the Application User" on page 163.

- Anonymous user

  You must define an anonymous user even if your application does not allow access by unregistered users. For more information, see"Configuring the Anonymous User" on page 170.

- Records for each user of the Siebel application

  Initially, create a test user to verify the authentication system.

- (Optional) Create a shared credentials user account.

  For more information, see "Configuring the Shared Database Account" on page 167.

  NOTE: If you use an LDAP security adapter, you can also store credentials for the shared database account as profile parameters for the LDAP security adapter.

Create three users in the LDAP or ADSI directory using values similar to those shown in Table 12 on page 143. Specify attribute names, such as uid and userPassword for an LDAP directory, as suggested here. Your entries might vary based on how you assign attributes in "Setting Up the LDAP or ADSI Directory" on page 141.

Table 12. Records in the LDAP or ADSI Directory

Type of User	Siebel User ID Attribute (uid for LDAP or sAMAccountName for Active Directory)	Password (userPassword attribute for LDAP or Active Directory password for AD)	Database Account Attribute (dbaccount)
Anonymous user	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 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	A database account is not required for the anonymous user if a shared database credentials account is implemented; the database credentials for the anonymous user are read from the shared database account user record or the relevant profile parameter of the LDAP security adapter.
Application user	APPUSER or a name of your choice	APPUSERPW or a password of your choice	A database account is not used for the application user.

Table 12. Records in the LDAP or ADSI Directory

Type of User	Siebel User ID Attribute (uid for LDAP or sAMAccountName for Active Directory)	Password (userPassword attribute for LDAP or Active Directory password for AD)	Database Account Attribute (dbaccount)
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 or the shared credentials user account.

Shared database credentials account user	SharedDBUser or a name of your choice
	The user name and password you specify for the shared database account must be a valid Siebel user name and password.
		SharedDBPW or a password of your choice	username=SHAREDDB USER
			password=*P*
			For information about formatting requirements for the database account attribute entry, "About Setting Up the LDAP or ADSI Directory" on page 119.

The example directory entries in Table 12 on page 143 implement 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 SharedDBUser attribute. The database account must match the database account you reserve for externally authenticated users described in "About Creating a Database Login" on page 140. The *P* symbol represents the password in that database account.

Optionally, complete other attribute entries for each user.

Adding User Records in the Siebel Database

This topic describes how to create a record in the Siebel database that corresponds to the test user you create in "Creating Users in the LDAP or ADSI Directory" on page 141.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in Appendix C, "Seed Data." This record must also match the anonymous user you created in "Creating Users in the LDAP or ADSI Directory" on page 141.

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 233.

The following procedure describes how to add user records to the Siebel database.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
2. Navigate to the Administration - User screen, then the Users view.
3. In the Users list, create a new record.
4. Complete the following fields for the test use using values similar to those shown in the following table, then save the record. You can complete other fields, but they are not required.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID Example: *TESTUSER*	Required. This entry must match the uid (LDAP) or sAMAccountName (ADSI) 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 "Seed Users" on page 354.

   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 "Seed Users" on page 354. You can complete other fields, but they are not required.

Setting Security Adapter Parameters in the SWSE Configuration File (eapps.cfg)

This topic describes the parameters you must enter in the SWSE configuration file (eapps.cfg) when you implement LDAP or ADSI security adapter authentication. For information about editing eapps.cfg parameters and about the purposes for the parameters, see "Parameters in the eapps.cfg File" on page 335.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

Enter values for eapps.cfg file parameters using values similar to those shown in Table 13 on page 146. Specify values for AnonUserName and AnonPassword in the defaults section of the eapps.cfg file if you are configuring LDAP or ADSI authentication for all your Siebel Business Applications. If you are implementing LDAP or ADSI authentication for a single application, as in this example, you specify these parameters in the application-specific section of the eapps.cfg file.

Table 13. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
[defaults]	SingleSignOn TrustToken UserSpec UserSpecSource	If these parameters are present, comment out each with a semicolon at the beginning of the line. Do the same if these parameters are present in any other sections.

Table 13. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
The section that is specific to your application, such as one of the following: [/eservice_enu] [/callcenter_enu] where _*enu* is the language code for U.S. English.	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. Whether or not you have to encrypt the password depends on the value specified for the EncryptedPassword parameter. For information on this parameter, see "Managing Encrypted Passwords in the eapps.cfg File" on page 45. Typically, password encryption applies to the eapps.cfg file. In this case, you must specify the encrypted password—unless you provide the password through the Siebel Configuration Wizard.
	ProtectedVirtualDirectory	If this parameter is present, comment it out with a semicolon at the beginning of the line.

Configuring Security Adapter Gateway Name Server Parameters

This topic describes the security-related configuration parameters you use for configuring an LDAP or ADSI security adapter that are defined in the Siebel Gateway Name Server. You can modify Gateway Name Server configuration parameters using Siebel Server Manager, or you can do so using the Siebel Configuration Wizard.

For information on editing Gateway Name Server parameters using the Siebel Configuration Wizard, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 134. For information on using Siebel Server Manager to edit Gateway Name Server parameters, see *Siebel System Administration Guide*.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

You can set Gateway Name Server security adapter parameters for the following:

- "Parameters for Enterprise, Siebel Servers, or Components" on page 148

- "Parameters for AOM Components" on page 149
- "Parameters for Security Adapter (Profile or Named Subsystem)" on page 149

Set security adapter parameters as described in each of these topics. For more information about these parameters, see "Siebel Gateway Name Server Parameters" on page 341.

Parameters for Enterprise, Siebel Servers, or Components

This topic lists security adapter parameters you can set at the Enterprise level, at the Siebel Server level, or at the component level. Applicable components for which you can set these parameters include all AOM components and the Synchronization Manager component (for Siebel Remote).

To implement LDAP or ADSI authentication for a single Siebel application, set the parameters for the applicable AOM component, such as for Siebel Call Center or Siebel eService, using values similar to those shown in Table 14 on page 148.

Table 14. Siebel Gateway Name Server Parameters (for Enterprise, Server, or Component)

Subsystem	Parameter	Guideline
Security Manager	Security Adapter Mode (SecAdptMode)	The security adapter mode to operate in: ■ For LDAP, specify LDAP. ■ For ADSI, specify ADSI.
	Security Adapter Name (SecAdptName)	The name of the security adapter. ■ For LDAP, specify LDAPSecAdpt or another name of your choice. ■ For ADSI, specify ADSISecAdpt or another name of your choice. The name represents the alias for the enterprise profile (named subsystem) for the specified security adapter.

Parameters for AOM Components

This topic lists parameters you set for the AOM component when implementing LDAP or ADSI authentication for a single Siebel application.

To implement LDAP or ADSI authentication for a single Siebel application, set the parameters for the applicable AOM component, such as for Siebel Call Center or Siebel eService, using values similar to those shown in Table 15 on page 149.

Table 15. Siebel Gateway Name Server Parameters (for AOM)

Subsystem	Parameter	Guideline
InfraUIFramework	AllowAnonUsers	Enter TRUE for LDAP or ADSI. You can set this parameter to FALSE if your Siebel application does not use functionality that requires anonymous browsing, such as anonymous catalog browsing or user self-registration.
Object Manager	OM - Proxy Employee (ProxyName)	Enter PROXYE.
	OM - Username BC Field (UsernameBCField)	For this example, leave this parameter empty.

Parameters for Security Adapter (Profile or Named Subsystem)

This topic lists parameters you set for the enterprise profile (named subsystem) for the specific security adapter you are configuring.

To implement LDAP or ADSI authentication for a single Siebel application, configure parameters for one of the following (defined as enterprise profile or named subsystem):

- **LDAP Security Adapter.** Typically, the alias for this adapter is LDAPSecAdpt.
- **ADSI Security Adapter.** Typically, the alias for this adapter is ADSISecAdpt.

Set the security adapter parameters using values similar to those shown in Table 16 on page 149.

Table 16. Siebel Gateway Name Server Parameters (for Enterprise Profile or Named Subsystem)

Parameter	Guideline
Security Adapter Dll Name (SecAdptDllName)	For LDAP, enter `sscfldap`. For ADSI, enter `sscfadsi`. Do not include the file extension (for example, do not specify `sscfldap.dll` for LDAP). The specified value is converted internally to the actual filename for your operating system.
Server Name (ServerName)	For LDAP and ADSI, enter the name of the computer on which the LDAP or ADSI server runs.

Table 16. Siebel Gateway Name Server Parameters (for Enterprise Profile or Named Subsystem)

Parameter	Guideline
Port (Port)	■ For LDAP, an example entry is 389. Typically, use port 389 for standard transmission or port 636 for secure transmission. ■ For ADSI, you set the port at the ADSI directory level, not as a configuration parameter.
Base DN (BaseDN)	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. You cannot distribute the users of a single Siebel application in more than one base DN. However, you can distribute them in multiple subdirectories—such as organization units (OU), which are used for LDAP. LDAP example entry: `ou=people, o=`*`domainname`* In the example, “o” denotes “organization” and is the domain name system (DNS) name for this server, such as *`computer.company.com`*. “ou” denotes “organization unit” and is the name of a subdirectory in which users are stored. ADSI example entry: `ou=people, DC=`*`domainname`*`, DC=com` Domain Controller (DC) entries are the nested domains that locate this server. Therefore, adjust the number of DC entries to represent your architecture.
Username Attribute Type (UsernameAttributeType)	LDAP example entry is uid ADSI example entry is sAMAccountName If you use a different attribute in the directory for the Siebel user ID, enter that attribute name.

Table 16. Siebel Gateway Name Server Parameters (for Enterprise Profile or Named Subsystem)

Parameter	Guideline
Password Attribute Type (PasswordAttributeType)	The LDAP entry must be userPassword. However, if you use the LDAP security adapter to authenticate against Microsoft Active Directory, set the value of this parameter to either unicodePWD or userPassword, depending on the code page used by the directory server. Active Directory does not store the password in an attribute so this parameter is not used by the ADSI adapter. You must, however, specify a value for the Password Attribute Type parameter even if you are using the ADSI adapter. Specify a value of either userPassword or unicodePWD, depending on the code page used by the directory server. In general, specify a value of userPassword if an ASCII code page is used by the directory server, and specify a value of unicodePWD if a Unicode code page is used.
Credentials Attribute Type (CredentialsAttributeType)	LDAP example entry is `mail` ADSI example entry is `physicalDeliveryOfficeName` If you used a different attribute in the directory for the database account, enter that attribute name.

Application User (ApplicationUser)	LDAP example entry:
	`uid=APPUSER, ou=People, o=`*`domainname`*
	ADSI example entry:
	`CN=APPUSER, CN=Users, DC=`*`computername`*`,`
	`DC=`*`domainname`*`, DC=com`
	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.

Table 16. Siebel Gateway Name Server Parameters (for Enterprise Profile or Named Subsystem)

Parameter	Guideline
Application Password (ApplicationPassword)	For LDAP and ADSI, enter APPUSERPW or the password assigned to the application user.

Shared Credentials DN (SharedCredentialsDN)	■ LDAP example entry:
	`uid=shared database account user User ID, ou=people, o=`*`domainname`*
	For example:
	`uid=SharedDBUser, ou=people, o=siebel.com`
	■ ADSI example entry:
	`CN=shared database account user User ID, ou=people, DC=computername, DC=domainname, DC=com`
	For example:
	`CN=SharedDBUser, ou=people, DC=qa1, DC=siebel, DC=com`

Configuring LDAP or ADSI Authentication for Developer Web Clients

This topic describes the tasks you must perform if you want to implement LDAP or ADSI security adapter authentication for Developer Web Clients.

This task is step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

To configure LDAP or ADSI authentication for Developer Web Clients, perform the following tasks:

- "Configuring Security Adapter Parameters for Developer Web Clients" on page 152
- "Setting a System Preference for Developer Web Clients" on page 153

Configuring Security Adapter Parameters for Developer Web Clients

For Developer Web Clients, security adapter parameters are configured in the configuration file of the application for which you are implementing LDAP or ADSI security adapter authentication, rather than in the Gateway Name Server.

Parameters in sections of the application configuration file that directly pertain to security adapters apply, in this context, only to the Siebel Developer Web Client. These parameters are counterparts to the Siebel Gateway Name Server parameters listed in Table 14 on page 148, Table 15 on page 149, and Table 16 on page 149.

To configure a security adapter for the Developer Web Client, provide parameter values, as indicated by the guidelines in Table 17 on page 153, in the configuration file for the Siebel application for which you are implementing LDAP or ADSI security adapter authentication.

You can use a text editor to make changes to an application configuration file, or you can do so using the Siebel Configuration Wizard. For more information about editing an application's configuration file and about the purposes for the parameters, see "Siebel Application Configuration File Parameters" on page 348. For a list of Siebel Business Applications configuration files, see *Siebel System Administration Guide*.

Table 17. Siebel Business Applications Configuration File Parameters

Section	Parameter	Value
[InfraUIFramework]	AllowAnonUsers	Enter TRUE for LDAP or ADSI. You can set this parameter to FALSE if the Siebel application does not use functionality that requires anonymous browsing, such as anonymous catalog browsing or user self-registration.
[InfraSecMgr]	SecAdptMode	■ For LDAP, specify LDAP. ■ For ADSI, specify ADSI.
	SecAdptName	■ For LDAP, specify LDAPSecAdpt or another name of your choice. ■ For ADSI, specify ADSISecAdpt or another name of your choice.
[LDAPSecAdpt]	For parameters, see Appendix B, "Configuration Parameters Related to Authentication."	For parameter values, see "Configuring Security Adapter Gateway Name Server Parameters" on page 147.
[ADSISecAdpt]	For parameters and suggested values, see Appendix B, "Configuration Parameters Related to Authentication."	For parameter values, see "Configuring Security Adapter Gateway Name Server Parameters" on page 147.

Setting a System Preference for Developer Web Clients

If you are configuring LDAP or ADSI authentication for the Siebel Developer Web Client, you must set the SecThickClientExtAuthent. system preference to True, as described in this topic.

Setting the SecThickClientExtAuthent. parameter to True allows security adapter authentication for users who log in through the Siebel Developer Web Client. System preferences are enterprise-wide settings, however, the SecThickClientExtAuthent system preference has no effect on security adapter authentication for users who log in through the Siebel Web Client.

Use the following procedure to specify a value for the SecThickClientExtAuthent parameter.

To set the SecThickClientExtAuthent parameter

1. Log in as an administrator to a Siebel employee application.
2. Navigate to the Administration - Application screen, then the System Preferences view.
3. In the System Preferences list, select the SecThickClientExtAuthent system preference.
4. In the System Preference Value column, enter TRUE.
5. Restart the Siebel Server.

Restarting Servers

This topic describes the Windows services on the Web server computer that you must restart to activate the changes you make during the process of configuring LDAP or ADSI security adapter authentication.

This task is step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

Stop and restart the following services:

- **IIS Admin service and Worldwide Web Publishing service.** 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 system service.** Stop and restart the Siebel Server. For details, see *Siebel System Administration Guide*.
- **Siebel Gateway Name Server system service.** Stop and restart the Siebel Gateway Name Server. For details, see *Siebel System Administration Guide*.

Testing the LDAP or ADSI Authentication System

After performing all the tasks required to implement LDAP or ADSI security adapter authentication, you can verify your implementation using the procedure in this topic.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 138.

The tests outlined in this topic allow you to confirm that the security adapter provided with Siebel Business Applications, your LDAP or ADSI 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 LDAP or ADSI authentication implementation, perform the following procedure.

To test your LDAP or ADSI authentication system

1. In a Web browser, enter the URL to your Siebel application, such as:

   ```
   http://www.mycompany.com/eservice_enu
   ```

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

2. Various links provide access to views intended for anonymous browsing. Some other links will require you to log in first.

   NOTE: Employee applications, such as Siebel Call Center, typically do not allow anonymous browsing, while customer applications such as Siebel eService do.

3. Navigate back to the Web page that contains the login text boxes, and then log in with the user ID and 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 or other application features might appear, indicating that the test user has authenticated successfully. The user record in the database provides views through the expanded responsibility of this registered user.

4. Click the Log Out link.

5. Repeat Step 1 on page 155 to access the login page. If a New User button is present, click it.

   If a New User button is not present, the Siebel application, without additional configuration, does not allow users to self-register.

6. In the Personal Information form, complete the required fields, as shown below, 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 user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. For information about user authentication architectures, see Chapter 6, “Security Adapter Authentication.”

Field	Description
Verify Password	Required when Password is required.
Challenge Question	Required. Enter a phrase for which there is an “answer.” If you later click Forgot Your Password?, 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 on page 155.

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

About Migrating from Database to LDAP or ADSI Authentication

When you install your Siebel Business Applications, three security adapters are provided for user authentication: a database security adapter, an ADSI security adapter, and an LDAP security adapter. The database security adapter is enabled by default. If you want to implement LDAP or ADSI security adapter authentication for a Siebel application that was previously configured to use database authentication, review the information in this topic.

There are a number of issues that you have to consider in deciding the most appropriate authentication method for your Siebel implementation, for example, some features, such as user self-registration, are unavailable with database authentication while some components, such as batch and system management components, must use database authentication. For information on the benefits and limitations of different security adapter authentication options, review the following topics:

- “Comparison of Authentication Strategies” on page 109
- “About Siebel Security Adapters” on page 110
- “Features Not Available for Database Authentication” on page 113
- “Comparison of LDAP and ADSI Security Adapters” on page 116

Migrating from Database to LDAP or ADSI Authentication

Migrating a Siebel application from database authentication to LDAP or ADSI authentication involves the same steps as those outlined in “Process of Implementing LDAP or ADSI Security Adapter Authentication” on page 138. In addition, you must perform the following steps:

1 Migrate your users from the Siebel database to the external directory server; ensure that you create an entry in the external directory for each user to be authenticated.

2 (Optional) Archive any Siebel user database accounts from the Siebel database that are not required for LDAP or ADSI authentication.

CAUTION: Do not archive the default Siebel administrator account, SADMIN, or the default database account that is used by Siebel LDAP and ADSI security adapters to connect to the Siebel database, for example, LDAPUSER. These database accounts are required when using LDAP or ADSI authentication.

About Password Hashing

User passwords or database credentials passwords can be hashed for greater security. This topic describes the password hashing options available with Siebel Business Applications.

Unlike encryption that involves two-way algorithms (encryption and decryption), hashing uses a one-way algorithm. A clear-text version of a password is hashed using a Siebel utility, then stored in the database or in an external directory such as LDAP or ADSI. During login, a clear-text version of a password is provided (such as by a user), which is then hashed and compared to the stored hashed password.

The password hashing options available with Siebel Business Applications are as follows:

- **User password hashing.** When you are using security adapter authentication (including database, LDAP or ADSI, or custom security adapters), user passwords can be hashed.

  An unexposed, hashed password is maintained for each user, while the user logs in with an unhashed (clear-text) version of the password. This password is hashed during login.

  Password hashing is a critical tool for preventing unauthorized users from bypassing Siebel Business Applications and logging directly into the Siebel database using an RDBMS tool such as SQL*Plus. It also prevents passwords intercepted over the network from being used to access the applications, because an intercepted hashed password will itself be hashed when login is attempted, leading to a failed login.

- **Database credentials password hashing.** When you are using security adapter authentication other than database authentication (including LDAP or ADSI or custom security adapters), or using Web SSO authentication, database credentials passwords can be hashed.

  An unexposed, hashed password for a database account is maintained, while an unhashed (clear-text) version of the password is stored in the LDAP or ADSI external directory. This password is hashed during login.

  Credentials password hashing prevents users from being able to log into the Siebel database directly using a password obtained through unauthorized access to the external directory, because the unhashed password will not match the hashed version stored in the database.

- **Password hashing utility.** Siebel Business Applications provide a password hashing utility called hashpwd.exe which uses the RSA SHA-1 hashing algorithm by default. For existing customers, the Siebel proprietary hashing algorithm (the mangle algorithm) is also available as an option for the hashpwd.exe utility.

  NOTE: New customers are required to use RSA-SHA1, and existing customers are strongly recommended to migrate to RSA-SHA1 promptly.

The following topics provide additional information about using password hashing with Siebel Business Applications:

- "Overview of the Login Process When Password Hashing Is Enabled" on page 158
- "Process of Configuring User and Credentials Password Hashing" on page 159
- "Running the Password Hashing Utility" on page 162

NOTE: For information about managing encrypted passwords in the eapps.cfg file, see "Managing Encrypted Passwords in the eapps.cfg File" on page 45. The password encryption mechanism described there is unrelated to the password hashing mechanism described in this topic.

Overview of the Login Process When Password Hashing Is Enabled

This topic describes the login process for a Siebel Business Applications user when password hashing has been implemented. For information on configuring password hashing, see "Process of Configuring User and Credentials Password Hashing" on page 159.

A user is logged into the Siebel application by the following process:

1. The user logs in with user credentials that include the unhashed password.
2. The AOM receives the user credentials and passes them to the authentication manager.
3. The authentication manager hashes the password, according to the configuration of the security adapter.
4. In a database authentication environment:
   a. The authentication manager passes the user credentials (user ID and hashed password) to the database security adapter.
   b. The database security adapter verifies that the hashed password matches the hashed password stored in the database for the user. It validates the credential by trying to connect to the database server. The security adapter confirms to the AOM, through the authentication manager, that the credentials are valid.
5. In an LDAP or ADSI authentication environment:
   a. The authentication manager passes the user credentials, including the hashed password, to the LDAP or ADSI security adapter.
   b. The LDAP or ADSI security adapter verifies that the hashed password matches the hashed password stored in the directory for the user, and then returns the database account and the Siebel user ID to the AOM through the authentication manager.
6. The AOM initiates a Siebel session for the user.

Process of Configuring User and Credentials Password Hashing

This topic describes how to implement password hashing for user passwords or for database credentials, and how to specify the default hashing algorithm.

Configuration parameters for all security adapters provided with Siebel Business Applications, and for custom security adapters you implement, specify the password hashing settings in effect. For LDAP or ADSI authentication, parameters are specified for the security adapter. For database authentication, the relevant parameters are specified for a data source referenced from the database security adapter, rather than specified directly for the security adapter.

To configure password hashing, perform the following tasks:

1. Review "Guidelines for Password Hashing" on page 159
2. Perform either or both of the following tasks, as appropriate:
   - "Configuring User Password Hashing" on page 160
   - "Configuring Database Credentials Password Hashing" on page 161

Some steps in these procedures, such as those for setting configuration parameter values using Siebel Server Manager, can alternatively be accomplished by using the Siebel Configuration Wizard.

Guidelines for Password Hashing

This topic describes the factors you have to consider if you choose to implement password hashing with Siebel Business Applications.

This task is a step in "Process of Configuring User and Credentials Password Hashing" on page 159.

Guidelines for using password hashing with Siebel Business Applications include the following:

- The password hashing utility, hashpwd.exe, does not automatically store hashed passwords in the Siebel database or LDAP or ADSI directory. The administrator is responsible for defining and storing the hashed passwords. A hashed password is stored in one of the following locations:
  - In a database authentication environment, the hashed password is set as the valid password for the database account.
  - In an LDAP or ADSI authentication environment, the hashed password is stored in the attribute specified for the user's password.
- The unhashed version of the password is given to a user to use when logging in.
- Stored passwords must first be hashed with the same hashing algorithm (typically, RSA SHA-1) that will be applied to the passwords in the authentication process.
- However, database credentials passwords stored outside of the Siebel database must be stored in unhashed form, because such passwords are hashed during the authentication process.

- With database authentication, the Siebel Server components that log in to the database must use the hashed password value stored in the Siebel database. Otherwise, the component login fails.

  For example, when you run the Generate Triggers (GenTrig) component, the value provided for the PrivUserPass parameter (used along with the PrivUser parameter) must be the hashed password value.

  To determine if a Siebel Server component uses a hashed password, select the component from the Enterprise Component Definition View and query for the component parameter OM - Data Source. If the value that OM - Data Source references has DSHashAlgorithm set to a hashing algorithm and DSHashUserPwd set to TRUE, it means that the component can accept an unhashed password and hash it using the specified parameters.

- Password hashing must be specified consistently for all Siebel Enterprise components that will work together. For example, all Siebel Servers subject to AOM load balancing must use the same security adapter settings, including those for password hashing, or component login fails.

- For the Siebel Mobile Web Client, password hashing for the local database password has the following requirements:

  - The parameter Encrypt client Db password (alias EncryptLocalDbPwd) must have been set to TRUE for the server component Database Extract (alias DbXtract) at the time the user's local database was extracted. See *Siebel Remote and Replication Manager Administration Guide* for details.

  - The database security adapter must be in effect for the Mobile Web Client, and the DSHashUserPwd and DSHashAlgorithm parameters must be set appropriately for the data source specified for the security adapter. For more information, see "Configuring Database Authentication" on page 112 and "Siebel Application Configuration File Parameters" on page 348.

Configuring User Password Hashing

The procedure in this topic describes how to configure user password hashing.

This task is a step in "Process of Configuring User and Credentials Password Hashing" on page 159.

To implement user password hashing

1. For each user, create and record a username and a password.
2. To hash one or more passwords, run the hashpwd.exe utility at a command prompt. For command syntax options, see "Running the Password Hashing Utility" on page 162.
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 hashed password.

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

- In an LDAP or ADSI authentication environment, set the values in the directory attributes for username and password to the username and the hashed password.

4. Using Siebel Server Manager, configure the security adapter for user password hashing.
   - For the database security adapter (typically, DBSecAdpt):
     - Set the DataSourceName parameter to the name of the applicable data source (for example, ServerDataSrc).
     - For the applicable data source, set the DSHashUserPwd parameter to TRUE.
     - For the applicable data source, set the DSHashAlgorithm parameter to RSASHA1 (this is the default value) or SIEBELHASH (the Siebel proprietary algorithm).
   - For the LDAP or ADSI security adapter (typically, LDAPSecAdpt or ADSISecAdpt):
     - Set the HashUserPwd parameter to TRUE.
     - Set the HashAlgorithm parameter to RSASHA1 (this is the default value) or SIEBELHASH (the Siebel proprietary algorithm).
5. Provide each user with the username and the clear-text password for logging in.

Configuring Database Credentials Password Hashing

The procedure in this topic describes how to configure database credentials password hashing.

This task is a step in "Process of Configuring User and Credentials Password Hashing" on page 159.

To implement database credentials password hashing

1. For each applicable database account, create and record a login name and a password.
2. To hash one or more passwords, run the hashpwd.exe utility at a command prompt. For command syntax options, see "Running the Password Hashing Utility" on page 162.
3. For each database account, assign the hashed passwords to their corresponding database accounts.

   For information about setting credentials for database accounts, see your RDBMS documentation.
4. In the LDAP or ADSI directory, specify the unhashed version of the password for the attribute that contains the database account.

   For information about required attributes in the directory, see "Requirements for the LDAP or ADSI Directory" on page 118.
5. Using Siebel Server Manager, configure the security adapter for credentials password hashing.
   - For the LDAP or ADSI security adapter:
     - Set the HashDBPwd parameter to TRUE.
     - The hash algorithm will be based on the setting you previously made for the `HashAlgorithm` parameter when you configured user password hashing.

Running the Password Hashing Utility

This topic describes how to hash user passwords using the hashpwd.exe utility. The hashpwd.exe utility is located in the directory *SIEBSRVR_ROOT*\bin (Siebel Server installation directory) or *SIEBEL_CLIENT_ROOT*\bin (Siebel Mobile or Developer Web Client installation directory).

You can hash passwords using the RSA SHA-1 hashing algorithm or the siebelhash algorithm. The procedures in this topic describe how to hash passwords using both algorithms.

When you have hashed user passwords using hashpwd.exe, store the hashed password values in the directory or database, as appropriate. For information on storing hashed passwords, see "Guidelines for Password Hashing" on page 159. For information about the password hashing options mentioned in the procedures in this topic, see "About Password Hashing" on page 157.

The following procedure describes how to run the hashpwd.exe utility using the default password hashing algorithm, RSA SHA-1.

To hash passwords using the RSA SHA-1 algorithm

- To hash passwords using the RSA SHA-1 algorithm, run the utility using one of the following syntaxes:
  - To hash individual passwords, use the following syntax:

    ```
    hashpwd password1 password2 ...
    ```

    ```
    hashpwd -a rsasha1 password1 password2 ...
    ```

  - To hash multiple passwords using a batch file, enter the passwords into a batch file (for example, the file might be named passwords.txt), and then specify the filename using the following syntax:

    ```
    hashpwd @password_file_name
    ```

The following procedure describes how to run the hashpwd.exe utility using the Siebel proprietary password hashing algorithm.

To hash passwords using the siebelhash algorithm

- To hash passwords using the Siebel proprietary password hashing algorithm, run the hashpwd.exe utility using one of the following syntaxes:
  - To hash individual passwords, use the following syntax:

    ```
    hashpwd -a siebelhash password1 password2 ...
    ```

  - To hash multiple passwords using a batch file, enter the passwords into a batch file (for example, the file might be named passwords.txt), and then specify the filename using the following syntax:

    ```
    hashpwd -a siebelhash @password_file_name
    ```

Security Adapter Deployment Options

This topic 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 security adapters and by adapters that comply with the *Siebel Security Adapter Software Developer's Kit (SDK) version 3.0*. For more information, see 476962.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Technical Note 415.

Depending on your security adapter or Web SSO implementation, you might have to configure the following:

- "Configuring the Application User" on page 163
- "Configuring Checksum Validation" on page 165
- "Configuring Secure Communications for Security Adapters" on page 166
- "Configuring the Shared Database Account" on page 167
- "Configuring Adapter-Defined User Name" on page 169
- "Configuring the Anonymous User" on page 170
- "Configuring Roles Defined in the Directory" on page 172

Configuring the Application User

This topic describes how to configure the directory application user. The application user is not an actual user who logs into an application; it is a special user defined to handle access to the directory.

The application user is the only user with search and write privileges to the LDAP or ADSI directory and this user must be defined in the following authentication strategies that implement a Siebel security adapter:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

By setting up an application user as the only user with search, read, and update 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 defined in the directory with the following qualities:

- This user provides the initial binding of the LDAP or Active Directory server with the AOM when a user requests the login page. Otherwise, by default, the anonymous user provides the initial binding.

- This user has sufficient permissions to read any user's information in the directory and do any necessary administration. The application user does all searching and writing to the directory that is requested through the security adapter.

  In a Siebel security adapter implementation, the application user must have search and write privileges for all user records in the directory. In a Web SSO implementation, the application must have, at least, search privileges.

  NOTE: If you are configuring an ADSI security adapter, ensure that the application user is either a domain user or has access to the directory server. If the application user cannot access the directory server, the authentication process fails.

- Permissions for the application user must be defined at the organization level (for example, OU for LDAP).

You maintain an 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. An encryption algorithm is applied to the application user password before it is sent to the database. The application user login must also be set up with the encrypted version of the password.

Perform the following procedure to define the application user.

To configure the 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 user name, 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. Enter the password in unencrypted form. If you implement an ADSI directory, you specify the password using Active Directory user management tools, not as an attribute.

2. For your Siebel security adapter, define the following parameter values for the security adapter's enterprise profile (such as LDAPSecAdpt or ADSISecAdpt) on the Siebel Gateway Name Server.

   - **ApplicationUser.** Enter the application user's full distinguished name (DN) in the directory, for example:

     ```
     ApplicationUser = "uid=APPUSER, ou=people, o=oracle.com"
     ```

   - **ApplicationPassword.** Enter the application user password (unencrypted).

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 341. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

Application User and Password Expiration Policies

Typically, user administration in an LDAP or ADSI directory 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.

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

For more information about account policies and password expiration, see "Login Security Features" on page 200.

Configuring Checksum Validation

The checksum validation option verifies that the security adapter loaded by the authentication manager is the correct version. It is 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.

Checksum validation for security adapters can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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

Checksum validation supports the following principles:

- A CRC (cyclical redundancy check) checksum value for the security adapter library file (such as the DLL file on Windows) is stored as a configuration parameter value for the security adapter.
- When a security adapter provides a user identity and database account to the AOM, a checksum value is calculated for that security adapter.
- The user is granted access if the two checksum values are equal.

The following procedure outlines the steps in implementing checksum validation.

To configure checksum validation

1. Enter and run the following command at a command prompt, using the required security adapter library file name (such as the DLL file on Windows) as the argument:

   ```
   checksum -f filename
   ```

   The utility returns the checksum value.

   For example, if you are using an LDAP security adapter, the following command:

   ```
   checksum -f sscfldap.dll
   ```

   returns something similar to:

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

   Specify a different DLL file if you are using an ADSI or a custom security adapter.

2. For the security adapter you are using, set the CRC configuration parameter to the checksum value that is calculated in Step 1 on page 166.

   The checksum value in this procedure is an example only. You must run the checksum utility as described to generate the value that is valid for your implementation. In addition, you must recalculate the CRC checksum value and update the CRC parameter value after upgrading your Siebel Business Applications by applying Quick Fixes, Fix Packs or moving to a new Siebel CRM release.

For information about setting Siebel Gateway Name Server configuration parameters, see “Siebel Gateway Name Server Parameters” on page 341. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

Configuring Secure Communications for Security Adapters

You can use SSL to transmit data between the security adapter provided with Siebel Business Applications and the LDAP or ADSI directory. Secure communications for the Siebel security adapter can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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 LDAP or ADSI security adapter.

NOTE: If you use the LDAP security adapter to authenticate users against an AD directory, you must configure SSL between the LDAP security adapter and AD directory server if you want to manage user passwords or create new users in the Active Directory.

The following procedure describes how to configure SSL for the LDAP security adapter.

To configure SSL for the LDAP security adapter

- Set the SslDatabase parameter value for the security adapter (LDAPSecAdpt) to the absolute path of the file ldapkey.kdb. This file, which is generated by IBM GSKit, contains a certificate for the certificate authority that is used by the directory server.

  For information about generating the SSL database file for an LDAP authentication environment, see "Generating a CMS Key Database Using IBM GSKit" on page 131.

The following procedure describes how to configure SSL for the ADSI security adapter.

To configure SSL for the ADSI security adapter

1. 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 profile parameter UseSsl to True for the ADSI Security Adapter profile (alias the ADSISecAdpt parameter).

   For information about setting Siebel Gateway Name Server parameters, see "Siebel Gateway Name Server Parameters" on page 341.

Configuring the Shared Database Account

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

The shared database account option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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.

The shared database account option is used differently by the LDAP and ADSI security adapters:

- For LDAP, the shared database account can be specified as profile parameters for the LDAP Security Adapter profile (alias LDAPSecAdpt) or as an attribute of the shared database account record in the LDAP directory.
- For ADSI, if the shared database account is specified, then database credentials are retrieved from a user if they are available to be extracted. If database credentials are not available from the user, they are instead retrieved from the shared database account.

The following topics describe in more detail how the LDAP and ADSI directory servers use the shared database account option.

Storing Shared Database Credentials as Attributes of the Directory Entry

This topic describes how to implement a shared database account and store the database credentials as attributes of the directory entry you create for the shared database account. This option is available to you when you use an ADSI directory or an LDAP directory.

To store the database credentials in an attribute of the directory entry

1. Create a database account to be shared by all users who log into a given Siebel application.

   For additional information on this task, see "About Creating a Database Login" on page 140.

2. Create a designated entry in the directory, and enter the user name and password for the common database account in one of that entry's attributes, such as the dbaccount attribute. You might have to create this attribute.

   NOTE: The user name and password you specify for the shared database account must be a valid Siebel user name and password.

   For information about formatting a directory attribute that contains the database account, see "Requirements for the LDAP or ADSI Directory" on page 118.

3. For each security adapter that implements this shared database account, define the following parameter values:

   - **CredentialsAttributeType.** Enter the attribute in which the database account is stored in the directory, such as dbaccount
   - **SharedCredentialsDN.** Enter the distinguished name (including quotes) for the designated entry, such as `"uid=SharedDBUser, ou=people, o=companyname.com"`

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 341. For Developer Web Client, define these parameters in the corresponding section in the application configuration file.

Storing the Database Credentials as Profile Parameters

This topic describes how to configure a shared database account for an LDAP directory and store the database credentials as parameters of the LDAP Security Adapter profile (alias LDAPSecAdpt). This option is available to you only when you use LDAPSecAdpt.

Do not use this option if you have to store more than one set of database credentials as only one set of database credentials can be stored as profile parameters.

To store the database credentials as profile parameters

1. Navigate to the Administration - Server Configuration screen, then the Profile Configuration view.
2. Select the LDAPSecAdpt profile.
3. Define the following parameter values for LDAPSecAdpt:

   - **SharedDBUsername.** The username to connect to the Siebel database.

- **SharedDBPassword.** The password to connect to the Siebel database.

NOTE: You must specify a valid Siebel user name and password for the SharedDBUsername and SharedDBPassword parameters.

Configuring Adapter-Defined User Name

You can configure your authentication system so that the username presented by the user and passed to the directory to retrieve a user's database account is not the Siebel user ID. For example, you might want users to enter an adapter-defined user name, such as their Social Security number, phone number, email address, or account number. The security adapter returns the Siebel user ID of the authenticated user and a database account from the directory to the authentication manager.

The adapter-defined user name option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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 might have users enter their telephone number, stored in the telephonenumber attribute, while their Siebel user ID is stored in the uid attribute.

The UsernameAttributeType configuration parameter defines the directory attribute that stores the username 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 (alias UsernameBCField) parameter for the AOM 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 parameter for the security adapter, and set the OM - Username BC Field parameter. If you do not define these parameters appropriately, 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 the work phone number.

The following procedure outlines how to configure an adapter-defined user name.

To configure an adapter-defined user name

1 For each security adapter (such as LDAPSecAdpt) that implements an adapter-defined user name, define the following parameter values:

Parameter	Value
UseAdapterUsername	TRUE
SiebelUserNameAttributeType	The attribute in which you store the Siebel user ID, such as uid (LDAP), or sAMAccountName (ADSI).
UsernameAttributeType	The attribute in which you store the adapter-defined user name, such as telephonenumber.

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 341. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

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

The AOM parameter to be populated is OM - Username BC Field.

For information about working with Siebel business components, see *Configuring Siebel Business Applications*. For information about working with configuration parameters, see *Siebel System Administration Guide*.

3 Using Siebel Server Manager, specify the User business component field name as the value for the OM - Username BC Field parameter. You can provide this value at the Enterprise, Siebel Server, or component level. If this parameter is not present in the parameters list, add it.

NOTE: The OM - Username BC Field parameter is case sensitive. The value you specify for this parameter must match the value specified for the parameter in Siebel Tools.

If you do not specify a field in the OM - Username BC Field parameter, the Siebel security adapter assumes that 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 configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

Configuring the Anonymous User

The anonymous user is a Siebel user with very limited access. The anonymous user (defined in the Siebel database) allows a user to access a login page or a page containing a login form. For LDAP or ADSI 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 LDAP or ADSI authentication. The anonymous user is required even if your applications do not allow access by unregistered users. When an AOM thread 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 page.

Anonymous Browsing and the Anonymous User

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. Unregistered users access Siebel Business Applications views and the database through the anonymous user record.

If you allow anonymous browsing, users can browse views that are not flagged for explicit login. If you disallow anonymous browsing, unregistered users have no access to any of the application's views but do still have access to an application's login page.

The following procedure describes how to configure the anonymous user.

To configure the anonymous user

1. Define a user in the directory using the same attributes as used for other users. Assign values in appropriate attributes that contain the following information:
   - **Siebel user ID.** Enter the user ID of the anonymous user record for the Siebel application you are implementing in the attribute in which you store the Siebel user ID.
   - **Password.** Assign a password of your choice. Enter the password in unencrypted form. If you implement an ADSI directory, you specify the password using ADSI user management tools, not as an attribute.
2. Edit the eapps.cfg file using a text editor and specify values for the following parameters:
   - **AnonUserName.** Enter the user name required for anonymous browsing and initial access to the login pages of the application you are implementing, for example, GUESTCST.
   - **AnonPassword.** Enter the password associated with the anonymous user. If necessary, you can manually encrypt this password using the encryptstring.exe utility. For additional information, see "Encrypting Passwords Using the encryptstring Utility" on page 46.

   You can define an anonymous user for a single application or as the default for all the Siebel Business 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, define the anonymous user in the [defaults] section of the eapps.cfg file. To override the default value for an individual application, list the AnonUserName and AnonPassword parameters in the applications section of the eapps.cfg file, for example, the [/eservice] section.

Configuring Roles Defined in the Directory

Responsibilities assigned to each user in Siebel Business Applications provide users with access to particular views in the application. Responsibilities are created in Siebel Business Applications and are stored in the Siebel database. One or more responsibilities are typically associated with each user in the Administration - Application screen.

Creating roles in the LDAP or ADSI directory is 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 associated with all the responsibilities that are directly or indirectly associated with the user.

You can choose to store users' Siebel responsibilities as roles in a directory attribute instead of in the Siebel database in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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, create responsibilities in Siebel Business Applications, but do not assign responsibilities to users through the Siebel application interface.

To configure roles defined in the directory

1. In the directory, define a directory attribute for roles.

   To ensure that you can assign more than one responsibility to any user, define the roles directory attribute as a multivalue attribute. The security adapters supported by Siebel Business Applications cannot read more than one responsibility from a single-value attribute.

2. For each user, in the directory attribute for roles, enter 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 multivalue field. Role names are case-sensitive.

3. Configure the security adapters provided with Siebel Business Applications to retrieve roles for a user from the directory by setting the RolesAttributeType parameter for the LDAP or ADSI security adapter. For example, for the LDAP security adapter, define the following parameter:

   ```
   RolesAttributeType= attribute_in_which_roles_are_stored
   ```

   For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 341. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

Security Adapters and the Siebel Developer Web Client

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

- AOM (through the siebel.exe program)
- Application configuration file
- Authentication manager and security adapter
- IBM LDAP Client (where applicable)

NOTE: Siebel Business Applications support for the Siebel Developer Web Client is restricted to administration, development, and troubleshooting usage scenarios only. Siebel Business Applications does not support the deployment of this client to end users.

When you implement security adapter authentication for Siebel Developer Web Clients, observe the following principles:

- It is recommended to use the remote configuration option, which can help you make sure that all clients use the same configuration settings. This option is described later in this topic.
- Authentication-related configuration parameters stored in application configuration files on client computers, or stored in remote configuration files, must generally contain the same values as the corresponding parameters in the Siebel Gateway Name Server (for Siebel Web Client users). Distribute the appropriate configuration files to all Siebel Developer Web Client users.

  For information about setting parameters in Siebel application configuration files on the Siebel Developer Web Client, see "Siebel Application Configuration File Parameters" on page 348.
- It is 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 "Configuring Checksum Validation" on page 165.
- In a security adapter authentication implementation, you must set the security adapter configuration parameter PropagateChange to TRUE, and set the Siebel system preference SecThickClientExtAuthent to TRUE, if you want to implement:
  - Security adapter authentication of Siebel Developer Web Client users.
  - Propagation of user administration changes from the Siebel Developer Web Client to an external LDAP or AD directory. (For example, if a user changes his or her password in the Developer Web Client, the password change is also populated to the directory.)

  For more information, see "Siebel Application Configuration File Parameters" on page 348 and "Configuring LDAP or ADSI Authentication for Developer Web Clients" on page 152.

- In some environments, you might want to rely on the data server itself to determine whether to allow Siebel Developer Web Client users to access the Siebel database and run the application. In the application configuration file on the local client, you can optionally define the parameter IntegratedSecurity for the server data source (typically, in the [ServerDataSrc] section of the configuration file).

  The IntegratedSecurity parameter can be set to TRUE or FALSE. The default value is FALSE. When TRUE, the Siebel client is prevented from prompting the user for a username and password when the user logs in. Facilities provided in your existing data server infrastructure determine if the user is allowed to log into the database.

  You can set the IntegratedSecurity parameter to TRUE with the database security adapter. See also "Configuring Database Authentication" on page 112.

  NOTE: Integrated Security is only supported for Siebel Developer Web clients that access Oracle and Microsoft SQL Server databases. This functionality is not available for Siebel Web clients or Siebel Mobile Web clients.

  For additional information on integrated authentication, see your third-party documentation. For Oracle, see the OPS$ and REMOTE_OS_AUTHENT features. For Microsoft SQL Server, see Integrated Security.

For more information about the Siebel Developer Web Client, see the *Siebel Installation Guide* for the operating system you are using and *Siebel System Administration Guide*.

Sample LDAP Section in a Configuration File

The following is an example of LDAP configuration information generated by the Siebel Configuration Wizard when you configure an LDAP security adapter for Developer Web Clients. For more information, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 134.

For information about setting Siebel configuration parameters, see "Siebel Application Configuration File Parameters" on page 348.

```
[LDAPSecAdpt]
SecAdptDllName = sscfldap
ServerName = ldapserver.siebel.com
Port = 636
BaseDN = "ou=people, o=xyz.com"
SharedCredentialsDN = "uid=HKIM, ou=people, o=oracle.com"
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = mail
RolesAttributeType = roles
SslDatabase = /suitespot/https-myhost/ldapkey.kdb
ApplicationUser = "uid=APPUSER, ou=people, o=xyz.com"
ApplicationPassword = APPUSERPW
HashDBPwd = TRUE
PropagateChange = TRUE
CRC =
SingleSignOn = TRUE
TrustToken = mydog
UseAdapterUsername = TRUE
```

```
SiebelUsernameAttributeType = PHONE
HashUserPwd = TRUE
HashAlgorithm = RSASHA1
```

Remote Configuration Option for Developer Web Client

This option applies to the Siebel Developer Web Client only. The remote configuration option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

With this approach, you create a separate text file that defines any parameter values that configure a security adapter. You configure all security adapter parameters, such as those in a section like [LDAPSecAdpt] or [ADSISecAdpt], in the remote file, not in the application configuration file.

Storing configuration parameters in a centralized location can help you reduce administration overhead. All Developer Web Clients can read the authentication-related parameters stored in the same file at a centralized remote location.

The examples below show 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. The following example is from the configuration file uagent.cfg for Siebel Call Center:

```
[InfraSecMgr]
SecAdptMode = LDAP
SecAdptName = LDAPSecAdpt
UseRemoteConfig = \\it_3\vol_1\private\ldap_remote.cfg
```

In this case, the configuration file ldap_remote.cfg would contain an [LDAPSecAdpt] section. It could be defined similarly to the example earlier in this topic, and would contain no other content. The application configuration file would contain the [InfraSecMgr] section as defined above. It would not contain an [LDAPSecAdpt] section—even if it did, it would be ignored.

To implement remote security configuration for Siebel Developer Web Clients, follow these guidelines:

- The [InfraSecMgr] section in the Siebel configuration file must include the UseRemoteConfig parameter, which provides the path to a remote configuration file. The path is specified in universal naming convention format—that is, for example, `\\server\vol\path\ldap_remote.cfg`.
- The remote security configuration file contains only a section for configuring the security adapter, such as the [LDAPSecAdpt] section.
- Each Developer Web Client user must have read privileges on the remote configuration file and the disk directory where it resides.

Authentication for Mobile Web Client Synchronization

This topic describes some of the processing that occurs to authenticate a remote user during synchronization. For detailed information about the synchronization process, see *Siebel Remote and Replication Manager Administration Guide*.

Note the following facts about Siebel Remote and remote users:

- Remote users do not connect to the Web server. When remote users synchronize, they connect directly from the Siebel Mobile Web Client to the Siebel Remote server—the Siebel Server designated to support synchronization with 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 Mobile Web Clients, such as two clients on two separate computers.

About the Synchronization Process for Remote Users

Siebel remote users connect to a local database on their client computers, make transaction modifications, and then synchronizes theses changes to the Siebel Remote server. This involves the following steps:

1. Launch the Siebel icon on the client computer, then enter a user ID and password.
2. In the Connect To parameter, choose Local.

   The user ID and password are validated by the local database residing on the client computer.
3. The Siebel application appears in the Web browser and the user navigates through the application and modifies data, as appropriate (insert, update, or delete operations).
4. Later, the user decides to synchronize the local database changes and download updates from the Siebel Remote server. This involves the following steps:

   a. Connect to the Siebel Remote server using a dial-up modem or LAN, WAN, or VPN connection.

   b. Launch the Siebel icon on the client computer, then enter 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 client computer.

   d. When the Siebel application appears in the Web browser, the user chooses the Synchronize Database menu item from the File menu.

      The user is now accessing the Siebel Remote server for synchronization, and is subject to authentication.

   e. Once the remote user is authenticated, synchronization begins.

Authentication Options for Synchronization Manager

The Synchronization Manager server component, for Siebel Remote, validates each incoming Mobile Web Client request. Synchronization Manager validates the mobile user's user ID against the list of valid Mobile Web Clients in the server database and validates that the effective end date is valid or NULL.

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

Synchronization Manager authenticates the Mobile Web Client's password by using the method specified using the Authentication Method configuration parameter (alias Authentication). Set this parameter for Synchronization Manager using Siebel Server Manager. For details, see *Siebel Remote and Replication Manager Administration Guide*.

The Authentication Method parameter can be set to one of the following values:

- **None.** Does not authenticate the Mobile Web Client's password. This is the default setting.
- **Database.** Uses the Mobile Web Client's user name and password to connect to the server database. Uses the database security adapter to do this (typically, DBSecAdpt).
- **SecurityAdapter.** Uses the security adapter specified using the parameters Security Adapter Mode and Security Adapter Name to authenticate the user. Depending on the security adapter in effect, the user can be authenticated against the database or against an LDAP or ADSI directory. Password hashing is subject to the configuration of this security adapter.

  The Security Adapter Mode and Security Adapter Name parameters can be set at the Enterprise or Siebel Server level, or set for the Synchronization Manager component. Database authentication is the default security adapter. You can use the same security adapter across the Siebel Enterprise, or use a different security adapter for Synchronization Manager than you do for the rest of the Enterprise. For more information, see "About Siebel Security Adapters" on page 110 and subsequent topics, earlier in this chapter.
- **Siebel.** Validates the Mobile Web Client's password against the password stored in the Mobile Web Client's screen. (This option uses the mangle encryption algorithm, which is no longer recommended.)
- **AppServer.** Verifies that the password is the same as the user's operating system password on the Siebel Server computer. (This option is no longer recommended.)

7 Web Single Sign-On Authentication

This chapter describes how to implement Web Single Sign-On (Web SSO) for user authentication. It includes the following topics:

About Web Single Sign-On

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

NOTE: Web SSO authentication does not apply to the Siebel Mobile Web Client. When connecting to the local database using Siebel Mobile Web Client, mobile users must use local database authentication. For a particular Siebel application, when users connect from the Siebel Developer Web Client to the server database, the authentication mechanism must be the same as that used for Siebel Web Client users. For information about authentication options for local database synchronization for mobile users, see *Siebel Remote and Replication Manager Administration Guide*.

See the following topics for additional information about Web Single Sign-On:

- "Web SSO Authentication Process" on page 179
- "Web SSO Limitations" on page 180

Web SSO Authentication Process

The steps in the Web SSO authentication process 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 SWSE passes the authenticated user’s username and the value for the TrustToken parameter to the authentication 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. In addition, the security adapter compares the TrustToken value provided in the request with the value stored in the Siebel Application Object Manager’s (AOM) configuration file. If the values match, the AOM accepts that the request has come from the SWSE; that is, from a trusted Web server.
4. The Siebel Application Object Manager (AOM) uses the returned credentials to connect the user to the database and to identify the user.

Related Topic

“About Web Single Sign-On” on page 179

Web SSO Limitations

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 Business Applications features, in a Web SSO environment:

- User self-registration
- Delegated administration of users
- Login forms
- Logout links or the Log Out menu item in the File application-level menu
- Change password feature (in Profile view of User Preferences screen)
- Anonymous browsing
- Switching from an anonymous user to a registered user while using the Shopping Cart

Verify that functionality you require does not rely on the capabilities in the previous list before you attempt to deploy such functionality in a Web SSO environment. For example, the Siebel eSales - Checkout Process workflow and user registration both make use of login forms.

Your Siebel Business Applications might require configuration changes to hide or disable the capabilities in the previous list. For information on hiding or disabling the capabilities listed, see *Configuring Siebel Business Applications*.

About Logging Out of a Web SSO Environment

Because Siebel Business Applications users in a Web SSO environment cannot use logout features, such users must end the application session by closing the browser window. In Microsoft Internet Explorer, do this by navigating to the File menu and choosing the Close menu item, or by clicking X in the top-right corner of the window.

For Siebel Business Applications that use high interactivity mode, either method of closing the browser window in a Web SSO environment causes the AOM to terminate the task (thread) for the user's session immediately.

For Siebel Business Applications that use standard interactivity mode, closing the browser window using either method in a Web SSO environment does not terminate the user’s session until the session timeout (SessionTimeout) has been reached. However, if you are using a third-party single sign-on product, for example, Oracle Enterprise Single Sign-On, the user session is terminated when the browser window is closed.

The SessionTimeout parameter is located in the eapps.cfg file, on the SWSE. For more information about this parameter, see “Parameters in the eapps.cfg File” on page 335.

Related Topic

“About Web Single Sign-On” on page 179

About Implementing Web SSO Authentication

To provide user access to Siebel Business Applications on a Web site implementing Web SSO, the Siebel Business 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

In a Web SSO environment, you must also provide your authentication service and any required components, such as an authentication client component.

Using Microsoft Windows Integrated Authentication

If you deploy Microsoft Windows Integrated Authentication as your Web SSO solution, make sure that your client and Web server meet one of the following conditions:

- Are in the same Windows 2000/2003 domain.
- Are in a trusted Windows 2000/2003 domain where a user’s account can be granted access to resources on the computer hosting Microsoft IIS.

NOTE: To deploy Microsoft Windows Integrated Authentication as your Web SSO solution, your Web server must be Microsoft ISS 5.0 or Microsoft ISS 6.0.

For more information, see Microsoft documentation.

Web SSO Implementation Considerations

Following are some implementation considerations for a Web SSO strategy:

- Users are authenticated independently of Siebel Business 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.

For more information about integrating third-party authentication software with Siebel Business Applications, contact the Siebel Alliance Group.

Web Single Sign-On Options

You can implement the following options 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. For details, see "Configuring the User Specification Source" on page 196.
- **Digital certificate authentication.** Siebel Business Applications support X.509 digital certificate authentication by the Web server. For information on implementing digital certificate authentication for Web SSO, see "Digital Certificate Authentication" on page 195.
- In addition, many options identified in "Security Adapter Deployment Options" on page 163 can be implemented for Web SSO.

Process of Implementing Web Single Sign-On

This topic outlines the tasks involved in implementing a Web SSO authentication system. The process outlined in this topic provides instructions for implementing and testing Web SSO authentication for a single Siebel application, using Microsoft Windows Integrated Authentication as your Web SSO solution. You can repeat the appropriate instructions in this process to provide Web SSO access to additional Siebel Business Applications. The instructions in this process implement the following basic configuration:

- Microsoft IIS Web server is deployed on Windows 2003. The Microsoft IIS Web server functions as the authentication service.
- The Active Directory Service Interfaces (ADSI) directory server and the Web server are installed on different computers. The ADSI directory functions as a directory of users for the following functions:
  - Authenticates Web server users.
  - Provides the Siebel user ID and the database account for authenticated Web server users.

- The ADSI security adapter communicates between the authentication manager and the ADSI directory.

NOTE: Implement Web SSO in a development environment before deploying it in a production environment.

To implement and test Web SSO, perform the following tasks:

1. Verify that all requirements are met.

   See “Requirements for Implementing Web SSO in a Specified Environment” on page 183.

2. (Optional) “Creating Protected Virtual Directories” on page 184.
3. Set up third-party Web SSO authentication.
4. Review “About Creating a Database Login” on page 186.
5. “Setting Up the ADSI Directory” on page 186.
6. “Creating Users in the Directory” on page 187.
7. “Adding User Records in the Siebel Database” on page 188.
8. “Setting Authentication Parameters in the SWSE Configuration File (eapps.cfg)” on page 190.
9. Configure authentication parameters, using one of the following methods:
   - Edit Siebel Gateway Name Server parameters. See “Setting Authentication Parameters for the Siebel Gateway Name Server” on page 191.
   - (Developer Web Clients only) “Editing Parameters in the Application Configuration File” on page 194.

     For Developer Web Clients only, configure authentication parameters in the application configuration file.
10. “Restarting Servers” on page 194.
11. “Testing Web SSO Authentication” on page 194.

Requirements for Implementing Web SSO in a Specified Environment

This topic outlines the requirements for implementing the Web SSO authentication environment described in “Process of Implementing Web Single Sign-On” on page 182.

This task is a step in “Process of Implementing Web Single Sign-On” on page 182.

The following requirements must be met before you setup the Web SSO environment:

- Your Web server and the ADSI directory are installed on different computers.

- Siebel Business Applications, including the Siebel Gateway Name Server and the Siebel Server, are installed. The Siebel Server, including affected AOMs, is installed on the Web server computer.

  These instructions are for a minimal, baseline configuration. In a production environment, it is not recommended to install the Siebel Server on the same computer as the Web server.

- You are experienced with administering ADSI directories. You can perform tasks such as creating and modifying user storage subdirectories, creating attributes, creating users, and providing privileges to users.

- If you use a non-Siebel security adapter, it supports the Siebel Security Adapter Software Developers Kit, described in "Security Adapter SDK" on page 24. You must adapt the applicable parts of the implementation to your security adapter.

Creating Protected Virtual Directories

This topic describes how to create virtual directories in a Web SSO implementation. Creating virtual directories allows users to access a Siebel application and anonymously browse specific views while requiring Web SSO authentication to access other views in the application.

This task is an optional step in "Process of Implementing Web Single Sign-On" on page 182.

Protected virtual directories are used with Siebel Business 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. and the user must enter a Web SSO login to proceed.

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

- Create the virtual directory.

  Optionally, instead of creating a new virtual directory, you can modify an existing virtual directory.

- Specify to the Web server a particular DLL file that allows the SWSE to communicate with the Web server.

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

Use the following procedure to create a virtual directory.

To create a virtual directory on Microsoft Internet Information Server

1. Start the Internet Service Manager. Choose Programs, Administrative Tools, and then the Internet Service Manager option.
2. In the Internet Service Manager explorer, right-click the default Web site, choose New, and then the Virtual directory option.

   The New Virtual Directory wizard appears.
3. Enter a virtual directory name for a Siebel application, then click Next. For example, enter p_eservice as a virtual directory for Siebel eService.
4. Enter the full path to the *SWEAPP_ROOT*`\public` directory, then click Next (where *SWEAPP_ROOT* is the directory in which you installed the SWSE).

   This subdirectory contains the contents to publish to the site.
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.

Use the following procedure to specify the DLL file that allows the SWSE to communicate with the Web server.

NOTE: The following procedure applies if you are using the Microsoft IIS Web server as your single sign-on authentication service. If you are using a different Web SSO solution, you might have to configure the virtual directory differently.

To allow the SWSE 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.
4. Click Browse, navigate to and select the sweiis.dll file in the *SWEAPP_ROOT*`\bin` directory, and then click Open (where *SWEAPP_ROOT* is the directory in which you installed the SWSE).

   The Add/Edit Application Extension Mapping dialog box appears, including the path to the sweiis.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 Integrated Authentication check box, and uncheck all others. Ensure that the Allow Anonymous Access box is unchecked.
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.

About 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 Business Applications, as described in "Seed Data" on page 353. Its login name is LDAPUSER, and its default password is LDAPUSER. It is recommended that you change the password. If this login name is not present, create it.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Setting Up the ADSI Directory

This topic describes how to set up the ADSI directory for a Web SSO implementation.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

In the implementation of Web SSO outlined, the ADSI directory performs two functions that might be handled by two separate entities in other Web SSO implementations.

- Users are authenticated through the ADSI directory performing its function as the Microsoft IIS Web server directory.
- The ADSI directory serves as 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 ADSI directory as the directory that provides the user IDs and the Siebel database account for authenticated users.
- Configure the Microsoft IIS Web server to authenticate against the Active Directory.

Configuring the ADSI Directory

The following procedure describes the steps involved in configuring the ADSI directory.

To configure the ADSI directory

1. Select a subdirectory in the ADSI directory to store users, for example, the Users subdirectory under the domain-level directory.

   You cannot distribute the users of a single Siebel application in more than one subdirectory. However, you can store multiple Siebel Business Applications' users in one subdirectory.

2. Define the attributes to use for the following user data (create new attributes if you do not want to use existing attributes):

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

3. Password. Assign a user password to each user using the ADSI directory user management tools. The user password is not stored as an attribute.

   NOTE: A user password is required for the ADSI directory only in its role as the Microsoft IIS Web server directory, which is the authentication service in this configuration. 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.

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

About Configuring the Microsoft IIS Web Server

You must configure the Microsoft IIS Web server to authenticate against the Active Directory. You can configure your Microsoft IIS Web server to use Basic authentication.

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

To implement Web SSO, you must create users in the ADSI directory, as described in this topic.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Create three users in the directory using values similar to those shown in Table 18 on page 188. The attribute names, sAMAccountName and Password, are those suggested in this example. Your entries might vary, depending on how you make attribute assignments in "Setting Up the ADSI Directory" on page 186.

Table 18. Directory Records

User	sAMAccountName	Password	Database Account

Anonymous user	■ 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 353, for a Siebel customer or partner application. For example, for 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=LDAPUSER
			password=*P*

Application user	APPUSER or a name of your choice	APPUSERPW or a password of your choice	A database account is not used for the application user.

A test user	TESTUSER or a name of your choice	TESTPW or a password of your choice	username=LDAPUSER
			password=*P*

The database account for all three users is the same, and must match the database account reserved for externally-authenticated users described in "About Creating a Database Login" on page 186. *P* represents the password in that database account. For information about formatting the database account attribute entry, see "Requirements for the LDAP or ADSI Directory" on page 118.

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

Complete other attribute fields for each user, as required.

Adding User Records in the Siebel Database

This topic describes how to create a record in the Siebel Database that corresponds to the test user you created in "Creating Users in the Directory" on page 187.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

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 233.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
2. Navigate to the Administration - User screen, and then the Users view.
3. In the Users list, create a new record.
4. Complete the following fields for the test user, then save the record. Use the indicated guidelines. Suggested entries are for this example. You can complete other fields, but they are not required.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. For example, TESTUSER. 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 32 on page 354.

   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 32 on page 354. You can complete other fields, but they are not required.

   This record must also match the anonymous user you create in "Creating Users in the Directory" on page 187. You can adapt a seed data anonymous user or create a new anonymous user for a Siebel employee application.

Setting Authentication Parameters in the SWSE Configuration File (eapps.cfg)

To implement Web SSO authentication, you must specify values for parameters in the SWSE configuration file, eapps.cfg, as indicted in this topic.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Provide parameter values in the eapps.cfg file, as indicated by the guidelines in Table 19 on page 190. For information about editing eapps.cfg parameters and about the purposes for the parameters, see "Parameters in the eapps.cfg File" on page 335.

Table 19. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
[defaults]	Various	The values of the parameters in this section are overridden by the parameter values you set in the sections for individual applications. For this scenario, you set Web SSO and related parameters in application-specific sections.
The section particular to your application, such as one of these: [/eservice_enu] [/callcenter_enu] where _enu is the language code for U.S. English.	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. Typically, password encryption applies to the eapps.cfg file. In this case, you must specify the encrypted password. See "Managing Encrypted Passwords in the eapps.cfg File" on page 45.
	SingleSignOn	Enter TRUE to implement Web SSO.
	TrustToken	Enter `HELLO`, or a contiguous string of your choice. In Web SSO mode when used with a custom security adapter, the specified value is passed as the password parameter to a custom security adapter—but only if the value corresponds to the value of the Trust Token parameter defined for the custom security adapter. Typically, password encryption applies to the eapps.cfg file. In this case, you must specify the encrypted value. See "Managing Encrypted Passwords in the eapps.cfg File" on page 45.

Table 19. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
	UserSpec	Example entry: 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	Example entry: Server REMOTE_USER is a Web server variable.
	ProtectedVirtualDirectory	Generally, enter the name of the protected virtual directory that you created in "Creating Protected Virtual Directories" on page 184. **NOTE:** It is recommended that this parameter is always used in a Web SSO implementation.
[swe]	IntegratedDomainAuth	Set to TRUE for Windows Integrated Authentication. This parameter is FALSE by default.

Setting Authentication Parameters for the Siebel Gateway Name Server

To implement Web SSO authentication, you must specify values for the Gateway Name Server parameters listed in this topic.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Set each Siebel Gateway Name Server parameter listed in Table 20 on page 192 for the component that corresponds to the Application Object Manager for the application you are implementing, such as Call Center Application Object Manager or eService Application Object Manager. Set the parameters at the component level and follow the guidelines provided in the table.

For information about setting Siebel Gateway Name Server parameters and the purposes for the parameters, see "Siebel Gateway Name Server Parameters" on page 341.

CAUTION: If you do not set the AllowAnonUsers parameter listed in Table 20 on page 192 to TRUE, browser looping behavior can occur.

Table 20. Siebel Gateway Name Server Parameters

Subsystem	Parameter	Guideline
InfraUIFramework	AllowAnonUsers	Enter TRUE.
	SecureLogin	Enter TRUE or FALSE. If TRUE, the login form completed by the user is transmitted over a Secure Sockets Layer (SSL). For information about other requirements for secure login, see "Login Security Features" on page 200.
Object Manager	OM - Proxy Employee	Enter PROXYE.
	OM - Username BC Field	Leave empty.

Table 20. Siebel Gateway Name Server Parameters

Subsystem	Parameter	Guideline
Security Manager	Security Adapter Mode	The mode for the security adapter. Values include: ■ DB ■ LDAP ■ ADSI ■ CUSTOM This parameter can be set at the Enterprise, Siebel Server, or component level. For more information, see Chapter 6, "Security Adapter Authentication."
	Security Adapter Name	The name of the security adapter. Names of security adapters provided by default include: ■ DBSecAdpt ■ LDAPSecAdpt ■ ADSISecAdpt This parameter can be set at the Enterprise, Siebel Server, or component level. For more information, see Chapter 6, "Security Adapter Authentication."
The enterprise profile or named subsystem for the security adapter you are using. For example: ■ DBSecAdpt for the database security adapter. ■ LDAPSecAdpt for the LDAP security adapter. ■ ADSISecAdpt for the ADSI security adapter.	Various	For more information about configuring parameters for each security adapter, see Chapter 6, "Security Adapter Authentication." See also Appendix B, "Configuration Parameters Related to Authentication."

Editing Parameters in the Application Configuration File

If you are implementing Web SSO authentication for the Developer Web Client, you must specify the parameter shown in Table 21 on page 194 in the configuration file for the Siebel application you are implementing. For information about editing an application's configuration file and about the purposes of the parameters, see "Siebel Application Configuration File Parameters" on page 348.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Table 21. Siebel Business Applications Configuration File Parameter Values

Section	Parameter	Guidelines for ADSI Security Adapter
[InfraUIFramework]	AllowAnonUsers	Enter TRUE. **NOTE:** If you do not set this parameter to TRUE, browser looping behavior can occur.

The AllowAnonUsers parameter in the InfraUIFramework section of the application configuration file applies to Developer Web Clients only. The corresponding AOM parameter, which applies to Web Clients, is set using Siebel Server Manager, and is listed in Table 20 on page 192. For a list of Siebel application configuration files, see *Siebel System Administration Guide*.

Restarting Servers

You must stop and restart the following Windows services on the Web server computer to activate changes you make to AOM configuration parameters when implementing Web SSO.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Stop and restart the following services:

- **Microsoft IIS Admin service and Worldwide Web Publishing service.** Stop the Microsoft IIS Admin service, and then restart the Worldwide Web Publishing Service. The Microsoft IIS Admin service also starts because the Worldwide Web Publishing Service is a subservice of the Microsoft IIS Admin service.
- **Siebel Server system service.** Stop and restart the Siebel Server. For details, see *Siebel System Administration Guide*.

Testing Web SSO Authentication

After performing all the tasks required to implement Web SSO authentication, you can verify your implementation using the procedure in this topic.

This task is a step in "Process of Implementing Web Single Sign-On" on page 182.

Perform the following procedure to confirm that the Web SSO components work together to:

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

To test Web SSO authentication

1. On a Web browser, enter the URL to your Web site, for example:

   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 gain access to the Web site.

3. On a Web browser, enter the URL to your Siebel application, for example:

   http://www.mycompany.com/eservice

   Alternatively, if you provide a link on the Web site, click it.

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

Digital Certificate Authentication

A digital certificate is a digital document that includes the public key bound to an individual, organization, or computer. 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 Business Applications support X.509 digital certificate authentication by the Web server. The Web server performs the digital certificate authentication and Siebel Business Applications accept the authentication result in the form of Web SSO.

For customers who have an existing PKI (Public Key Infrastructure) with client certificates, Siebel Business Applications support the use of X.509 certificates to authenticate the users of an application. This authentication is accomplished 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 "About Implementing Web SSO Authentication" on page 181, with the following specific guidelines:

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

Parameter	Comment
SingleSignOn = TRUE	None
TrustToken = HELLO	None
ClientCertificate = TRUE	None
UserSpec = CERT_SUBJECT or REMOTE_USER	For client authentication on Windows and AIX, use CERT_SUBJECT. For other UNIX operating systems, use REMOTE_USER.
SubUserSpec = CN	This parameter value tells the application to extract the username from the certificate name. For the Oracle iPlanet Web Server (formerly known as the Sun Java System Web Server), this setting is ignored.
UserSpecSource = Server	None

- Set the Siebel Gateway Name Server parameter, SecureBrowse, to False for the component that corresponds to the Application Object Manager for the application you are implementing, such as Call Center Application Object Manager.
- For each security adapter (such as LDAPSecAdpt) that is to support certificate-based authentication, define the following parameter values:

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

Configuring the User Specification Source

The User Specification Source option can be implemented in a Web SSO authentication strategy.

In a Web SSO implementation, the SWSE 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.

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 must only be set after the user is authenticated, and it must 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.

The following procedure describes how to specify the source of a username: either a Web server environment variable or an HTTP request header variable.

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, for example, [/eservice].
  - UserSpec = *name of the variable*

    For example, set UserSpec to `REMOTE_USER` if UserSpecSource is set to Server. If UserSpecSource is set to Header, the value of UserSpec is the variable that is passed into the HTTP header; the name of the variable must not be prefaced with HTTP_.

  - UserSpecSource = Server, if you use a 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 Microsoft IIS Web server, first configure the Microsoft IIS Web server to allow anonymous access. You make this security setting for the default Web site in the Microsoft IIS Service Manager.

For information about setting parameters in the eapps.cfg file, see "Parameters in the eapps.cfg File" on page 335.

8 Security Features of Siebel Web Server Extension

This chapter describes several options that relate to security issues and the Siebel Web Server Extension (SWSE). It includes the following topics:

Configuring a Siebel Web Client to Use SSL

You can configure Siebel Business Applications to specify whether or not URLs must use SSL over HTTP (HTTPS protocol) to access views in Siebel Business Applications. You can specify that HTTPS must be used to access specific views, to access all views, or is not required to access views.

If you use the HTTPS protocol, be aware of the following issues:

- You can switch between secure and nonsecure views in Siebel customer applications, but not in employee applications (such as Siebel Call Center). For employee applications, if any views are to be secure, then all views must be secure.
- Your Web server must be configured to support HTTPS.

  You must install a certificate file on the Web server with which you want to secure communication. For more information, see "About Certificates and Key Files Used for SSL Authentication" on page 67.

Two factors determine whether or not 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.

  You can set the Secure property of a specific view to indicate whether or not the HTTPS protocol must be used to access the view. The ability to selectively secure individual views applies to standard interactivity applications only, not high interactivity applications.

  For information about the Secure attribute for a view, see *Configuring Siebel Business Applications*.
- The value (TRUE or FALSE) of the SecureBrowse component parameter.

  You can specify a value for the SecureBrowse parameter to indicate whether or not the HTTPS protocol must be used to access all the views in an application.

The following procedure describes how to configure your application to use HTTPS or HTTP for the views in an application.

To configure your application to use HTTPS or HTTP for views

- Using Siebel Server Manager, specify one of the following values for the SecureBrowse component parameter:
  - SecureBrowse is set to TRUE. If SecureBrowse is set to TRUE, HTTPS is required for all views in the application, regardless of how the Secure attribute is set for individual views.
  - SecureBrowse is set to FALSE. If SecureBrowse is set to FALSE, then HTTP is used for all views in the application, except for views for which the Secure attribute is set to TRUE. Secure views require HTTPS.

  NOTE: In releases of Siebel Business Applications before Siebel CRM 8.0, values for the SecureLogin and SecureBrowse parameters for Siebel Web clients were specified in the [SWE] section of the Siebel application configuration file. Since Siebel CRM 8.0, SecureLogin and SecureBrowse are Application Object Manager (AOM) parameters which are set using Siebel Server Manager.

You can also specify that user credentials entered at login are transmitted from the Web client to the Web server using the HTTPS protocol by setting values for the SecureLogin parameter. For information on how to set this parameter, see "Login Security Features" on page 200. For general information about using SSL with Siebel Business Applications, see Chapter 5, "Communications and Data Encryption."

Login Security Features

This topic describes features and considerations associated with user login to Siebel Business Applications. A login page or a login form embedded in a Siebel application page collects user credentials.

A user must login, thereby identifying himself or herself as a registered user, to be allowed access to protected views in Siebel Business 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 *Configuring Siebel Business Applications*. For information about anonymous browsing, see "Configuring the Anonymous User" on page 170.

Siebel Business Applications also provide other features on a login form besides user credentials collection, such as remembering a username 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.

Implementing Secure Login

With secure login, you can specify to the Siebel Web Engine to transmit user credentials entered in a login form from the browser to the Web server by using Secure Sockets Layer (SSL)—that is, over HTTPS.

Secure login can be implemented in the following authentication strategies:

- Security adapter authentication: database authentication

- Security adapter authentication: LDAP, ADSI, or custom
- Web SSO authentication

For each Siebel application where you want to implement secure login, you set the value of the SecureLogin component parameter to TRUE. The following procedure demonstrates how to set this parameter for the Siebel Call Center application. To implement secure login, you must also have a certificate from a certificate authority on the Web server where you installed SWSE.

To implement secure login

1. Navigate to the Administration - Server Configuration screen, and then the Servers view.
2. Select the Siebel Server of interest.
3. Click the Components view and select the component of interest. For example, select Call Center Object Manager (ENU) in a U.S. English deployment if you want to set secure login for the Siebel Call Center application.
4. Click the Parameters view and select the record for SecureLogin.
5. In the Value on Restart field, enter TRUE.
6. Restart the component to apply the change.

   For information about administering Siebel Server components, see *Siebel System Administration Guide*.

For information about setting Siebel configuration parameters, see Appendix B, “Configuration Parameters Related to Authentication.”

Logging Out of Siebel Business Applications

Users of Siebel Business Applications can end a Siebel session by using the application log out features or by closing the browser window.

In Microsoft Internet Explorer, the browser window is closed by choosing File and then Close, or by clicking X in the top-right corner of the window. For Siebel Business Applications that use high interactivity mode, either method of closing the browser window causes the Siebel user to be logged out of the application.

With Siebel Business Applications that use standard interactivity mode, clicking the X box in the top-right corner of the application window closes the window but does not log the user out of the Siebel application. Users of standard interactivity applications must end the Siebel session by choosing File, and then Close from the Web browser menu to make sure they have logged out of the application.

You cannot select File and then Close if Web Single Sign-On authentication is implemented.

Remember My User ID and Password

A user can check the Remember My User ID and Password check box when logging into a Siebel application. By doing so, the user can access the same Siebel application without having to log in again—provided the user did not log out of the Siebel application by selecting the Log Out option from the File menu.

Remember My User ID and Password uses the auto-login credential 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 and the auto-login credential cookie, see "About Using Cookies with Siebel Business Applications" on page 204.

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 "Managing Forgotten Passwords" on page 226.

Account Policies

For enhanced security, you might want to implement the following account policies. Account policies are functions of your authentication service. If you want to implement the following 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 are enforced by Siebel Business Applications.

- An account lockout after a specified number of failed attempts to log in.

  Account lockout protects against password guessing attacks. Siebel Business 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 Business Applications and users will be notified to change their passwords.

Password Expiration

Password expiration is handled by the external LDAP or ADSI directory, and is subject to the configuration of this behavior for the third-party directory product.

For example, when a password is about to expire, the directory might provide warning messages to Siebel Business Applications to display when the user logs in. Such a warning would indicate the user's password is about to expire and must be changed. If the user ignores such warnings and allows the password to expire, then the user might be required to change the password before logging into the application. Or, the user might be locked out of the application once the password has expired.

Password expiration configuration steps for each directory vendor will vary. For more information, see the documentation provided with your directory product. More information about password expiration for use with Active Directory is provided below.

Password expiration can be implemented if you are using security adapter authentication (LDAP, ADSI, or applicable custom security adapter), or if you are using database authentication and password expiration is supported by the RDBMS.

Password Expiration for ADSI Directories

For ADSI directories, factors that affect the password state include the following attributes and parameters:

- Password Never Expires (attribute for user object)
- User Must Change Password At Next Logon (attribute for user object)
- Last Time User Set Password (attribute for user object)
- Maximum Password Age (attribute for domain)
- Password Expire Warn Days (parameter for ADSI security adapter)

When you configure password expiration for ADSI, you add the parameter Password Expire Warn Days (alias PasswordExpireWarnDays) to the ADSI security adapter. Set the value to the number of days you want to provide a warning message before a user's password expires.

NOTE: The attributes Password Never Expires and User Must Change Password at Next Logon are mutually exclusive, and cannot both be checked for a user.

The state of each user's password is determined by the following logic:

- If Password Never Expires is checked for a user, this user will never get a password expired error, regardless of the settings of other attributes.
- Else, if User Must Change Password At Next Logon is checked for a user, this user will get a password expired error, regardless of the settings of other attributes.
- If neither of the above attributes are checked for a user, the following behavior applies:
  - If Maximum Password Age is set to 0 for the domain, the user does not get a password expired error. No password expires in the domain.
  - If Maximum Password Age is not set to 0 for the domain, and if the difference between the current time and the last time a user has set the password (the value of the Last Time User Set Password attribute for the user) is larger than the value of Maximum Password Age, the user gets a password expired error.
  - If the difference between current time and the last time a user has set the password is smaller than the value of the Password Expire Warn Days parameter (set for the ADSI security adapter), the user gets a password expiring warning message.
  - If the difference between current time and the last time the user has set the password is smaller than Maximum Password Age, and larger than Password Expire Warn Days, the user logs in successfully and does not get error or warning message.

Confirm all third-party directory product behavior and configuration with your third-party documentation.

URL Login

Users can log into Siebel Business Applications by presenting user credentials as parameters in a URL. The user does not have to manually type credentials into a login form.

NOTE: When URL login is used, user passwords might be transmitted in clear text over the network. However, you can encrypt the connection using SSL to make sure that user passwords are not transmitted in clear text. For more information about using SSL, see "Process of Configuring Secure Communications" on page 66.

The easiest, but least secure, option for a form of Web SSO to Siebel Business 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.

The following is a sample showing the URL syntax:

```
http://siebel.com/eservice_enu/
start.swe?SWECmd=ExecuteLogin&SWEUserName=HKIM&SWEPassword=HKIM
```

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 user's login credentials. You must use a SWE expression, as shown in the following example. This example shows a drilldown to a particular service request, after the user has logged in. In this example, the username and password for HKIM are represented using escape characters: %48%4B%49%4D. (Note that such character strings are not secure.)

```
http://siebel.com/eservice_enu/
start.swe?SWECmd=ExecuteLogin&SWEUserName=%48%4B%49%4D&SWEPassword=%48%4B%49%4D
&SWEAC="SWECmd=InvokeMethod,SWEMethod=Drilldown,SWEView=Service+Request+List+View+
(SCW),SWEApplet=Service+Request+List+Applet+(SCW),SWEField=SR+Number,SWERowIds=SWE
RowId0%3d1-15P"
```

You must use commas instead of ampersands (&) as delimiters between arguments in a SWE expression.

About Using Cookies with Siebel Business Applications

Siebel Business Applications running in the Web browser can optionally use cookies for a variety of purposes. Some optional Siebel Business Applications functionality requires the ability to use cookies. More details are provided in the topics about each particular type of cookie.

Unless otherwise noted, all of the cookies described in this topic apply to both high interactivity and standard interactivity applications. All cookies used by Siebel Business Applications are encrypted using standard encryption algorithms provided by RSA.

Siebel Business Applications use the following kinds of cookies:

- **Session cookie.** Manages user sessions for Siebel Web Client users. For details, see "Session Cookie" on page 205.

- **Auto-login credential cookie.** Stores user credentials for Siebel Web Client users. For details, see "Auto-Login Credential Cookie" on page 207.
- **Siebel QuickStart cookie.** Used by the Mobile Web Client when Siebel QuickStart is used. For details, see "Siebel QuickStart Cookie" on page 207.

For information about enabling cookies in the Microsoft Internet Explorer Web browser, see "Enabling Cookies for Siebel Business Applications" on page 207.

Session Cookie

The session cookie consists of the session ID generated for a user's session. This cookie is used to manage the state of the user's session. The session cookie applies to the Siebel Web Client only.

Cookie modes are determined on the SWSE by the setting of the SessionTracking parameter in the eapps.cfg file. The settings are Automatic, Cookie, or URL.

- Using the default SessionTracking setting of Automatic, the SWSE runs in cookie-based mode. However, if a browser does not support cookies or if a user's browser is configured to not allow cookies, the SWSE uses URLs instead of cookies.
- To force the SWSE to always use cookie-based mode, set SessionTracking to Cookie.
- To force the SWSE to always use URLs, and not cookies, set SessionTracking to URL.

For information about setting parameter values in the eapps.cfg file, see Appendix B, "Configuration Parameters Related to Authentication."

Some Siebel Business Applications requirements relating to the settings of the SessionTracking parameter are as follows:

- The Quick Print feature requires that SessionTracking be set to either Automatic (the default) or URL. For information about using this printing feature, see *Siebel Fundamentals*. For information about browser requirements for this feature, see *Siebel System Administration Guide*.
- Inbound EAI HTTP Transport requires cookie-based mode. You can omit the SessionTracking parameter, or set it to either Automatic (the default) or Cookie, in each eapps.cfg file section whose name starts with eai. For more information about inbound EAI HTTP Transport, see *Transports and Interfaces: Siebel Enterprise Application Integration* and other relevant Siebel EAI documentation.
- Remember My User ID and Password requires that SessionTracking be set to either Automatic (the default) or Cookie. Make sure that cookies are enabled in the browser. See also the description of the auto-login credential cookie.

For information about server redirection mechanisms that involve cookies, see *Siebel Portal Framework Guide*.

Session Tracking Using Cookies

This topic describes the behavior of cookie-based mode. Cookie-based mode applies when SessionTracking is set to `Cookie`, or when SessionTracking is set to `Automatic` and the user's browser accepts cookies.

When a user successfully logs into the application, a unique session ID is generated. The components of the session ID are generated in the Siebel Server and sent to the Session Manager running in the SWSE. In cookie-based mode, the session ID is passed to the user's browser in the form of a nonpersistent cookie.

Session ID components include the applicable server ID, process ID, and task ID, combined with a timestamp. All values are in hexadecimal form, as shown:

```
server_ID.process_ID.task_ID.timestamp
```

For example, the session ID might resemble this:

```
sn=!1.132.6024.3ca46b0a
```

The session cookie is nonpersistent and is stored in memory only. It stays in the browser for the duration of the session, and is deleted when the user logs out or is timed out.

The session ID is encrypted in the cookie if the EncryptSessionId parameter is set to TRUE in the eapps.cfg file. The RC2 algorithm encrypts the session ID in the cookie using a 56-bit encryption key. The result of this encryption is then encoded using base64 Content-Transfer-Encoding. Encrypting the session ID prevents unauthorized attackers from capturing the cookie and determining its format.

You can increase the encryption key length to 128-bits for RC2 and up to 256-bits for AES. To increase the encryption key length, you have to install the Siebel Strong Encryption Pack. For more information about the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97.

For every application request that the user makes during the session, the cookie is passed to the Web server in an HTTP header as part of the request. Without a valid cookie in the HTTP header, the Web server will not honor that request.

NOTE: If the user changes the password during an application session, then the password information in the session cookie might no longer allow the user to access the Siebel Reports Server during this session. (This issue applies when using both database authentication and password hashing.) After changing the password, the user must log out and log in again in order to be able to run reports.

Session Tracking Using URLs

This topic describes session tracking behavior when URLs rather than cookies are used to manage user sessions. When SessionTracking is set to URL, or when SessionTracking is set to Automatic and the user's browser does not accept cookies, the session ID is passed as an argument in the SWE construct of the URL. Any URL request passed to the Web server from the browser must include a valid session ID, or the Web server rejects it.

The session ID in the URL is encrypted if the EncryptSessionId parameter is set to TRUE in the eapps.cfg file. The RC2 algorithm encrypts the session ID by using a 56-bit encryption key unless the SWSE specifies the encryption key length. The result of this encryption is then encoded using Base64 Content-Transfer-Encoding. Encrypting the session ID prevents unauthorized attackers from capturing the cookie and determining its format.

You can increase the encryption key length to 128-bits for RC2 and up to 256-bits for AES. To increase the encryption key length, you have to install the Siebel Strong Encryption Pack. For more information about the Siebel Strong Encryption Pack, see "About the Siebel Strong Encryption Pack" on page 97.

A user session is managed using URLs when the browser does not send back a session cookie to the Siebel Web Engine. This event can be caused by cookies being disabled in the user's browser, or by a browser that does not support cookies.

You might want Siebel Business Applications to manage all user sessions using URLs instead of cookies if, for example, security requirements do not permit cookies.

Auto-Login Credential Cookie

The auto-login credential cookie underlies the Remember My User ID and Password feature on the login page. This cookie consists of the username and password for a given user, and the URL string used to access the application. The auto-login credential cookie is persistent and is stored on the user's browser in encrypted form (it is always encrypted). The RC4 algorithm encrypts this cookie. The result of this encryption is then encoded using base64 Content-Transfer-Encoding. This cookie applies to the Siebel Web Client only.

The auto-login credential cookie is not mandatory. It is an optional way to allow users not to have to enter their username and password every time they log in. If the user subsequently accesses the application URL through another browser window, the user information is provided to the application so the user does not have to log in again.

The format of the auto-login credential cookie is as follows:

```
start.swe=encrypted_user_information
```

NOTE: Functionality provided by the auto-login credential cookie is not available if cookie-based mode is not supported.

Siebel QuickStart Cookie

The Siebel QuickStart cookie is created for the Mobile Web Client when Siebel QuickStart is used. This Siebel client supports employee applications in high interactivity mode only.

The Siebel QuickStart cookie, named siebel.local.client, is persistent and does not contain Siebel session ID data.

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

Enabling Cookies for Siebel Business Applications

This topic describes how to enable the Microsoft Internet Explorer Web browser to handle cookies used by Siebel Business Applications.

Review instructions for your supported browser version.

To enable cookies using Internet Explorer 6.0

1. From the Tools menu, select the Internet Options menu item.
2. Click the Privacy tab.
3. In Privacy settings, click Advanced.
4. Verify that Override automatic cookie handling is checked. Also consider:
   - If First-party Cookies is set to Accept, then all Siebel cookies are enabled.
   - If First-party Cookies are blocked, you can still enable the session cookie by checking Always allow session cookies.
5. Click OK, then click OK again.

9 User Administration

This chapter provides information about registering and administering users of Siebel employee, partner, and customer applications. It includes the following topics:

About User Registration

A user who is not a registered Siebel Business Applications user has no authenticated access to the Siebel database. Depending on the Siebel application, unregistered users can be assigned various levels of access. Minimally, the user can access a login page. By default, or by your configuration, unregistered users can also be given 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 Business 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 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, might or might 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 ID and password, is enough to allow this user to be authenticated.

For more information about authentication and propagation of user data, see Chapter 6, "Security Adapter Authentication."

Requirements for User Registration

You must complete the following implementations before you can register users:

- Install your Siebel Business Applications.
- Set up and configure your user authentication architecture.
- Create database accounts for users, as required by your authentication architecture.

For information about user authentication, see Chapter 6, "Security Adapter Authentication."

Seed Data for User Registration

When you install your Siebel Business Applications, you are provided seed data that is related to user registration, user authentication, and user access to Siebel Business Applications. The seed data includes users, responsibilities, positions, an organization, and a database login. References to the seed data appear throughout this chapter. For detailed information on seed data and for procedures for viewing and editing seed data, see Appendix C, "Seed Data."

Configuring Anonymous Browsing

This topic provides information about anonymous browsing and how to configure it for Siebel Business Applications. The following topics provide more detailed information:

- "About Anonymous Browsing and Unregistered Users" on page 210
- "Implementing Anonymous Browsing" on page 211
- "Configuring Views for Anonymous Browsing or Explicit Login" on page 212

About Anonymous Browsing and Unregistered Users

Several Siebel Business 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 Application Object Manager (AOM) 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 page.

For information about the anonymous user's role in user authentication, see Chapter 6, "Security Adapter Authentication."

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 to support anonymous browsing, or to require explicit login instead.

For Siebel Business Applications for which anonymous browsing is implemented by default, 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.

Set up your user authentication architecture before configuring an application for user access. Make sure that the anonymous user already exists 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 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 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 these responsibilities to the existing seed responsibility in the anonymous user's 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 Chapter 10, “Configuring Access Control.” For information about assigning a responsibility to a user, see “Internal Administration of Users” on page 233. For information about seed data, see Appendix C, “Seed Data.”

Setting Configuration Parameters for Anonymous Browsing

You must set the following configuration parameters to allow anonymous browsing.

- **AllowAnonUsers.** Set this parameter in the Siebel application configuration file to TRUE.

  For information about setting parameter values in application configuration files, see “Siebel Application Configuration File Parameters” on page 348.

- **AnonUserName.** This parameter from the eapps.cfg file is the user name for an anonymous user that is stored in the directory and also in the Siebel database.

  The anonymous user provides binding between the directory and the AOM 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.

  For information about setting parameter values in the eapps.cfg file, see “Parameters in the eapps.cfg File” on page 335.

- **AnonPassword.** This parameter from the eapps.cfg file is the authenticated password that is paired with AnonUserName.

Configuring Views for Anonymous Browsing or Explicit Login

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 *Configuring Siebel Business Applications*.

To set or remove the explicit login requirement for a view

1. Start Siebel Tools.
2. From the Tools menu, choose the Lock Project menu item.
3. In Object Explorer, select the View object type.

   The Views list appears.

4. Select a view.

5 For each view, set the Explicit Login property to TRUE for explicit login. Or, set it to FALSE to allow anonymous browsing.

6 Recompile the Siebel repository file, and unlock the project.

About Self-Registration

Several Siebel Business Applications allow users to self-register as default functionality. This topic observes the following principles about self-registration functionality that is provided by default with your Siebel Business Applications:

- Self-registration applies to Siebel customer and partner applications.
- Self-registration can be implemented only in Siebel Business Applications whose clients use standard interactivity. It cannot be implemented for Siebel employee applications or for any other Siebel application that uses the high interactivity client.
- You can configure any eligible Siebel application to either allow or disallow self-registration.
- You implement LDAP or ADSI security adapter authentication with Siebel Business 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 Business 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 Business Applications, including user self-registration. For information about user authentication, see Chapter 6, "Security Adapter Authentication."

Self-registration functionality for Siebel customer and partner applications is included in your Siebel Business Applications installation.

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 Sales.** A user self-registers to be allowed to make an online purchase.
- **Siebel Partner Portal.** A user self-registers as an individual to become a partner user with limited access, or a user self-registers as a request for his or her company to be approved as a partner. In either case the user is assigned a limited responsibility that contains views to master data, but not to transactional data. This responsibility differs from that for a partner user in an approved partner company. For more information on registering partners and partner users for Siebel Partner Portal, see *Siebel Partner Relationship Management Administration Guide*.

Self-registering involves the following steps:

1 The user clicks New User on a Siebel Business Applications page—for example, the Siebel eService home page.

The Personal Information form appears.

2 The user completes the form, then clicks Next. For example, fields for Siebel eService are shown below.

Field	Guideline
First Name	Required. Enter any name.
Last Name	Required. Enter any name.
Email	Required. Enter any valid email address.
Time Zone	Required. Specify the time zone.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. For information about user authentication architectures, see Chapter 6, “Security Adapter Authentication.”
Verify Password	Required when Password is required.
Challenge Question	Required. The user enters a phrase for which there is an answer typically known only to this user. 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 Partner Portal or Siebel Sales, the user does one of the following:

- A user who self-registers for Siebel Partner Portal chooses to register as an individual or to request that his or her company be approved to become a partner. In either case, the user completes a form requiring company information.

- A user who self-registers for Siebel Sales completes forms to provide some or all of the following: payment information, address information, or wireless access 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

Self-registration comprises several components:

- 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.

Self-Registration and 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.

Different Siebel Business Applications in the same implementation can use different anonymous users. Two user records, identified by their user IDs GUESTCST and GUESTCP, are provided as seed data in the Siebel database for use as anonymous users. Appendix C, "Seed Data," describes seed data users, responsibilities, and the Siebel Business 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.

NOTE: When a user self-registers through partner applications, such as Siebel Partner Portal, data is also written to the Contact business component (or equivalent).

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 determines 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 Business 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 value 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. You cannot directly modify a seed responsibility.

For information about creating a responsibility or adding views to a responsibility, see Chapter 10, "Configuring Access Control."

Setting Configuration Parameters for Self-Registration

The user directory can be administered through Siebel Business 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.

Set the PropagateChange parameter to TRUE for the security adapter in order for user data, including user name and password, to propagate to the user directory when users self-register from the Siebel Web Client. For information about setting this parameter, see "Siebel Gateway Name Server Parameters" on page 341.

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 for Self-Registration

When you install your Siebel Business Applications, you are provided several workflow processes that control self-registration for several Siebel Business Applications. The self-registration 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 Sales. 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

The registration workflow processes branch at various stages depending on these cases:

- The application is Siebel Partner Portal.
- The application is other than Siebel Partner Portal. This is the default case, and it includes Siebel Sales, Siebel eService, Siebel Customer, Siebel Training, Siebel Events, and Siebel Marketing.

Table 22 on page 218 lists the views specified in the workflow processes that provide interactive forms during self-registration.

Table 22. Self-Registration Workflow Views

View Name	Applications Using This View	Description
VBC User Registration Initial Form View VBC User Registration Password Error Msg View VBC User Registration Missing Info Msg View VBC User Registration Legal Confirmation View VBC User Registration Login Error Msg View VBC User Registration Confirmation Msg View VBC User Registration Declined View VBC User Registration Create User Error Msg View VBC User Registration Security Setup Error Msg View	All	These views, common to all applications that use the User Registration Process, comprise two groups: ■ 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.
VBC User Registration Contact Information View	Default	This view is the Contact Information form used by default.
VBC User Registration Company Information - Company View (SCW) VBC User Registration Company Information - Individual View (SCW) VBC User Registration Contact Information View (SCW)	Siebel Partner Portal	These views collect contact information and information about the user's company.

For the self-registration workflow processes to be invoked, they must have the Active status.For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

Modifying Self-Registration Views and Workflows

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.

The views used in the self-registration workflow processes are based on the VBC User Registration virtual business component, which collects the user data. The data is written to the User Registration business component and the Siebel database only when all stages of collecting user data are completed. Before you make any modifications, you have to understand how these components handle the user data.

The User Registration and User business components are both based on the same database tables: S_PARTY, S_CONTACT, and S_USER. 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 process provides the following benefits:

- If the self-registration process is terminated before completion, you do not have 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 *Configuring Siebel Business Applications*.

Revising a Workflow Process

The self-registration workflow processes for your business might 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. For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

Creating Custom Business Services

Siebel Business 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 *Configuring Siebel Business Applications*.

Redefining Required Fields

As default functionality, a user who is self-registering is required to provide entries in certain fields. These fields can differ depending on the application. A required field is indicated in the user interface by an asterisk, where the field appears in a form.

For a view used in the self-registration workflow processes, you can change whether a field is required. Use Siebel Tools to determine the view that includes a self-registration field.

The CSSSWEFrameUserRegistration frame 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, use Siebel Tools to modify the applet that contains the form. The following procedure is intended to present the main steps you must perform in Siebel Tools. For detailed information about working with applets and views in Siebel Tools, see *Configuring Siebel Business Applications*.

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 type.

The Views list appears.

4 Select a view that includes a self-registration field.

5 In Object Explorer, expand the View Web Template child object type, 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 Items list.

6 In the View Web Template Items 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 type, and then expand the Control child object type.

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 that appears in the Name column—for example, MiddleName.

9 In Object Explorer, click the Applet User Prop object type.

The Applet User Properties list displays the user properties for the applet in the Applets list.

10 With the Applet User Properties list active, from the Edit menu, select the New Record menu item.

A new user property record appears.

11 Complete the following fields. Use the indicated guidelines.

Field	Guideline
Name	Required. Enter Show Required and a sequence number one greater than the highest existing sequence number. For example, if Show Required 6 is the highest sequenced entry, enter Show Required 7. This entry is case-sensitive.
Value	Required. The name of the field that you recorded in Step 8 on page 221, 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.

NOTE: To make a required field no longer required in the user interface, follow the steps in the preceding procedures, with the following exception: in the Applet User Properties list, either check the Inactive column for the record you added in Step 10 on page 221, 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 last name, into a text box on a form.
- The text box is mapped to a field in the VBC User Registration virtual business component, such as LastName. Consequently, the data is written to that field.
- Data from the virtual business component VBC User Registration is written to the User Registration business component. The User Registration business component writes to the same database tables as the User business component. Consequently, each field is actually stored as part of a user record.

  NOTE: No data from the VBC User Registration virtual business component 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 order:

- Siebel Tools tasks
- Siebel Workflow tasks (using Business Process Designer in Siebel Tools)

Siebel Tools Tasks for Adding or Deleting Fields

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 identify the major tasks required. For detailed information about modifying views and applets, see *Configuring Siebel Business Applications*.

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 field in the VBC User Registration virtual business component. Use the exact same field name.
7. Configure the appropriate applet to expose the new field.
8. If necessary, configure the new field so that a self-registering user is required to complete it.

9 Recompile the Siebel repository file, and unlock the User Registration project.

NOTE: 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.

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 *Configuring Siebel Business Applications*.

Creating a New View for Self-Registration

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 *Configuring Siebel Business Applications*.

Managing Duplicate Users

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 by the Check User Key step.

Modifying Updated Fields for a Duplicate User

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 *Configuring Siebel Business Applications*.

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 VBC User Registration virtual business component that you want to exclude from updating.
   a. In the Object Explorer, click Business Component.
   b. In the Business Components list, query or scroll to select the VBC User Registration business component.
   c. In the Object Explorer, expand the Business Component item, then select the Field child item.
   d. In the Fields list, query or scroll to select the field you will exclude.
4. Add the appropriate business service user property.
   a. In the Object Explorer, click Business Service.
   b. In the Business Services list, query or scroll to select the User Registration business service.
   c. In the Object Explorer, expand the Business Service item, then select the Business Service User Prop child item.
   d. In the Business Service User Props list, create a new record.

   Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter `Exclude From Update` *number*, where *number* is the next number in the sequence for this particular user property. For example, enter `Exclude From Update 3`. This entry is case-sensitive.
Value	Enter the field name from the VBC User Registration virtual business component that you noted in Step 3 on page 224.

5. Recompile the Siebel repository file and unlock the User Registration project.

Modifying 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 *Configuring Siebel Business Applications*.

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 and the Business Service User Properties child list appear.
5. In the Business Services list, select User Registration.
6. Delete a field from the duplication comparison:
   a. In the Business Service User Properties list, select the record with name `App User Key: Default` *`number`* or `App User Key: Siebel eChannel` *`number`* (for Siebel Partner Portal) 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. Use the indicated guidelines.

Field	Guideline
Name	Enter `App User Key: Default` *`number`* or `App User Key:` *`application number`*, where *`application`* is the name of the Siebel application, and *`number`* is the next number in the sequence for this particular user property. This entry is case-sensitive. For example, you might enter `App User Key: Default 2` to add a field for Siebel eService, or `App User Key: Siebel eChannel 4` to add a field for Siebel Partner Portal.
Value	Enter the name of the field in the User Registration business component that you want to add to the duplication check.

8. Recompile the Siebel repository file and unlock the User Registration project.

Deactivating the Duplicate User Check

You can deactivate the duplicate user 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 Framework: Workflow Guide*.

To deactivate the self-registration deduplication check

1. In Siebel Tools, select Workflow Process in the Object Editor.
2. Query or scroll to select User Registration SubProcess.
3. Create a revised copy of User Registration SubProcess, as described in "Modifying Self-Registration Views and Workflows" on page 219.
4. Right-click and choose Edit Workflow Process to edit the revised copy.

   The Process Designer appears, showing the current workflow process.
5. For each process step that applies to your application, record the sources of all connectors to the step and the destination of the single connector from the step. Reroute the connectors to bypass the step. For all Siebel Business Applications, choose the Check User Key step.
6. Delete the bypassed process step, which must now not be the source or destination of any connector.
7. Right-click and choose All Processes.

   The Workflow Processes list appears again. The revised process is still selected.
8. Click Deploy.

Managing Forgotten Passwords

This topic describes how to manage forgotten passwords.

If a user who has previously self-registered on a Siebel customer or partner 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.

Forgot Your Password? is a default feature of Siebel customer and partner applications, but it is available only if you implement LDAP or ADSI security adapter authentication. If you want to implement 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. Consult your third-party vendor documentation for more information about performing these tasks.

For more information about managing forgotten passwords, see the following subtopics:

- "User Experience for a Forgotten Password" on page 227
- "Defining Password Length for System-Generated Passwords" on page 227
- "Architecture for Forgotten Passwords" on page 229

- "Modifying the Workflow Process for Forgotten Passwords" on page 229
- "Modifying Workflow Process to Query Null Fields" on page 230
- "Modifying Workflow Process to Request Different Identification Data" on page 231

User Experience for a Forgotten Password

A user who has previously self-registered can retrieve a new password, if he or she has forgotten their existing password. On a future login, this user can change the new password in the User Profile view.

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.

Defining Password Length for System-Generated Passwords

This topic describes how to configure the length of passwords generated by Siebel Business Applications for users who had previously self-registered but who have forgotten their password. For information on the forgotten password feature, see "Managing Forgotten Passwords" on page 226 and "User Experience for a Forgotten Password" on page 227.

When a user requests a new password using the Forgot Your Password feature, the User Registration business service invokes the SetRandomPassword method to create the new password. The SetRandomPassword method uses the rand() method to generate a password that is composed of randomly selected alphanumeric characters (the alphabetic characters a to z, and the numerals 0 to 9). The generated password does not contain special characters.

To ensure that generated passwords conform to your company’s policy on password length, you can specify minimum and maximum character lengths for passwords by adding two user properties to the User Registration business service in Siebel Tools. These user properties are RandPassMinLength and RandPassMaxLength. The User Registration business service method, SetRandomPassword, uses the values of these two user properties when it is invoked.

To define minimum and maximum values for password length

1. Open Siebel Tools and, in the Object Explorer, click Business Service.

   The Business Services list appears.

2. In the Business Services list, query or scroll to select the User Registration business service.
3. From the Tools menu, select the Lock Project menu item.
4. In the Object Explorer, click Business Service User Props.

   The Business Service User Props list appears.

5. Right-click in the Business Service User Props list and select New Record from the displayed context menu.

   A new record field appears.

6. Complete the fields for the new record, as shown in the following table.

In this field...	Enter...
Name	RandPassMinLength
Value	Enter the minimum number of characters that your company’s password policy states a password must contain. The default value is 5.

   This defines the minimum number of characters that a password can contain.

7. Step off the record to save changes.
8. Repeat Step 5, Step 6, and Step 7 with modifications for Step 6, as shown in the following table.

In this field...	Enter...
Name	RandPassMaxLength
Value	Enter the maximum number of characters that your company’s password policy states a password must contain. The default value is 15.

   This defines the maximum number of characters that a password can contain.

9. Recompile the Siebel repository file, and unlock the User Registration project.

Architecture for Forgotten Passwords

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 "User Experience for a Forgotten Password" on page 227, 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 fields in the User Registration business component. This 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 the Workflow Process for Forgotten Passwords

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 prove he or she owns the record by answering the challenge question.

Table 23 on page 230 describes the arguments for the FindContact method.

Table 23. FindContact Method Arguments

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	■ 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 that matches the criteria is not identified, 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 Workflow Process to Query 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 Query User step (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.

You make this change by modifying the Query User step for a revised copy of the User Registration Forgot Password Process workflow process, then activating this copy. When you create input arguments, enter the fields and values described in Table 24 on page 231.

Table 24. Values for QueryAllFields Input Argument

Field	Value
Input Argument	QueryAllFields
Type	Literal
Value	Y

For detailed information about modifying workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

Modifying 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, you must do the following tasks:

- Modify the user interface
- Modify User Registration Forgot Password Process input arguments

Modifying the User Interface for User Registration

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 *Configuring Siebel Business Applications*.

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 what field to add. Add to both the VBC User Registration virtual business component and the User Registration business component the field that corresponds to the field you want to add. Use the same names for these fields.

   For more information, see “Modifying Self-Registration Views and Workflows” on page 219.

   a. In the Object Explorer, click Business Component.

   b. In the Business Components list, query or scroll to select the User Registration business component.
   c. In the Object Explorer, expand Business Component, then click its Field child item.
   d. In the Fields list, add the field you require for this business component.
   e. Repeat this process for the VBC User Registration virtual business component.

4. Configure the applet VBC User Registration Initial Form Applet to expose or hide the field.
   a. In the Object Explorer, click Applet.
   b. In the Applets list, query or scroll to select the applet VBC User Registration Initial Form Applet.
   c. In the Object Editor, expand Applet, then click its Control child item.
   d. In the Controls list:
      - If you want to hide a field, select its record in the Controls list and check its Inactive field.
      - If you want to add a field, add a new record in the Controls list. 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 field that you determined in Step 3 on page 231, such as City
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 VBC User Registration Initial Form Applet to display or hide the field.
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 Web templates and applets, see *Configuring Siebel Business Applications*.

Modifying Input Arguments for the Workflow Process

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.

You make this change by modifying the input arguments for the Query User step for a revised copy of the User Registration Forgot Password Process workflow process, then activating this copy. When you create input arguments, enter the fields and values described in Table 25 on page 233.

Table 25. Values for Input Arguments for Query User Step

Field	Guideline
Input Argument	Enter the name of the field in the User Registration business component that you noted in Step 3 on page 231 of "Modifying the User Interface for User Registration" on page 231, such as City. This is the field in the existing user records with which the comparison is made.
Type	Pick Process Property.
Property Name	Pick the process property that corresponds to the field in the User Registration business component that you noted in Step 3 on page 231 of "Modifying the User Interface for User Registration" on page 231, such as City. The process property has the same name as the field, by convention.
Property Data Type	This field automatically populates with the data type of the process property.

Internal Administration of Users

You can provide an employee, a customer, or a partner user with access to one or more Siebel Business 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

Implement the authentication architecture 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:

- **Database security adapter 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.

- **LDAP or ADSI 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.

  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 Siebel user IDs stored in the directory to be managed from within Siebel Business Applications, including allowing Siebel user IDs to be propagated to the directory. For information about user authentication, see Chapter 6, "Security Adapter Authentication."

  NOTE: Make sure the application user has write privileges to the user directory. The application user is the only user who create or modifies users in 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 Business Applications documentation. You must provide authentication credentials to the new user.

Adding a User to the Siebel Database

A record exists for each user of a Siebel application 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 customer applications such as Siebel Sales, 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 Chapter 10, "Configuring Access Control."

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.

NOTE: You can modify field values for existing employees, partner users, or contact users, such as in the event of a name change. However, changing the user ID for such a user presents special issues, because this ID might be stored in various other types of records, using a field such as CREATOR_LOGIN (where a foreign key to the user record is not used instead). Values for such fields are not automatically updated when the user ID is updated. If you change the user ID, you must also update such values in other records.

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, tools, assignment rules, and availability. By doing so, you can use the employee record and its attributes with features such as Siebel Assignment Manager.

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.
2. Navigate to the Administration - User screen, and then the Employees view.

   The Employees list appears.
3. Add a new record.
4. Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier. If you implement database authentication, this field must be the login name for a database account.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. For information about user authentication architectures, see Chapter 6, "Security Adapter Authentication."
Responsibility	Required. Pick one or more responsibilities which include appropriate views for the employee. If the administrator who is creating this user has a value in his or her New Responsibility field, then that responsibility is assigned to the user being created by default. For information about the New Responsibility field, see "Modifying the New Responsibility Field for a User Record" on page 240.

Field	Guideline
New Responsibility	Optional. 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 "Modifying the New Responsibility Field for a User Record" on page 240.
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	Required. 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. (This field appears on the More Info form.)
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. (This field appears on the More Info form.) For information about organization access control, see Chapter 10, "Configuring Access Control."

Completing Employee Setup

You can set up employees either before or after you assign them a responsibility. For more information about completing employee setup, see the initial setup topic in *Siebel Applications Administration Guide*. Also see *Siebel Assignment Manager Administration Guide* and *Siebel Project and Resource Management Administration Guide*.

Deactivating an Employee

You can deactivate an employee by dissociating the employee record from its responsibilities, altering the user ID, changing the employee's status to Terminated, and removing the employee's access to the database.

To deactivate an employee

1. Navigate to the Administration - User screen, and then the Employees view.

   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 might 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. Select the Job Information tab.

6. Change the Employment Status field from Active to Terminated.

7. Remove the employee’s access to the database.

   If you implemented database user authentication, 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 directory (such as LDAP or ADSI) is shared by many applications, do not delete the user from the directory. 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 might 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 Administration - Partner screen in Siebel Partner Manager or another Siebel employee application for which you have licensed this screen.

For information about using the Administration - Partner screen, see *Siebel Partner Relationship Management Administration Guide*.

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 Sales or students who use Siebel Training. 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 Administration - User screen. The procedure in this topic applies to contact users to whom you are providing a login to the Siebel database.

CAUTION: You can modify field values for existing contact users, such as in the event of a name change. However, changing the user ID for such a user presents special issues, because this ID might be stored in various types of records, using a field such as CREATOR_LOGIN (where a foreign key to the user record is not used instead). Values for such fields are not automatically updated when the user ID is updated. If you change the user ID, you must manually update such values in other records.

To add a new contact user

1. Log in as an administrator to a Siebel employee application.
2. Navigate to Administration - User screen, and then the Users view.

   The Users list appears.
3. Add a new record.

4 Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. For information about user authentication architectures, see Chapter 6, “Security Adapter Authentication.”
Account	Pick one or more accounts to associate to the user. Specify one as the primary account. By default, the user sees this account when he or she logs in. For information about the function of the account in delegated administration, see “Delegated Administration of Users” on page 241.
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 his or her New Responsibility field, then that responsibility is assigned to this user by default.
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 “Modifying the New Responsibility Field for a User Record” on page 240.
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.
Work Phone # Home Phone # Fax #	The application interprets only the digits the user provides. Any separators are disregarded.

The new user appears in the Users list.

Promoting a Contact to a Contact User

You can promote an existing contact to a contact user by assigning user credentials and a responsibility to a Person record (a contact).

To promote an existing contact to a contact user

1. Log in as an administrator to a Siebel employee application.
2. Navigate to the Administration - User screen, and then the Persons view.

   The Persons list appears.
3. Select the record of the contact to promote.
4. Enter values for the User ID, Password, Responsibility, and New Responsibility fields, as described in "Adding a New Contact User" on page 238.

Modifying the New Responsibility Field for a User Record

A user record can have a value in the New Responsibility field in the Users view. 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 all types of users (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 can choose whether or not 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 might 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.
2. Navigate to the Administration - User screen, and then the Users view.

   The Users list appears, containing all the employees, partner users, and contact users in the database.
3. In the Users list, select the user record to modify.
4. In the form, pick a new value in the New Responsibility field, then save the record.

   The user must log out and log in for the New Responsibility value to become active.

Delegated 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 for Delegated Administration

Delegated administration is default functionality of most Siebel customer and partner applications, but it is available only if you implement LDAP or ADSI 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. Such configuration guidelines are not provided in Siebel Business Applications documentation.

Delegated administration requires you configure the LDAP or ADSI 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 Business Applications, including delegated administration of users. For information about user authentication, see Chapter 6, “Security Adapter Authentication.”

NOTE: Make sure the application user for your Siebel customer or partner application has write privileges to the user directory.

Access Considerations for Delegated Administration

A delegated administrator (a user at a customer or partner company) has restricted access to user data.

- **Customer applications.** A delegated administrator can only see users who 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 required for delegated administration. Siebel Business Applications provide seed responsibilities for delegated administrators of customer and partner applications.

For information about seed responsibilities, see Appendix C, "Seed Data."

Delegated user administration screens, navigation, and procedures vary somewhat among Siebel Business Applications. The remaining topics describe delegated administration that is representative of customer and partner applications.

Registering Contact Users—Delegated Administration

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. Your host company associates responsibilities with an organization. A delegated administrator can only assign responsibilities to users, including seed responsibilities, that are associated 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. The proxy employee is provided as seed data and is associated with the default organization. As with other seed data that Siebel Business Applications provide, you cannot modify the proxy employee. This means that to associate a delegated administrator with an organization other than the default organization, you have to make a copy of the proxy employee record and rename it. You then assign the renamed proxy employee to the organization that you want to associate the delegated administrator with. A responsibility is associated with an organization by an administrator at your company using an employee application such as Siebel Call Center.

For example, if the Siebel Application Object Manager in use is the eCustomer Application Object Manager (ENU) and the proxy employee (PROXYE) is assigned the position Proxy Employee in Default Organization, the eCustomer Application Object Manager (ENU) runs under the Default Organization context. If you have to run the eCustomer Application Object Manager (ENU) under the China Organization, you create a copy of:

- eCustomer Application Object Manager (ENU) and rename it (for example, eCustomer_China)
- Proxy Employee and rename it (for example, PROXYE_CHINA)

You then assign the modified proxy employee (PROXYE_CHINA) to a position in the China Organization. This results in the application (`http://WebServer/eCustomer_China`) connecting to the China Organization because PROXYE_CHINA is associated with a position in this organization. For more information on the proxy employee, see "Seed Employee" on page 353.

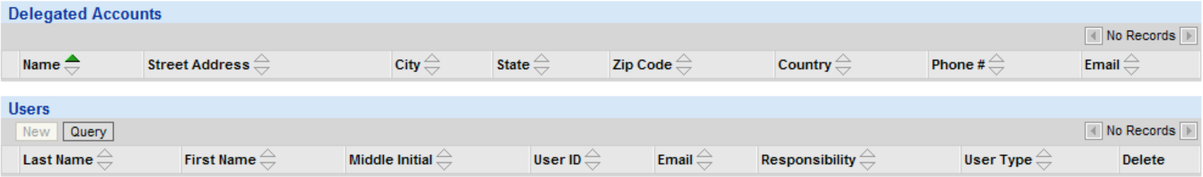
To register a new customer user (by a delegated administrator)

1 Log into a Siebel customer application that implements delegated administration, such as Siebel Sales or Siebel eService.

   NOTE: The delegated administrator must have user type Web Delegated Customer Admin.

2 Click My Account, and then click User Administration under My Company.

   Lists of delegated accounts and associated users appears, as shown below. The lists can vary somewhat by application.



Delegated Accounts

Name	Street Address	City	State	Zip Code	Country	Phone #	Email

Users

Last Name	First Name	Middle Initial	User ID	Email	Responsibility	User Type	Delete

3 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.

4 Create a new record.

5 Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. For information about user authentication architectures, see Chapter 6, "Security Adapter Authentication."
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 "Modifying the New Responsibility Field for a User Record" on page 240.
Home Phone # Work Phone # Work Fax #	The application interprets digits only in these telephone number entries. Any separators are disregarded.

The new record appears in the Users list.

Registering Partner Users—Delegated Administration

A delegated administrator using a partner application, such as Siebel Partner Portal, 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 can assign responsibilities to partner users. The delegated administrator can assign only those responsibilities that your host company has associated with the delegated administrator’s partner organization. An administrator at your company associates partner organizations with responsibilities using an employee application such as Siebel Partner Manager.

To provide a new partner user with access to the database, a delegated administrator must assign a responsibility when registering the partner user.

To register a new partner user (by a delegated administrator)

1. Log into a partner application that implements delegated administration, such as Siebel Partner Portal.

   NOTE: The delegated administrator must have user type Web Delegated Customer Admin.

2. Navigate to Administration.
3. In the Explorer, expand the organization in which you will create the partner user.
4. Click the Users child item to display the users in this organization.
5. In the Edit User form, create a new record to add a new user. Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.

Field	Guideline
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. For information about user authentication architectures, see Chapter 6, “Security Adapter Authentication.”
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.
Responsibility	Pick one or more responsibilities, such as a seed responsibility provided for partner 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 “Modifying the New Responsibility Field for a User Record” on page 240.
Work Phone # Home Phone # Work Fax # Pager #	The application interprets digits only in these telephone number entries. The user can enter any separators.

The new partner user record appears in the Users list.

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 Business Applications. The procedures in this topic are representative of those in Siebel employee, partner, and customer applications. Procedures in individual applications can 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, choose My Account, My Settings, and then User Profile. The User Profile form appears.
   - In a Siebel partner application, choose Profile. The Personal Profile form appears.
   - In a Siebel employee application, from the Tools menu, choose the User Preferences menu item. The User Profile 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, then saves the record.

Changing a Password

If you implement database or security adapter authentication, then a user can change the login password.

If you want to implement 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 Siebel Business Applications views. Configuration guidelines are not provided in Siebel Business Applications documentation.

To change a password, a user accesses the profile form as described in "Editing Personal Information" on page 247, and then completes the appropriate fields. The password-related fields are not editable if the password cannot be changed in the current authentication architecture.

Mobile users using the Siebel Mobile Web Client can also change their passwords for the local database and for synchronization. For details, see *Siebel Remote and Replication Manager Administration Guide*.

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.

Data visibility for a user is generally determined by the active position, rather than by a union of the user's associated positions. However, catalog and group visibility are based upon the user's employee record and are independent of the user's active position. Users who are associated with more than one position have visibility to all records associated with a catalog that is associated with any of their positions (or associated with another applicable access mechanism).

To understand data visibility for a user, you must consider which access-control mechanisms are associated with the user (positions, user lists, access groups, and so on) and with which catalogs or categories those mechanisms are associated.

To change the active position in a Siebel employee application

1. Navigate to the User Preferences screen, and then the Change Position view.

   The Change Position list appears.

2. Click on a position record to select it, and then click Change Position.

   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.

10 Configuring Access Control

This chapter discusses mechanisms you can use to control access to data and Siebel Business Applications functionality. It includes the following topics:

About Access Control

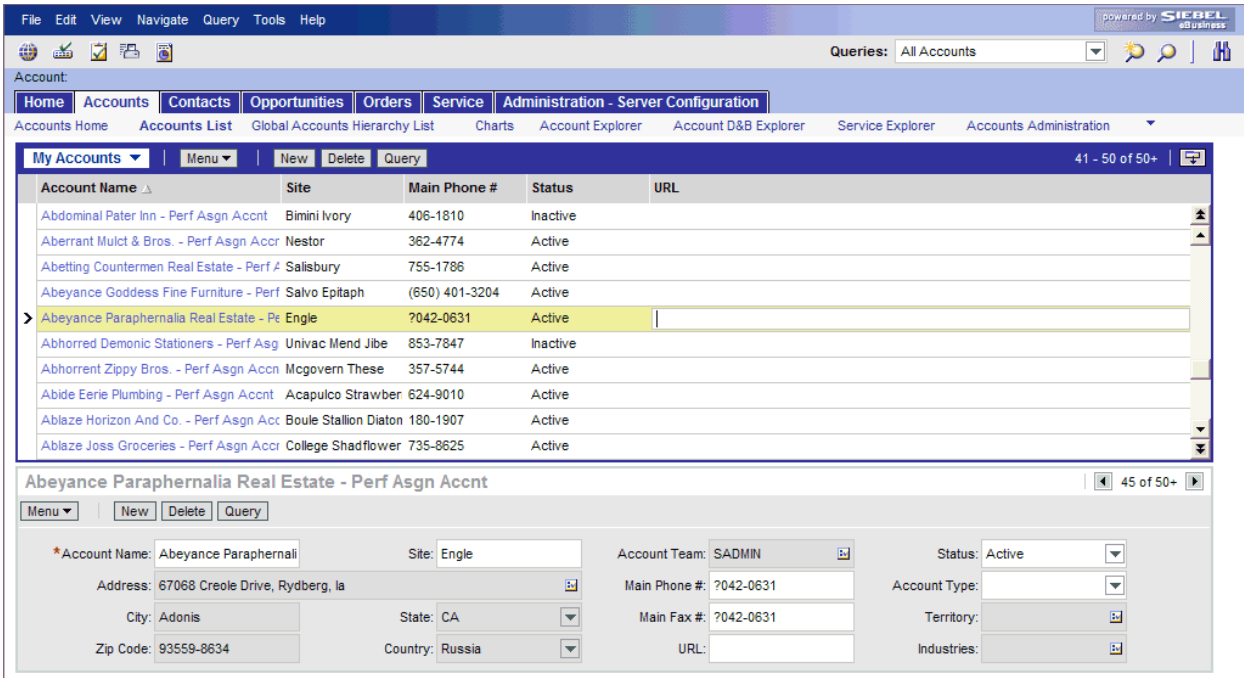
Access control is the term used to describe the set of Siebel Business Applications mechanisms that control user access to data and application functionality.

When reviewing the access control topics, determine how the terminology and concepts presented here correspond to your company's internal terminology and structure. The topics in this chapter explain the mechanisms and their general use, but you will have to decide during the planning stage how to combine the mechanisms to meet your business and security requirements.

In Siebel Business Applications, a screen represents a broad area of functionality, such as working on accounts. Each screen is represented as a tab at the top of the window. In the example below, the Accounts screen is displayed.

Each screen contains multiple views to provide different kinds of access to the data. To the user, a view is simply a Web page. Within a view, the user can see lists of data records or forms, presenting individual or multiple records, and sometimes child records. (These lists and forms are referred to as applets in a configuration context.) Each view (or grouping of views) is represented by text in the link bar below the screen tabs.

For example, Figure 6 on page 250 shows the Account List View, which corresponds to the applet title My Accounts (the current visibility filter selection). Multiple view modes provide access to different views that filter the data differently. In the Account List View, the current user can view accounts owned or assigned to this user. This view includes an Accounts list and an accompanying form with detail for the selected account. Choosing All Accounts from the visibility filter displays the All Account List View instead—assuming the user has access to this view.



Account Name	Site	Main Phone #	Status	URL
Abdominal Pater Inn - Perf Asgn Accnt	Bimini Ivory	406-1810	Inactive	
Aberrant Mulct & Bros. - Perf Asgn Accr	Nestor	362-4774	Active	
Abetting Countermen Real Estate - Perf A	Salisbury	755-1786	Active	
Abeyance Goddess Fine Furniture - Perf	Salvo Epitaph	(650) 401-3204	Active	
Abeyance Paraphernalia Real Estate - Pe	Engle	?042-0631	Active	
Abhorred Demonic Stationers - Perf Asg	Univac Mend Jibe	853-7847	Inactive	
Abhorrent Zippy Bros. - Perf Asgn Accn	Mcgovern These	357-5744	Active	
Abide Eerie Plumbing - Perf Asgn Accnt	Acapulco Strawber	624-9010	Active	
Ablaze Horizon And Co. - Perf Asgn Acc	Boule Stallion Diaton	180-1907	Active	
Ablaze Joss Groceries - Perf Asgn Accr	College Shadflower	735-8625	Active	

Abeyance Paraphernalia Real Estate - Perf Asgn Accnt

*Account Name:	Abeyance Paraphernali	Site:	Engle	Account Team:	SADMIN	Status:	Active
Address:	67068 Creole Drive, Rydberg, la			Main Phone #:	?042-0631	Account Type:	
City:	Adonis	State:	CA	Main Fax #:	?042-0631	Territory:	
Zip Code:	93559-8634	Country:	Russia	URL:		Industries:	

Figure 6. My Accounts View

Access control elements include the following:

- **Application-level access control.** The set of screens that a user has access to are determined by the applications that your company has purchased. Each application is made of a set of available screens.

- **View-level access control.** Within the available screens, you can control the views that are available to a particular user through responsibilities. A responsibility defines a collection of views that represent the data and functionality required to perform a job function.

- **Record-level access control.** You can control data records that each user can see through a variety of mechanisms, including direct record ownership by a user, being on a team working with the record, or being a member of the same organization as the record owner.

The sections that follow examine access control further:

- **Parties.** People, entities representing people, and collections of people are unified as parties. Different party types have different access control mechanisms available. For details, see “Access Control for Parties” on page 251.

- **Data.** The type of data and whether the data is categorized determines which access control mechanisms can be applied. For details, see "Access Control for Data" on page 254.
- **Access control mechanisms.** Access control mechanisms you apply to parties and data determines what data a user sees.

For further information, see also the following:

- "Access Control Mechanisms" on page 256
- "Planning for Access Control" on page 266
- "About Implementing Access Control" on page 272
- "Implementing Access-Group Access Control" on page 289

Access Control for Parties

Individual people, groupings of people, and entities that represent people or groups are unified in the common notion of *parties*. For technical information about how parties function at the data model level, see "Party Data Model" on page 315.

Parties are categorized into the following party types: Person, Position, Organization, Household, User List, and Access Group. Table 26 on page 251 describes the qualitative differences among different parties and identifies the applicable party type for each party.

Table 26. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Person (or Contact)	Person	■ An employee at a customer company. ■ An employee at a competitor's company.	■ 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	Person	■ A registered customer on your Web site. ■ A self-registered partner user, that is, one who has no position.	■ A User is a Person who can log into your database and has a responsibility that defines what application views are accessible. ■ A self-registered partner on a Siebel partner application has a responsibility, but does not have a position like a full Partner User has.
Employee	Person	■ An employee at your company.	■ An Employee is a User who is associated with a position in a division within your company.

Table 26. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Partner User	Person	■ An employee at a partner company.	■ 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.
Position	Position	■ A job title within your company. ■ A job title within a partner company.	■ 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 can have a parent position. It can 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 26. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Account	Organization	■ A company or group of individuals with whom you do business.	■ An account is typically made up of contacts. ■ An account is not a division, an internal organization, or an external organization. ■ An account can have a parent account. It can also have child accounts. ■ An account can be promoted to a partner organization.
Division	Organization	■ An organizational unit within your company such as Manufacturing or Corporate. ■ A group of people operating within a particular country.	■ 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 can have a parent division. It can also have child divisions. ■ Data cannot be associated directly with a division. (Divisions that are not designated as organizations do not drive visibility.)
Organization	Organization	■ An organizational unit within your company, such as your European organization. ■ A partner company.	■ An organization is a division that is designated as an organization. ■ 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 be associated with only one organization: itself or an ancestor division that is also an organization.

Table 26. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Household	Household	■ A group of people, typically a family, who reside at the same residence. ■ A group of purchasers who live in different residences.	■ Typically, a household is a group of individual consumers who are economically affiliated and share a common purchasing or service interest. ■ A household can have any combination of contacts, users, employees, and partner users as members. ■ An individual can belong to more than one household.
User List	User List	■ A support team made up of some internal employees and some partner users.	■ A user list is an ad hoc group of people. It can 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	■ 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.	■ 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 can have a parent access group. It can also have child access groups.

Access Control for Data

The following groupings of data are necessary for purposes of discussing access control:

- **Customer data**
  - Customer data includes contacts and transactional data such as opportunities, orders, quotes, service requests, and accounts.
  - Access is controlled at the data item level, through a mechanism such as individual record ownership or ownership by an organization.
- **Master data**
  - Master data includes the following referential data: products, literature, solutions, resolution items, decision issues, events, training courses, and competitors.

  - Master data can be grouped into categories of similar items—for example, hard drives. Categories can then be organized into catalogs—for example, computer hardware—which are hierarchies of categories. Access can be controlled at the catalog and category levels through access groups, which is the recommended strategy for controlling access to master data. For more information about creating catalogs, see *Siebel eSales Administration Guide*.
  - Master data can be associated with organizations. By associating master data with organizations, access can be controlled at the data item level. This strategy requires more administration than the access group strategy.

  NOTE: Divisions provide a way to logically group positions and assign currencies. Organizations provide a mechanism to control data access.

- **Other data**
  - Other data includes referential data that is not master data, such as price lists, cost lists, rate lists, and SmartScripts.
  - Access is controlled at the data item level.

Data Categorization for Master Data

Master data can be organized into catalogs made up of hierarchical categories. Organizing data this way serves 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. For example: Computer Hardware, Hard Drives, and then Server Drives.
- **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, training subject areas, or channel partners.

A catalog is a single hierarchy of categories, as illustrated in Figure 7 on page 255.

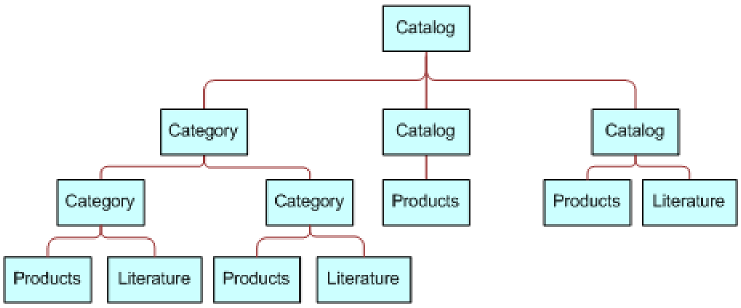


Figure 7. Example Catalog and Category Hierarchy

The following properties apply to catalogs and categories:

- A catalog is a collection or 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.

Access Control Mechanisms

The major access control mechanisms include the following, which are described in the topics that follow:

- **Personal access control.** For details, see "About Personal Access Control" on page 256.
- **Position access control.** This includes single-position, team, and manager access control. For details, see:
  - "About Position Access Control" on page 257
  - "About Single-Position Access Control" on page 258
  - "About Team (Multiple-Position) Access Control" on page 258
  - "About Manager Access Control" on page 259
- **Organization access control.** This includes single-organization, multiple-organization, and suborganization access control. For details, see:
  - "About Organization Access Control" on page 260
  - "About Single- and Multiple-Organization Access Control" on page 261
  - "About Suborganization Access Control" on page 263
- **All access control.** For details, see "About All Access Control" on page 264.
- **Access-group access control.** For details, see "About Access-Group Access Control" on page 265.

About Personal Access Control

If individual data can be associated with a user's Person record in the database, then you can restrict access to that data to that person only.

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 Change Requests, and My Service Requests.

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 access control. For example, the My Opportunities view applies position access control.

For information about business component view modes, see "Business Component View Modes" on page 279.

For information about implementing access control in a view, see "Listing View Access Control Properties" on page 283.

About Position 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 access control to the data by one or more of the following means:

- **Single-position access control.** You can associate a single position to individual data records. For details, see "About Single-Position Access Control" on page 258.
- **Team access control.** You can associate multiple positions, in the form of a team, to individual data. For details, see "About Team (Multiple-Position) Access Control" on page 258.
- **Manager access control.** You can grant access concurrently to data associated with a position and data associated with subordinate positions in a reporting hierarchy. For details, see "About Manager Access Control" on page 259.

An employee or partner user can be associated with one or more positions, of which only one can be the active position at a given time. All types of position access control for an employee or partner user are 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, from the User Preferences screen.
- A partner user must designate another position as the primary position, and then log in again.
- You can configure an agent who uses Siebel CTI to automatically change positions based on the data provided for an incoming call.

For information about Siebel CTI and related modules, and about setting up agents, see *Siebel Communications Server Administration Guide*.

About Single-Position Access Control

You can associate a single position to individual data. For example, in the My Quotes view, an employee logged in using a particular position can see only the quotes associated with that position. Some other views that apply single-position access control are My Forecasts and My Quotes.

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, or 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 279.

For information about implementing access control in a view, see "Listing View Access Control Properties" on page 283.

About Team (Multiple-Position) 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 can 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 team access control follow, with the display names for the field representing the team:

- The My Opportunities view has a Sales Team field.
- The My Accounts view has an Account Team field.
- The My Contacts view has a Contact Team field.
- The My Projects view has an Access List field.

Although the field for the team can contain multiple positions, only one name is displayed without drilling down. In a view that uses team access control, for example My Projects, the name of the active login is displayed. Other views, such as those using organization access control, can also have a field for the 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 team access control. However, *My* does not always imply team access control. Some *My* views apply personal, organization, or single-position access control. For example, the My Activities view applies personal access control.

A business component's view modes determine whether team access control can be applied in a view that is based on the business component. To have 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 team's members is designated as the primary member. The primary member is a factor in manager access control, but not in team access control.

If a business component is configured for team access control, any new record added for that type of component follows this rule: the user who created the record is added to the record's team and is set to be the primary.

For information about business component view modes, see "Business Component View Modes" on page 279.

For information about implementing access control in a view, see "Listing View Access Control Properties" on page 283.

About 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.

Manager-subordinate relationships are determined from a position hierarchy. One position hierarchy is included as seed data when you install Siebel Business Applications.

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 can be in the same division or a different division. For example, a sales manager in the Sales division might report to a sales vice president in the Corporate division.

In a view using manager access control, this employee or partner user has access to data according to the following behavior:

- 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 team access control, then the user sees data for which the user's active position is on the team or any subordinate position that is the primary member on the team. This is the standard behavior, known as primary manager visibility.

- A business component using team access control can be configured to allow the user to see data for all subordinate positions, regardless of whether they are the primary position for a record. This is known as nonprimary manager visibility.

  To configure nonprimary manager visibility, define a user property called Manager List Mode for the business component, and set it to Team (rather than the default value of Primary). For more information about the Manager List Mode user property, see *Siebel Developer's Reference*.

  NOTE: Configuring nonprimary manager visibility to support mobile users requires changes to docking visibility rules. Customers who require this functionality must engage Oracle's Application Expert Services. Contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance from Oracle's Application Expert Services.

- If the business component on which the view is based uses personal access control, the behavior is similar to that for position access control:

  - For single-owner access control, the user sees data associated directly with the user's active position or with subordinate positions.

  - For multiple-owner access control, the user sees data for which the user's active position is on the team, or any subordinate position that is the primary member of the team.

Views that apply manager access control generally contain the phrase *My Team's* in the title, such as My Team's Accounts. (In some cases, the word *My* is omitted.)

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 or Person. In a view using manager access control, if the manager user has no subordinate positions defined, the user cannot create new records in the view. The New button and the New Record command are unavailable.

For information about business component view modes, see "Business Component View Modes" on page 279. For information about implementing access control in a view, see "Listing View Access Control Properties" on page 283.

About Organization Access Control

When individual data can be associated with an organization, you can apply organization access control to the data by one or more of the following means:

- **Single-organization access control.** You can associate a single organization with individual data. For details, see "About Single- and Multiple-Organization Access Control" on page 261.

- **Multiple-organization access control.** You can associate multiple organizations with individual data. For details, see "About Single- and Multiple-Organization Access Control" on page 261.

- **Suborganization access control.** You can grant access concurrently to data associated with an organization and data associated with subordinate organizations in the organizational hierarchy. For details, see "About Suborganization Access Control" on page 263.

NOTE: Siebel 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 "About Position Access Control" on page 257.

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 Chapter 6, "Security Adapter Authentication," and "Seed Data" on page 353.

About Single- 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 suborganization access control, but not in multiple-organization access control.

Table 27 on page 262 lists data on which you can apply organization access control and indicates, for some of the most commonly used Siebel objects, whether a single organization, or multiple organizations, can be associated with the data.

Table 27. Data Enabled for Organization Access Control

Object Type	Object	Relationship
Customer data	Account	Multiple
	Competitor	Multiple
	Contact	Multiple
	Forecast Series	Multiple
	Household	Multiple
	Marketing Event/Activity	Multiple
	Opportunity	Multiple
	Order	Multiple
	Partner	Multiple
	Product Defect	Multiple
	Project	Multiple
	Quote	Multiple
	Service Request	Multiple
	User List	Multiple
Referential data (includes master data)	SmartScript	Multiple
	Literature	Multiple
	Price List	Multiple
	Cost List/Rate List	Multiple
	Period	Single
	Product	Multiple
	Catalog	Not applicable (catalogs use access-group access control)
Administrative data	Employee	Multiple
	Division	Single
	List of Values Type	Multiple
	List of Values	Single
	Position	Single
	Responsibility	Multiple

NOTE: Customizable products that you create with Siebel Configurator include some exceptions to organizational access rules. For information about customizable product visibility, see *Siebel Product Administration Guide*.

All (but not *All across*) is frequently in the title 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 "About All Access Control" on page 264. For information about business component view modes, see "Business Component View Modes" on page 279. For information about implementing access control in a view, see "Listing View Access Control Properties" on page 283.

About Suborganization Access Control

Suborganization access control, based on hierarchical organizations, is analogous to manager access control, which is 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 rollup 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 rollups of the continental sales organizations and the regional sales organizations.

Subordinate relationships are determined from the organizational hierarchy, as an administrator can view by navigating to the Administration - Group screen, and then the Organizations view.

The organizational hierarchy is included as seed data when you install Siebel Business Applications. 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 suborganization 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 descendant 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 descendant organization is the primary organization.

The titles of default views applying suborganization 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 suborganization access control. Suborganization 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 279. For information about implementing access control in a view, see "Listing View Access Control Properties" on page 283.

About 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 can be a person, a position, a valid primary position on a team, 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 does not have to be associated with the data.

All access control 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-organization 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 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 279. For information about implementing access control in a view, and for information about Admin mode, see "Listing View Access Control Properties" on page 283.

About Access-Group Access Control

Access groups are used to control access to master data by diverse groups of party types. An access group is a collection of any combination of positions, organizations, account, households, 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.

NOTE: Although you can add divisions to access groups, doing so has no effect on visibility. Use organizations instead.

A user is associated with an access group if, during the current session, the user is associated with a position, organization, account, household, 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, decision issues, events, training courses, 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 decision issue items. For an illustration of an access group hierarchy (master data), see "Access Control for Data" on page 254.

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 items 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 access control type is typically used in product picklists and other lists of products, such as a recommended product list.

For more information about data and data categorization, see "Access Control for Data" on page 254. For more information about parties, see "Access Control for Parties" on page 251.

Planning for Access Control

Two main strategies are available for controlling access to data in Siebel Business Applications:

- **Multiple-organization access control.** This strategy limits data access to only those organizations that 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 more information, see "About Organization Access Control" on page 260, the topics following this one, and "About Implementing Access Control" on page 272.

- **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. This strategy can be applied to master data only.

  For more information, see "About Access-Group Access Control" on page 265 and "Implementing Access-Group Access Control" on page 289.

NOTE: Configuring changes in access control for Siebel Business Applications can be a very complex task. Such changes can have significant implications for the entire application and can involve significant risks. For these reasons, it is recommended that you contact Oracle's Professional Services for a design review prior to undertaking any major modifications to access control in Siebel Business Applications. Contact your Oracle sales representative to request assistance from Oracle's Professional Services.

Access Control and 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. You also define the types of data and objects that people have to access and work with to perform their job functions. How you define the structure of your business environment directly impacts how access control applies to your users.

This topic provides some background information about business environment structure. If your enterprise is large and complex, you can accurately reflect its structure as you set up your Siebel Business Applications. 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 elements shown in Table 28 on page 267.

Table 28. Elements of Business Environment Structure

Element	Parent-Child	Description
Divisions	Yes	Subunits of your company's (or partner company's) organizations. Used to set default currencies. Can be used in Actuate reports. Not used to control visibility of data.
Organizations	Yes	The major parts or entities that make up your company (or your partner companies). Used to control visibility of data. See "About Organization Access Control" on page 260.
Positions	Yes	Control the data set (records) to which a user has access. See "About Position Access Control" on page 257.
Responsibilities	No	Control the views to which a user has access.
Employees	No	Individual users in your company and in partner companies who have access to your company's data.

You can set up divisions, organizations, 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 from the responsibility record, or you can associate the responsibility with the employee from the employee record.

Because organizations are based on divisions, it might be best to create your hierarchy of divisions first, and then to determine which of these divisions will be designated as organizations.

NOTE: Changing your company structure—such as positions and divisions—can cause Siebel Remote components (Transaction Router) to reevaluate access control for all objects related to the objects that have changed. This can result in diminished performance. For more information, see *Siebel Remote and Replication Manager Administration Guide.*

Benefits of Multiple 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 assign skills to organizations, which allows Assignment Manager to make assignments based on organization.

- It allows you to set up multitenancy for call centers. For more information, see *Siebel Communications Server Administration Guide*.

Deciding Whether to Set Up Multiple Organizations

If Siebel Business Applications is already deployed, and you do not have to change your users' visibility (access), your company might not require 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 might want to use organizations to support specific versions of a limited number of data entities such as products and price lists.
- **Complex global enterprise.** If you have a full-scale global enterprise that encompasses multiple internal and external businesses, each of which is made up of multiple business units, your company will benefit from implementing organizations. In this circumstance, some data must be available only to some business 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 can make fewer views available to these external organizations than to your internal organizations. You can 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 Siebel Assignment Manager or Siebel Workflow rules apply to different parts of your company, then your company will benefit from implementing organizations. For example, a company might want some Assignment Manager rules to apply to a telesales organization and other rules to apply to customers of its Web site.
- **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 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*.

Planning for Divisions

This topic and those that follow explain the common tasks for defining a company structure in Siebel Business Applications. These include tasks for defining divisions, organizations, responsibilities, and positions.

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.

To implement Siebel Business Applications, you must set up at least one division.

An organization can contain multiple divisions, but a given division can only be part of one organization. Organizations can be arranged into a hierarchy of parent organizations and suborganizations. 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. Divisions can also be used by Actuate reports. For more information on reports, see *Siebel Reports Administration Guide*.

NOTE: You cannot delete or merge division records, because business components throughout Siebel Business Applications refer to organization records. Deleting or merging 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.

Planning for 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).

The organization associated with the employee’s active position determines visibility for the employee. Conversely, the organizations that are associated to the employee, such as using the Employee Organization field in the Employee business component, determine visibility to the employee record for this employee.

Setting up organizations is an optional step in your implementation. If you are upgrading from a previous version of Siebel Business Applications, 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 want to divide your company into multiple structural units, you can create multiple organizations.

You might 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 *Configuring Siebel Business Applications*.

The following are best practices for working with organizations:

- Merging organizations is not recommended. Because many business objects are configured for multiple-organization access control, you might disrupt these relationships to a significant extent and get unexpected results.

- It is recommended that you do not change the name of the default organization, which is Default Organization. This record is seed data that is referenced in many places. If your company decides to change the default organization name, the name must be unique from any other organization or division name. References to Default Organization in other locations must also be changed.

  For example, if you are using Siebel Assignment Manager, you might have to rename references in assignment objects to the new name for the default organization. For more information, see *Siebel Assignment Manager Administration Guide* and *Configuring Siebel Business Applications*.

NOTE: You cannot delete organization records. Business components throughout Siebel Business Applications 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.

Planning for 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.

An employee must have a position in order to create and use accounts, opportunities, contacts, and other customer data objects in Siebel Business Applications. Each position typically has only one associated employee. In some circumstances such as job-sharing situations, a position might 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 might 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, which allows for manager access control. The parent position gains visibility to all the sets of data visible to the individual child positions. (Usually, the data will be displayed only where the child position is the primary on the team or record.)

Siebel Business Applications allow users to change their position to another position to which they have already been given access by the administrator. A user can change positions while logged in by navigating to the Tools menu, choosing the User Preferences menu item, and then selecting the Change Position tab. The user can select a different position in the list, and then click the Change Position button. 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.

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, Assignment Manager might not be able to assign resources to activities for that account.

If you rename a position, check the following to make sure the name change is reflected correctly:

- Assignment rules, if you have used these positions in assignment rules. For more information, see *Siebel Assignment Manager Administration Guide*.
- Workflow processes, if you have used these positions in workflow processes. For more information, see *Siebel Business Process Framework: Workflow Guide*.
- 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*.
- The Position field of the Employees view.

NOTE: 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 reextraction is not required. This is because in the database table where position names are stored, this column has enterprise-wide visibility. In other words, changes to this column are distributed to all users. See also "Position Data Model" on page 319.

Planning for 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 Siebel Business Applications' information and functions. You must assign responsibilities to all users. Without a responsibility, a user cannot use Siebel Business Applications, because that user cannot access any views.

You can also assign tab layouts and tasks to responsibilities. For more information, see "Managing Tab Layouts Through Responsibilities" on page 298 and "Managing Tasks Through Responsibilities" on page 302.

It is recommended that you use the responsibilities that are provided as seed data, where applicable. Then define any additional responsibilities you require that correspond to the major job functions in your organization.

For example, you might use or 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.

As appropriate, you can specify that a view will be read-only for a given responsibility.

To define a responsibility, you must specify which views are available to that responsibility. You can use the seed responsibilities that come with Siebel Business Applications. These can be copied and then customized.

NOTE: You cannot modify or delete the seed responsibilities. For instance, you cannot change the Siebel administrator responsibility. You can copy the seed responsibilities and modify the copies.

When you are defining responsibilities, consider the following issues:

- Grant access to the System Preferences view to only a selected group of administrators. Do not give end users access to the System Preferences view. System preferences control many things throughout the system, including some server logic and processing for Siebel Remote and Siebel Assignment Manager.
- Do not add Administration views to responsibilities associated with end users. Likewise, limit access to the Master Forecasts, Mobile Web Clients, Responsibilities, Views, and Territories views. The work performed with these views has far-reaching implications for the entire application.
- Where users require access to data presented in a view, but must not be able to create or modify data, specify that the view is read-only for this responsibility. (If any one responsibility for a user is associated with a view that is *not* marked with the Read Only View flag, the view will not be read-only for this user, regardless of how the flag is set for any other responsibility.)
- You might want to hide access to license keys by deleting the license key-related views from a user's responsibility. For more information about license keys, see *Siebel Applications Administration Guide*.
- 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 picklist.
- If you log into the application through the normal Siebel Web Client, you can add new views to responsibilities by navigating to the Administration - Application screen, and then the Responsibilities view.

About Implementing 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 topic specifies where to find these settings within Siebel Tools, but in most cases it 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 *Configuring Siebel Business Applications* and *Using Siebel Tools*.

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 representative.

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 might have personal or position 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.

Applications and 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 Business Applications.

To see which views an application includes

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, and then the Views view.

   The views defined for an application are listed.

For information about configuring screens and views, see *Configuring Siebel Business Applications*.

Setting Up Divisions, Organizations, Positions, and Responsibilities

This topic describes how to set up divisions, organizations, positions, and responsibilities.

Setting Up Divisions

This topic describes how to set up divisions.

To set up a division

1. Navigate to the Administration - Group screen, and then the Internal Divisions view.
2. In the Divisions form, add a new record and complete the necessary fields.

   Some fields are described in the following table.

Field	Guideline
Parent Division	If this division is a subdivision, select the parent division. This allows a division to be associated with another division.
Organization Type	Indicates the type of organization, which controls where in the application a division will appear for selection purposes. For example, divisions with Organization Type = Service appear for selection in the Group field on the Service screen, Service Requests view.
Organization Flag	When selected, indicates that the division is also an organization. The system copies that division into the Organization view.

Setting Up Organizations

This topic describes how to set up organizations.

To set up an organization

1. Navigate to the Administration - Group screen, and then the Organizations view.

2 In the Organizations form, add a new record and complete the necessary fields.

Some fields are described in the following table.

Field	Guideline
Parent Organization	If this organization is a suborganization, select the parent organization. This allows an organization to be associated with another organization.
Partner Flag	Used for Siebel PRM. This is a read-only check box. When the box is checked, this indicates that the organization represents an external enterprise that is a partner of your company. Partners are registered and promoted to organizations using the Approved Partners view in the Administration - Partner screen, as described in *Developing and Deploying Siebel Business Applications*.

Setting Up Positions

This topic describes how to set up positions.

To set up a position

1 Navigate to the Administration - Group screen, and then the Positions view.

2 In the Positions form, add a new record and complete the necessary fields.

Some fields are described in the following table. Most fields in the 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	Guideline
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.
Position Type	Type of position. This field is informational and has no impact on visibility.
Territory	This field is a read-only multi-value group. You cannot enter a value manually. For use by Siebel Assignment Manager.

Setting Up Responsibilities and Adding Views and Users

This topic describes how to set up responsibilities and add views and users.

To define a responsibility and add views and users

1. Navigate to the Administration - Application screen, and then the Responsibilities view.

   By default, the Responsibilities view shows all responsibilities, regardless of organization. However, you might want to configure new views in Siebel Tools that restrict the visibility to responsibilities. For more information on configuring views, see *Configuring Siebel Business Applications*.

2. In the Responsibilities 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. When you add a view, set the flag Read Only View if it must be read-only for users with this responsibility.

   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.

   You can also delete employees from the Users list.

Responsibilities and Access Control

A responsibility corresponds to 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 link bar, or in any other picklist. 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 Administration - Application screen. The administrator sees this screen listed in the Site Map and can navigate to the views it includes. A customer care agent typically does not have administrative views in a responsibility, so the agent would not see this screen or its views listed in any context.

Each user's primary responsibility also controls the default screen or view tab layout for the user. For more information, see "Managing Tab Layouts Through Responsibilities" on page 298.

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 Representative responsibility.

NOTE: Modifying visibility or responsibility settings for an application can in some cases require that the associated Siebel Application Object Manager (AOM) be restarted in order for these new settings to take effect for users of the Siebel Web Client. If you have only modified responsibilities, then you can clear cached responsibilities instead, without restarting the AOM. For more information, see "Clearing Cached Responsibilities" on page 310.

Associating a Responsibility with Organizations

You can associate a responsibility with one or more organizations. Responsibilities must be associated with organizations only when you are implementing delegated administration of users, such as for Siebel Partner Portal (for Siebel PRM).

A partner user can see responsibilities that are associated with the organization with which the user is associated for the session. A partner user is associated with the organization with which his or her primary position is associated.

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 must 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.

Associate each responsibility with at least one organization if you include views that use either position or organization access control in the responsibility.

Local Access for Views and Responsibilities

Each view and each responsibility has a Local Access flag. Together, these settings determine whether views can be accessed by Siebel Mobile Web Client users with particular responsibilities.

The setting of the Local Access flag does not affect access to a view for users using either the Siebel Web Client or Siebel Developer Web Client.

When Local Access is set to TRUE (checked), all users with the view in one of their responsibilities can access the view when using the Siebel Mobile Web Client (connected to the local database). When Local Access is set to FALSE (unchecked), users cannot access the view when using the Mobile Web Client.

The Local Access flag appears in the following locations:

- **Default Local Access flag.** Navigating to the Administration - Application screen, and then the Views view. The Default Local Access setting defines a default setting to be inherited for the view, unless the setting is overridden in another context.

- **Local Access flag.** Navigate to the Administration - Application screen, Responsibilities, and then the Views list. The Local Access setting displays or overrides the default setting applicable to a view record that is a child to the current responsibility. The setting affects a view only as it is made available to users through association with a specific responsibility record.
- **Local Access flag.** Navigate to the Administration - Application screen, Views, and then the Responsibilities list. The Local Access flag displays or overrides the default setting applicable to the view record that is the parent to the current responsibility. The setting affects a view only as it is made available through association with a specific responsibility record.

The Local Access field is a mechanism for controlling which views mobile users can work in, when using the Siebel Mobile Web Client. In addition to enabling or disabling local access to views based on responsibility, administrators can provide different sets of views for access by different mobile users. For more information, see *Siebel Remote and Replication Manager Administration Guide*.

CAUTION: 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 All access control, see "About All Access Control" on page 264.

Read Only View for Responsibilities

Each responsibility has a Read Only View flag. Set this flag to True to prevent a user from creating data in a view or modifying existing data in a view. To make sure that a user cannot create or modify data in a view, you must select this flag for all responsibilities associated with the user that access the view.

The Read Only View flag appears in the following locations:

- Navigate to the Administration - Application screen, Responsibilities, and then the Views list.
- Navigate to the Administration - Application screen, Views, and then the Responsibilities list.

Assigning a Responsibility to a Person

You can add a responsibility to a Person, User, Employee, or Partner record. The following procedure describes how to add a responsibility to a Person record. You can assign a responsibility in the Users list or Employees list in the Administration - User 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 into a Siebel employee application as an administrator.
2. Navigate to the Administration - User screen, then the Persons view.
3. Select a Person record.
4. In the form, click the select button on the Responsibility field.

   A list of the responsibilities assigned to this Person appears.

5. In the Responsibilities list, click New.

   A list of responsibilities available for assigning appears.

6. Select one or more responsibilities, and then click OK.

   The selected responsibilities appear in the list of responsibilities for this Person.

7. Click OK.

8. Save the record.

If you want to assign the same responsibility to multiple users, you can alternatively add the users to the responsibility through the Administration - Application 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 might connect the data to the person by comparing the data's Owner Id field to the person's user ID. Another business component might 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 + (the plus sign) to expand the Business Component object type.

   The Business Component subtree appears.

3. Click the BusComp View Mode icon.

   The Business Components list and its BusComp View Modes detail list appear.

4. In the Business Components list, select a business component for which there are records in the BusComp View Modes list.

   A record in the BusComp View Modes list represents one view mode the business component can assume.

Business Component View Mode Fields

The following fields in the BusComp View Modes list in Siebel Tools determine allowable visibility for a business component.

- **Owner Type.** This field specifies 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 the user is associated with the record, 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 multivalue 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 multivalue 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 multivalue links are 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 multivalue 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 the Link object type listing in Siebel Tools, 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. Both view modes are required because the creator and the customer care agent both require access to the data based on a person.

For information about working with business components, see *Configuring Siebel Business Applications*.

Viewing an Applet’s Access Control Properties

A view presents a collection of lists, forms, and trees at once. These lists and forms are referred to as applets in a configuration context.

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 applets and their properties. For more information, see *Configuring Siebel Business Applications*.

To view an applet’s properties

1. Launch Siebel Tools.
2. In the Object Explorer, click + to expand the Applet object type.

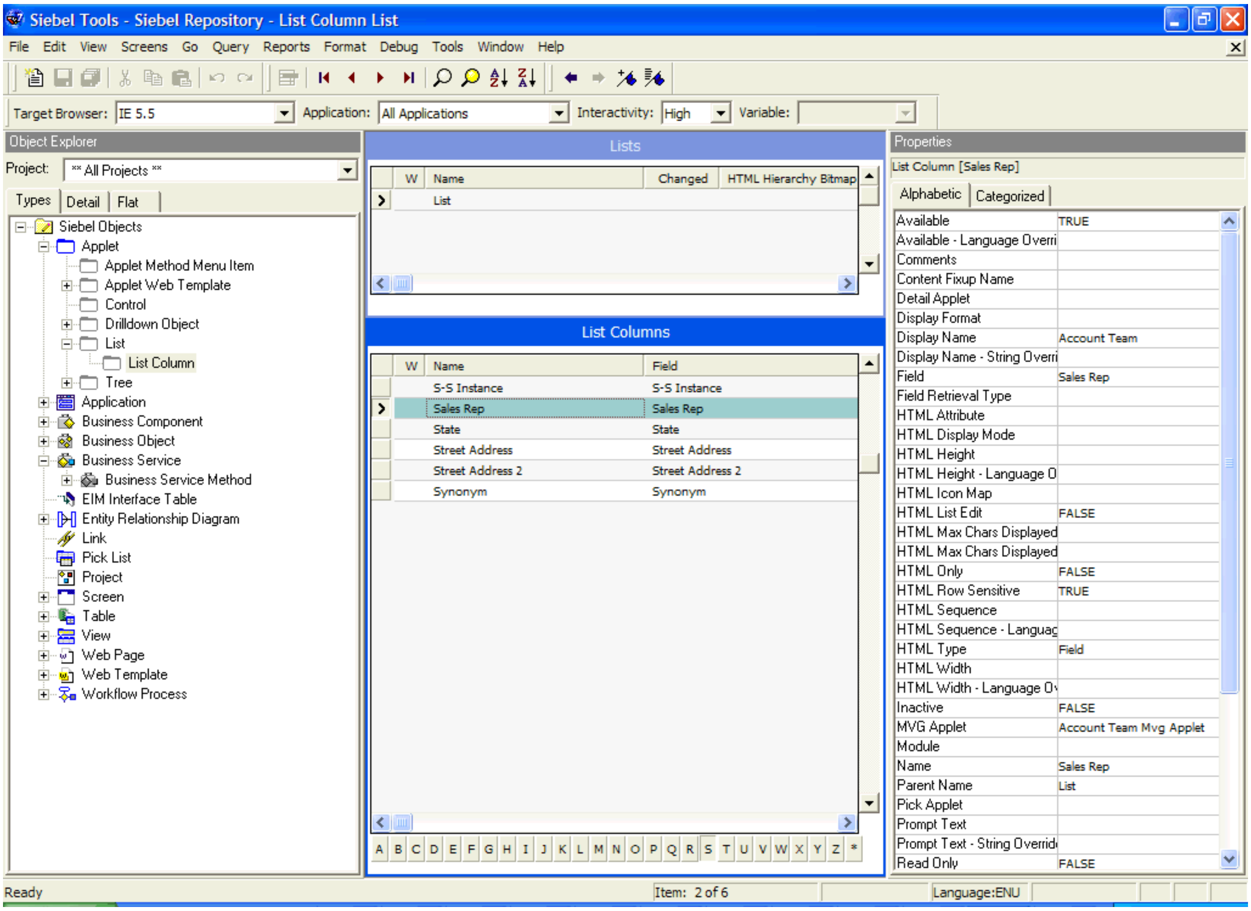
   The Applet subtree and the Applets list appear.
3. To see a particular applet property, click the icon for its subcomponent or click + to expand the subtree for a subcomponent, and then click its subcomponent.

   A detail list for the subcomponent appears below the Applets list. Two applet properties in particular contribute to data visibility: Business Component and Display Name.

4 In the Object Explorer, choose Applets, List, and then List Columns.

As shown in Figure 8 on page 283, the List Columns list shows the business component fields that this applet will display. For each business component field, the Display Name entry in the accompanying Properties list 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.



Target Browser: IE 5.5 Application: All Applications Interactivity: High Variable:

Project: ** All Projects **

Lists

W	Name	Changed	HTML Hierarchy Bitmap
	List		

List Columns

W	Name	Field
	S-S Instance	S-S Instance
	Sales Rep	Sales Rep
	State	State
	Street Address	Street Address
	Street Address 2	Street Address 2
	Synonym	Synonym

List Column [Sales Rep]

Available	TRUE
Available - Language Overri	
Comments	
Content Fixup Name	
Detail Applet	
Display Format	
Display Name	Account Team
Display Name - String Overri	
Field	Sales Rep
Field Retrieval Type	
HTML Attribute	
HTML Display Mode	
HTML Height	
HTML Height - Language O	
HTML Icon Map	
HTML List Edit	FALSE
HTML Max Chars Displayed	
HTML Max Chars Displayed	
HTML Only	FALSE
HTML Row Sensitive	TRUE
HTML Sequence	
HTML Sequence - Languag	
HTML Type	Field
HTML Width	
HTML Width - Language O	
Inactive	FALSE
MVG Applet	Account Team Mvg Applet
Module	
Name	Sales Rep
Parent Name	List
Pick Applet	
Prompt Text	
Prompt Text - String Overrid	
Read Only	FALSE

Figure 8. Lists and List Columns for an Applet

Listing 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 list a view's access control properties

1. Launch Siebel Tools.
2. In the Object Explorer, click the Views object type.

   The Views list appears.

The following fields in the Views list help determine data visibility.

- **Title.** The title is the name given to a view in the user interface. Specify a title that suggests 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.

  When the view property Visibility Applet is defined on a view, this view is considered to be associated with its own, independent visibility. The Siebel application re-queries this view when you choose it, according to the Visibility Applet Type (the default Visibility Applet Type is All).

  NOTE: Do not specify the Visibility Applet property on detail views, where the current record context and the current query must be retained.

  - 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 link bar 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 picklist for this field:
  - **All.** A view of this type applies *All* access control.

    The user can access all records, except for those with a missing or invalid owner.
  - **Personal.** A view of this type 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.

    The Personal view mode of the Quote business component is specialized to display quotes created by the user and assigned to somebody else.

- **Sales Rep.** A view of this type applies single-position or team access control.

  The user can access records owned by the user's position or records whose 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.** A view of this type 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 team access control, then the user sees data for which the user's active position is the primary position on the team, or for which a subordinate position is the primary member on the team.

  To use this visibility applet type, the business component can also have a view mode with owner type Position.

- **Organization.** A view of this type 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.** A view of this type applies suborganization 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 descendant 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 descendant organization is the primary organization.

  Descendant 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.** A view of this type 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, household, 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, household, 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 picklists 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.

  Despite setting the visibility type to Catalog, you might be able to see extra products in product picklists and other lists of products. This is expected behavior for products that belong to public catalogs.

- **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 insert, delete, merge, and update restrictions for the business component used by applets of the view are ignored (including those restrictions specified by the following business component user properties: No Insert, No Delete, No Merge, No Update).

  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 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.)

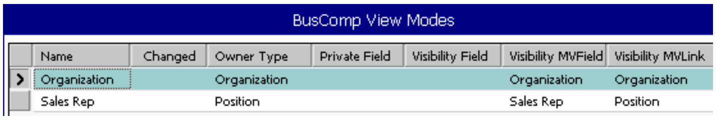
CAUTION: Views using Admin mode are intended for access by administrators and are typically included in a grouping of like views in an administration screen, such as Administration - Application. Do not include views in Admin mode in a screen with views not set for Admin mode. When a user transitions 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.

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 (SRF).

For more information about required practices when using Siebel Tools, see *Configuring Siebel Business Applications*.

Figure 9 on page 287 shows the BusComp View Modes list in Siebel Tools, for the Account business component. As indicated by the Owner Type field, organization and position view modes are allowed. As indicated in Visibility MVField, accounts can be associated with multiple organizations and multiple positions (for example, sales teams).

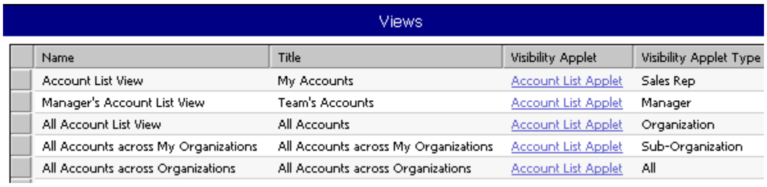


BusComp View Modes

Name	Changed	Owner Type	Private Field	Visibility Field	Visibility MVField	Visibility MVLink
Organization		Organization			Organization	Organization
Sales Rep		Position			Sales Rep	Position

Figure 9. Account Business Component View Modes

Figure 10 on page 287 shows five views in the Views list in Siebel Tools. The Title field shows the display name for the view. All five views have Account List Applet as their visibility applet. Account List Applet is based on the Account business component.



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 10. Example Views Based on the Account Business Component

These five example views provide different lists of account data because they have different visibility applet types specified, as shown below in Table 29 on page 288.

Table 29. Example Account Views and Visibility Applet Types

View	Visibility Applet Type	Data Access
Account List View (displayed as My Accounts)	Sales Rep	Team access control applies. The visibility applet type is applied to a business component for which multiple positions can be associated. For this view, access is granted to account data where the user’s position is on the account team.
Manager’s Account List View (displayed as Team’s Accounts)	Manager	Manager access control applies. The visibility applet type is applied to a business component for which multiple positions can be associated. For this view, access is granted to account data where 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 access control applies. The visibility applet type is applied to a business component for which multiple organizations can be associated. For this view, access is granted to account data where a user’s primary organization is one of the organizations with which the account is associated.
All Accounts across My Organizations	Sub-Organization	Suborganization access control applies. The visibility applet type is applied to a business component for which multiple organizations can be associated. For this view, access is granted to account data where the user’s active organization or a descendant organization is the primary organization.
All Accounts across Organizations	All	All access control applies. The Account business component has only position and organization view modes. For this view, access is granted to all account data for which there is a primary position on the account team or an organization associated with the account.

Implementing 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 descendant groups (child, grandchild, and so on) are automatically associated with the category. Conversely, if an access group is disassociated with a category, then its descendant 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 button provides that the access group is automatically associated with that category’s descendant categories (child, grandchild, and so on). Therefore, users associated with the access group have access to the data in those descendant categories.
  - If the access group is disassociated with the category, then the access group is automatically disassociated with that category’s descendant categories. If the access group is disassociated with one of the descendant categories, then the access group’s cascading visibility is granted only down to, but not including, that descendant category.
  - Once the Cascade button 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 button is not used, access is limited to the individual category to which the access group is associated.

Scenario For Implementing Access-Group Access Control

This topic gives one example of how access-group access control might be used. You might use access-group access control differently, depending on your business model.

Assume that 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:

- Provide your base resellers access to basic product information resources—service FAQs, product documentation, and product training classes.
- In addition to basic product information, provide your "premier" resellers access to more sales-specific resources—marketing FAQs, documents that provide guidance on customer decision issues, and sales training classes.
- In addition to product and sales resources, provide your alliance resellers access to resources to help design entire marketing campaigns—competitive briefs and training classes.
- As the status of a reseller changes, the administration required to change the reseller's access to data must be minimal.

Figure 11 on page 290 illustrates one access control structure that solves this business problem.

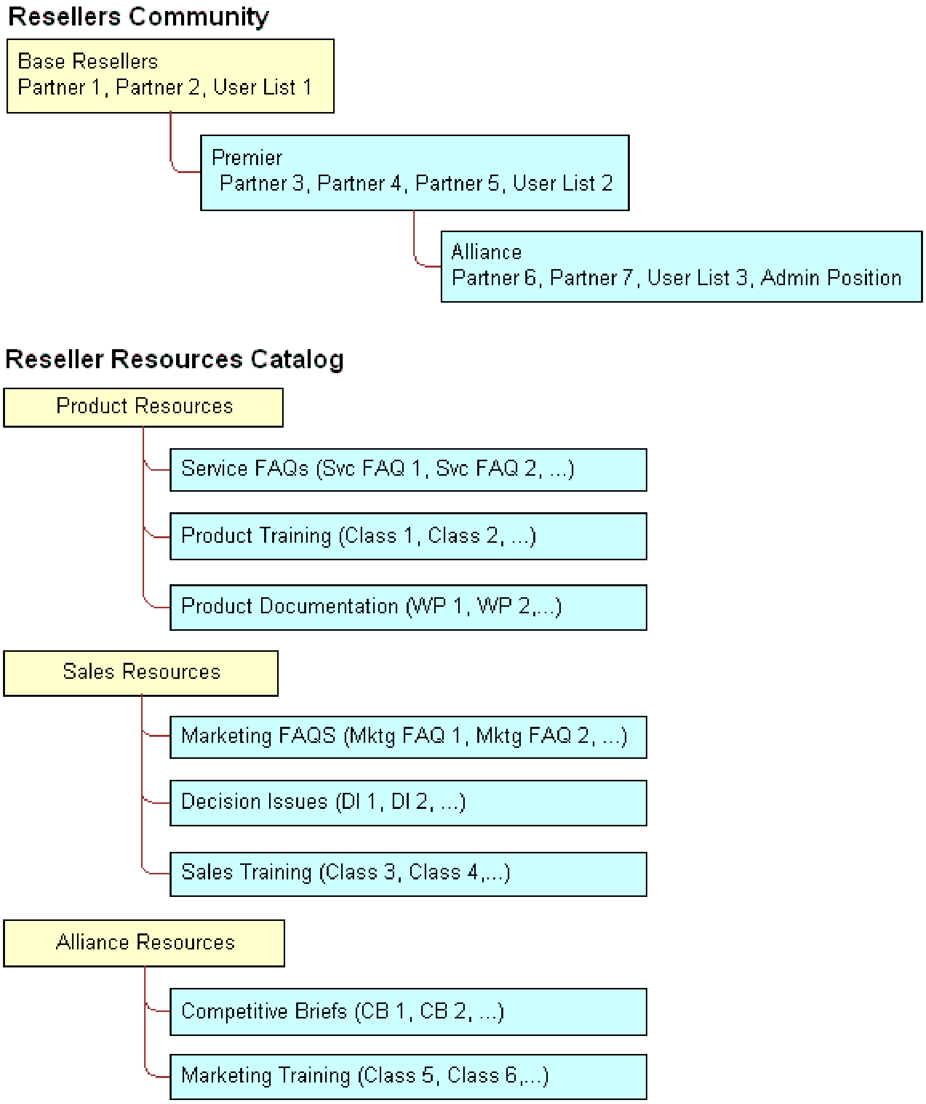

Resellers Community
Base Resellers
Partner 1, Partner 2, User List 1
Premier
Partner 3, Partner 4, Partner 5, User List 2
Alliance
Partner 6, Partner 7, User List 3, Admin Position
Reseller Resources Catalog
Product Resources
Service FAQs (Svc FAQ 1, Svc FAQ 2, ...)
Product Training (Class 1, Class 2, ...)
Product Documentation (WP 1, WP 2,...)
Sales Resources
Marketing FAQS (Mktg FAQ 1, Mktg FAQ 2, ...)
Decision Issues (DI 1, DI 2, ...)
Sales Training (Class 3, Class 4,...)
Alliance Resources
Competitive Briefs (CB 1, CB 2, ...)
Marketing Training (Class 5, Class 6,...)

Figure 11. Reseller Resources Access Control Example

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 Resellers 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 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 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 Reseller Resources access control structure

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 use the Cascade button.

   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 Resources category, and use the Cascade button.

   Access is inherited by the Alliance access group from the Premier group, and access cascades from the Sales 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 Resources category.

4. Associate the Alliance access group with the Sales Resources category, and use the Cascade button.

   No group inherits access from the Alliance group. Access cascades from the Alliance Resources category to its subcategories containing data. The resulting behavior is that only the Alliance group has access to the subcategories 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 Partner Portal, 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*.
- Creating and administering user lists and access groups, see "Implementing Access-Group Access Control" on page 289.

Viewing Categorized Data (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 Sales and Siebel Partner Portal, as 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 and Info Center Explorer screens.

The Info Center Explorer provides a tree interface for navigating all the catalogs to which the user has access, down to the data item level. Info Center, as compared to Info Center Explorer, shows how categorized data can be presented in Siebel Business Applications using a rich and more open user interface.

To view categorized data in Info Center

1. Navigate to Info Center.

   The Info Center screen appears, showing accessible catalogs and their first-level categories.

2. Click a category link. For example, you might choose Decision Issues.

   The category appears, showing its data items and its first-level subcategories.

3. Click a data item to view it, or drill down on a subcategory link to see its contents.

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 required.
- Administer the party types that are members of access groups—positions, organizations, households, and user lists.
- Administer access groups—build the access groups and modify their structures as required.
- Associate access groups with catalogs and categories of data.

About Administering Catalogs of Data

You can do the following catalog and category administration tasks in the Administration - Catalog 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 Partner Portal, as well as in Info Center.
- 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* and *Siebel Partner Relationship Management Administration Guide*.

Administering Positions, Organizations, Households, and User Lists

Access groups are made up of positions, organizations, households, and user lists.

About Administering Positions

You must do the following administrative tasks with positions:

- Create positions.
- Associate positions with employees and partner users.
- Maintain position hierarchies.

About 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.

About Administering Households

You must do the following administrative tasks with households:

- Create households.
- Associate contacts with households.
- Maintain household data.

For information about administering households, see *Siebel Applications Administration Guide*.

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 "Access Control for Parties" on page 251.

The following procedure describes how to create a user list.

To create a user list

1. Navigate to the Administration - Group screen, then the User Lists view.
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. Save the record.

The following procedure describes how to modify a user list by adding or deleting users.

To add users to a user list

1. Navigate to the Administration - Group screen, then the User Lists view.
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, Household, and User List into access groups for the purpose of controlling their individual members' access to data.

You administer access groups by navigating to the Administration - Group screen, then the Access Groups view. This view 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 descendants. Therefore, an access group can 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 "Access Control for Parties" on page 251 and "About Access-Group Access Control" on page 265.

Creating an Access Group

You can create an access group in the Administration - Group screen.

To create an access group

1. Navigate to the Administration - Group screen, then the Access Groups view.

   The Access Groups tree and the Access Groups list are displayed.
2. In the Access Groups list, add a new record.

   A new access group record.
3. Complete the following fields, then save the record. Use the guidelines below.

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. Navigate to the Administration - Group screen, then the Access Groups view.

   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, households, 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, save the record.

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. Navigate to the Administration - Group screen, then the Access Groups view.

   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. Click Save.
   - From the Parent Access Group field, 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 descendant 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 descendant access groups associated with the category are not displayed in the list of groups associated with the category.
- **Cascade button.** Clicking the Cascade button provides the given access group with visibility to all of the child categories of the current catalog or category. Clicking this button repeatedly has no effect. You must manually disassociate the group from the child categories to undo the access cascade.
- **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. Navigate to the Administration - Catalog screen, then the Access Groups view.
2. Select a catalog from the Catalogs list.
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, save the record.
6. Select an access group, and then click Add.

   The access group appears under the Access Group tab.

7. Complete the following fields, then save the record. Use the guidelines provided below.

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 descendant categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendant 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. Navigate to the Administration - Catalog screen, then the Access Groups view.
2. In the Catalogs list, drill down on a catalog name.

   The Categories list for the catalog appears.
3. Click the Access Groups view 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, save the record.
7. Select an access group, and then click Add.

   The access group appears under the Access Group tab.
8. Complete the following fields, and save the record. Use the guidelines provided below.

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 descendant categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendant 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 category's descendant categories.

Managing Tab Layouts Through Responsibilities

Siebel Business Applications administrators can manage default screen and view tab layouts that are specific to job functions. Tab layouts are managed through responsibilities.

Administrators can use the Responsibilities view (Responsibility Detail - Tab Layout View) in the Administration - Application screen to define a default tab layout for each responsibility. Administrators can administer both view access and default tab layout from this view.

To ease the administrative burden of setting up default tab layouts and associating them with responsibilities, Siebel Business Applications ship with many predefined responsibilities that are preconfigured with default tab layouts.

For example, the Universal Agent responsibility for Siebel Call Center has associated with it both screen and view access as well as a default tab layout. These are the views required most often for users holding that job function. Each time a user with this responsibility logs in, this user has access to all screens and views for that responsibility, and for all other responsibilities the user is associated with.

However, the user sees in the application user interface only the simplified default screen and view tab layout associated with the user's primary responsibility—for example, the layout associated with the Universal Agent responsibility, if this is the user's primary responsibility.

Each user can modify personal tab layout settings by using the Tab Layout view in the User Preferences screen (from the Tools menu, choose the User Preferences menu item). Once the user has modified the tab layout, these settings will always override the default tab layout associated with the user's primary responsibility. For more information, see *Siebel Fundamentals*.

If users select a screen from the Site Map that is not part of their tab layout, a screen tab is created for that screen which is only available for that session.

Specifying Tab Layouts For Responsibilities

The Tab Layout view is used for basic tab layout management tasks such as reordering or hiding screen and view tabs for different responsibilities, as well as for exporting and importing tab layouts. See "Exporting and Importing Tab Layouts" on page 300.

To let you manage screens and views for multiple applications, tab layout administration uses four lists:

- **Responsibilities list.** Includes all the responsibilities in the repository.
- **Applications list.** Includes all the Siebel Business Applications in the repository, and specifies for which application you are managing tab layouts.
- **Screen Tab Layout list.** Specifies which screens are displayed for each application.
- **View Tab Layout list.** Specifies which views are displayed for each screen.

You must select an application because you might be administering responsibilities for a different application than the one you are logged into as an administrator. For example, you use Siebel Partner Manager to administer responsibilities for partners who will use Siebel Partner Portal.

To specify the tab layout for a responsibility

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, then the Responsibilities view.

3. In the Responsibilities list, select the responsibility you want to associate tab layouts with.
4. Click the Tab Layout view tab.
5. In the Tab Layout list, select an application associated with the responsibility.
6. 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.
7. 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.

Assigning a Primary Responsibility

Each user can have multiple responsibilities assigned, in order to provide access to all necessary views. One responsibility is defined as the primary responsibility. The user sees the tab layout associated with his or her primary responsibility. The Site Map provides this user with access to the superset of screens and views defined in the responsibilities with which the user is associated.

To assign a primary responsibility to a user, perform the following procedure.

To assign a primary responsibility to a user

1. Navigate to Administration - User, and then the Users screen.
2. Select a User record.
3. In the form, click the select button on the Responsibility field.

   A list of the responsibilities assigned to the User appears.
4. In the Responsibilities dialog box, set the primary responsibility for the user by checking the Primary flag of one of the selected responsibilities.

NOTE: By default, the first responsibility assigned to a user (based on timestamp) becomes the primary responsibility. Particularly for customers who are upgrading, the administrator must verify that the correct primary responsibility is assigned to each user, or specify the desired primary responsibility.

Exporting and Importing Tab Layouts

You can export and import tab layouts, in order to copy a tab layout from one responsibility to another.

For example, if you have a tab layout associated with one responsibility and you want to apply it to another responsibility, you can first export the desired tab layout settings to an XML file, optionally modify the file, and then import it to the target responsibility.

Tab layouts associated with responsibilities are stored in the Siebel File System as attachments. These files are automatically routed to mobile users.

Exporting Tab Layouts

This topic provides the procedure for exporting tab layouts to an XML file.

To export tab layouts

1. Navigate to the Administration - Application screen, then the Responsibilities view.
2. In the Responsibilities list, click the Tab Layout view tab.
3. Select the responsibility that has the desired tab layout.
4. Select a record in the Applications list.

   You can select multiple applications and export the tab layouts for a responsibility for one or more associated applications. The XML file will contain screen tab and view tab settings for the selected applications. When you later import the XML file, tags in the file specify the applications that will be affected if tab layouts are subsequently imported from this file.

5. Click the menu button in the Responsibilities list and select Export Tab Layout.
6. Save the XML file.

   For example, to save tab layout settings for a responsibility designed for field engineers who use Siebel Field Service, you might export a file such as Siebel Field Service@Field Engineer.xml.

Importing Tab Layouts

This topic provides the procedure for importing tab layouts from an XML file you previously exported to.

To import tab layout to a target responsibility

1. Navigate to the Administration - Application screen, then the Responsibilities view.
2. Click the Tab Layout view tab and select the target responsibility in the Responsibilities list.
3. Click the menu button in the Responsibilities list and select Import Tab Layout.
4. In the import dialog box, choose the XML file for the Application Tab Layout you want to import.

5. Click Import.

   After you have imported the XML file, default tabs in the application correspond to those defined in the file you imported.

   NOTE: Importing a tab layout file hides and resequences views for affected users. Although you cannot roll back imported changes directly, you can still modify tab layout settings in the Responsibilities Administration view, or you can modify the XML file and reimport it.

Managing Tasks Through Responsibilities

A user with an administrator login can control access to tasks by associating tasks with user responsibilities. To access a task, a user must be assigned the responsibility that allows access to the task. A user who is assigned more than one responsibility can access any task that is associated with one of his or her responsibilities.

The administrator can also define hyperlinks to the tasks associated with a responsibility; these task links then appear on the home page of the users who are assigned the responsibility.

The following topics describe how to associate responsibilities and tasks:

- "Associating Responsibilities with a Task" on page 302
- "Creating Task Links for a Responsibility" on page 303

For more information about tasks, see *Siebel Business Process Framework: Task UI Guide*.

Associating Responsibilities with a Task

The following procedure describes how to associate responsibilities with a task to control access to the task. You carry out the following procedure through the Registered Tasks Administration view.

To associate responsibilities with a task

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, then the Tasks view.
3. In the Registered Tasks list, select the task that you want to associate with responsibilities.
4. In the Responsibilities list, click New.

   The Tasks dialog box appears.
5. Select a responsibility, then click OK.

   The responsibility appears in the Responsibilities list and is associated with the task you selected in Step 3.
6. If appropriate, select or clear the check boxes for Allow Delete and Allow Transfer.

- Allow Delete

  Select the Allow Delete check box if you want an employee with the associated responsibility to be able to delete the task.

- Allow Transfer

  Select the Allow Transfer check box if you want an employee with the associated responsibility to be able to transfer the task.

  For information about deleting or transferring tasks, see *Siebel Business Process Framework: Task UI Guide*.

7 Step off the record to save changes.

Creating Task Links for a Responsibility

After creating a responsibility, you can create links to the tasks commonly performed by employees who have that responsibility. These links are then displayed in the task list on the home page for these employees.

For each task link, you enter a caption, an image file, and a description. In addition, specify the view where the task is performed. When the user clicks on the hyperlink for this task on the home page, this view appears.

Personalization of this type is already specified for various seed responsibilities.

To create task links for a responsibility

1 Log in as an administrator.

2 Navigate to Administration - Application, and then the Responsibilities screen.

3 In the Responsibilities list, select the responsibility you want to associate with task links.

4 Click the Links tab.

5 In the Links list, do one of the following:

- Click Add to display the Add Links list, from which you can select an existing task link to add to the list of task links associated with the responsibility.
- Click New to add a new task link for this responsibility, and enter the following information:

Field	Guideline
Name	Enter the name of the task.
Caption	Enter a caption for the task; this is displayed as a hyperlink in the task list.
Description	Enter a description of the task; this is displayed under the caption in the task list.
Destination View	Click the select button and choose the view that appears when the user clicks the hyperlink for this task.

Field	Guideline
Sequence	Optionally, specify the order in which this task is displayed in the task list for this responsibility on the home page. If this field is left blank, tasks are displayed in the order that you list them.
Image	Select the graphic image that is displayed as a hyperlink to the left of this task in the task list.
Group	This field is used if search specifications are applied to filter the tasks that are displayed in the task applet, if multiple task applets are associated with the responsibility.

Administering Access Control for Business Services

Business services can be accessed by all users by default. However, the administrator can restrict access to specified business services and business service methods. The administrator can then associate responsibilities with the restricted business services or associate the business services with responsibilities. This allows the administrator to restrict access to business services based on the end user's responsibility. To access a restricted business service, an end user must be associated with the responsibility that allows access to the restricted business service. An end user who is assigned more than one responsibility can access any restricted business service that is associated with one of his or her responsibilities.

For business services that allow you to specify a view mode to access data, you can specify which view mode can be used by different responsibilities. The following list describes the view modes that can be associated with a responsibility to restrict the set of data records a user with the responsibility accesses. The list also indicates the relationship that exists between each view mode:

- Personal < Sales Rep << Manager < Organization << Sub-Organization < All
- Group < Catalog < All

In the preceding list, the level of visibility broadens as you read from left to right. For example, the Manager view mode grants access to more data than the Sales Rep view mode. The character < indicates a non-hierarchical relationship between view modes. For example, the relationship between Manager view mode and Organization view mode. The characters << indicate a hierarchical relationship between view modes. For example, the relationship between Sales Rep view mode and Manager view mode.

The capabilities described in the preceding paragraphs allow you to manage access to business services (and associated methods) by end users based on the responsibilities assigned to the end user. The following topics provide more detailed information on business services:

- "Associating a Business Service with a Responsibility" on page 305
- "Associating a Responsibility with a Business Service" on page 306
- "Example of Associating a Responsibility with Business Service Methods" on page 308
- "Clearing Cached Business Services" on page 309

- "Disabling Access Control for Business Services" on page 309

Associating a Business Service with a Responsibility

This topic describes how you can associate a business service with a responsibility to control access to the business service and its methods. You carry out the following procedure through the Responsibilities view.

To associate a business service with a responsibility

1. Log in as an administrator.

2. Navigate to the Administration - Application screen, Responsibilities, and then the Business Service view.

3. In the Responsibilities list, select the responsibility that you want to associate with a business service.

4. In the Business Service list, click New to select a business service to associate with the responsibility selected in Step 3.

   The Business Service dialog box displays the list of business services that are currently associated with the responsibility selected in Step 3.

5. In the Business Service dialog box, click New.

   A new record appears in the Business Service list view.

6. Click the Select button in the Name field.

   The Business Service dialog box appears.

7. Select a business service to associate with the responsibility selected in Step 3, and then click OK.

   The selected business service appears in the Business Service list view.

8. In the Business Service Method list, click New to specify the business service methods to which the responsibility selected in Step 3 gains access.

   The Business Service Method dialog box appears. This dialog box displays the list of Business Service methods to which access is currently controlled.

9. If the business service method to which you want to allow the responsibility access appears in the Business Service Method dialog box, select it, then click OK and go to Step 13. If not, go to Step 10.

   TIP: To allow you to restrict access to business service methods without associating them with a real responsibility, Siebel Business Applications have provided a responsibility `Default Bus Service Method Access Control User`. Use the steps described in this procedure to associate all business service methods to which you want to control access with `Default Bus Service Method Access Control User`. This makes sure that the Business Service Method dialog box is populated with the business service methods to which you want to control access.

10 In the Business Service Method dialog box, click New.

A new record appears in the Business Service Method list view.

11 Click the Select button in the Name field.

The Business Service Method dialog box appears.

12 Select a business service method to associate with the responsibility selected in Step 3, and then click OK.

The selected business service method appears in the Business Service Method list view.

By default, if you do not specify the business service methods to which the responsibility gains access, then the responsibility gains access to all business service methods of the business service provided that none of the business service methods have restricted access.

13 From the Broadest Visibility drop-down list, select the view mode to associate with the responsibility.

The business service selected in Step 7 must support view modes to allow you to select a value from the Broadest Visibility drop-down list.

14 Step off the record to save changes.

Associating a Responsibility with a Business Service

This topic describes how you can associate a responsibility with a business service to control access to the business service and its methods. You carry out the following procedure through the Business Service Access view.

To associate a responsibility with a business service

1 Navigate to the Administration - Application screen, then the Business Service Access view.

2 In the Business Service list, click New to select a business service.

A new record appears in the Business Service list.

3 Click the Select button in the Name field.

The Business Service dialog box appears.

4 Select the business service to which you want to control access, then click OK.

The selected business service appears in the Business Service list view.

5 In the Access By Responsibility list view, click New.

The Add Responsibilities dialog box appears.

6 Select a responsibility to associate with the business service that you selected in Step 4, and then click OK.

The selected responsibility appears in the Access By Responsibility list view.

7 In the Business Service Method list, click New to specify the business service methods to which the responsibility selected in Step 6 gains access.

The Business Service Method dialog box appears. This dialog box displays the list of business service methods to which access is currently controlled.

8 If the business service method to which you want to allow the responsibility access appears in the Business Service Method dialog box, select it, then click OK and go to Step 11. If not, go to Step 9.

TIP: To allow you to restrict access to business service methods without associating them with a real responsibility, Siebel Business Applications have provided a responsibility Default Bus Service Method Access Control User. Use the steps described in this procedure to associate all business service methods to which you want to control access with Default Bus Service Method Access Control User. This makes sure that the Business Service Method dialog box is populated with the business service methods to which you want to control access.

9 Click the Select button in the Name field.

The Business Service Method dialog box appears.

10 Select a business service method to associate with the responsibility selected in Step 3, and then click OK.

The selected business service method appears in the Business Service Method list view.

By default, if you do not specify the business service methods to which the responsibility gains access, then the responsibility gains access to all business service methods of the business service provided that none of the business service methods have restricted access.

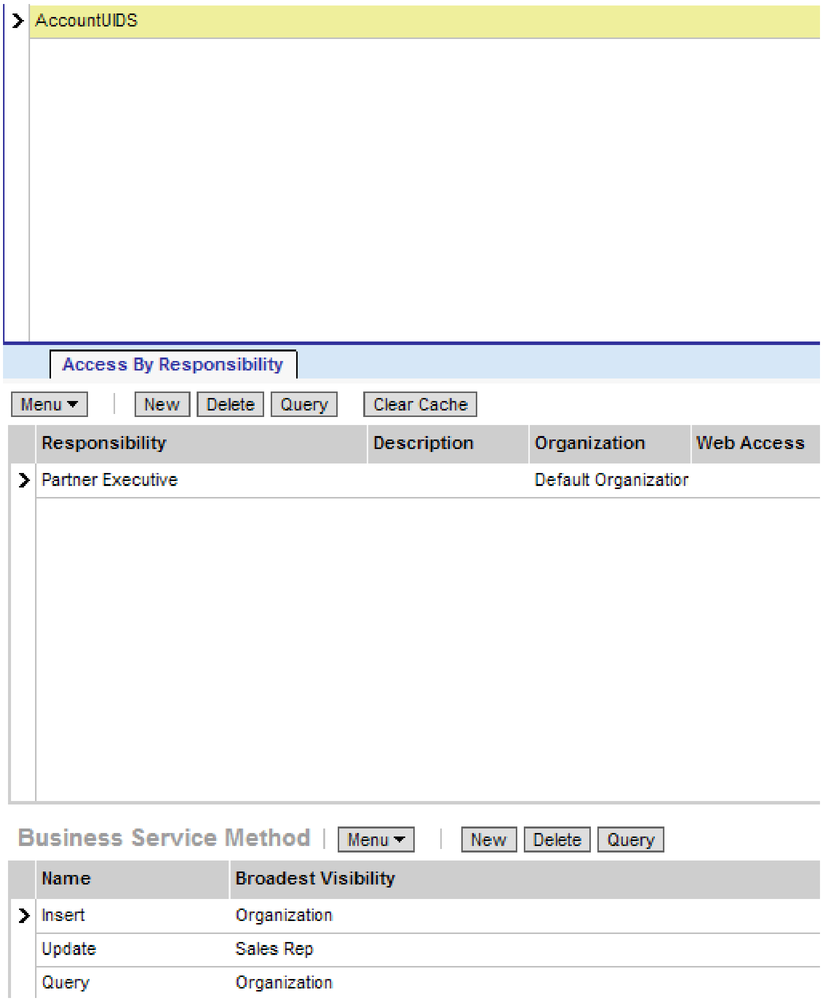
11 From the Broadest Visibility drop-down list, select the view mode to associate with the responsibility.

The business service selected in Step 4 must support view modes to allow you to select a value from the Broadest Visibility drop-down list.

12 Step off the record to save changes.

Example of Associating a Responsibility with Business Service Methods

Figure 12 on page 308 shows the modifications made in the Business Services Method applet so that a user with Partner Executive responsibility can invoke the business service methods Query, Update, and Insert of the business service AccountUIDS.



AccountUIDS

Responsibility	Description	Organization	Web Access
Partner Executive		Default Organizatior	

Name	Broadest Visibility
Insert	Organization
Update	Sales Rep
Query	Organization

Figure 12. Business Service Methods Associated with a Responsibility

A user with Partner Executive responsibility in the example illustrated in Figure 12 can:

- View all accounts that belong to the his or her organization because the business service method Query has Broadest Visibility equal to Organization.
- Update accounts for the sales team of which he or she is a member because the business service method Update has Broadest Visibility equal to Sales Rep.

- Insert a new account as the business service method Insert has Broadest Visibility equal to Organization. If the new account entry matches an existing account entry in the user's organization, an error message appears.

Clearing Cached Business Services

A business service is cached when a user logs in who has access to that business service through the responsibility associated with the user. Users have access only to those business services that were defined for applicable responsibilities at the time that they logged in, even though an administrator might have changed access to business services since that time.

If an administrator makes any changes that affect a user's access to a business service and its associated methods, then the administrator must clear the cache in order to instruct the Siebel application to read updated values from the database. Clearing the cache makes these changes to the business service available to users who log in subsequently or who log out and log in again. The Siebel Server does not have to be restarted.

To clear cached business services

1. Navigate to the Administration - Application screen, Responsibilities, and then the Business Service view.
2. Select the business service in the Business Service list, and then click Clear Cache.

   Changes to the business service that you made prior to clicking Clear Cache are made available to end users the next time that they log in.

Disabling Access Control for Business Services

Enabling access control for business services can have an effect on response times for your Siebel Business Applications. If you do not require access control for business services (that is, you only require prerelease 7.8 access control functionality), you can disable it at the component level for a specific application. To disable access control for business services, you set the parameter OM - Enable Resource Access Control = FALSE for the selected component. The following procedure demonstrates how to set the value for OM - Enable Resource Access Control.

NOTE: The default value for OM - Enable Resource Access Control is True.

To disable access control for business services

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. In the Siebel Servers list, select the Siebel server that hosts the component for which you want to disable access control for business services.
3. In the Components tab, select the component for which you want to disable access control for business services.

4. Click the Parameters tab and query for the parameter `OM - Enable Resource Access Control`.

   The record for `OM - Enable Resource Access Control` appears.

5. In the Value on Restart field, enter False.

6. Step off the record to save changes.

Administering Access Control for Business Processes

Business processes can be accessed by all users by default. However, a user with an administrator login can restrict access to specified business processes and can then associate responsibilities with the restricted business processes, or associate the restricted business processes with responsibilities. This allows the administrator to restrict access to business processes based on the end user's responsibility. To access a restricted business process, an end user must be associated with the responsibility that allows access to it. An end user who is assigned more than one responsibility can access any restricted business process that is associated with one of his or her responsibilities.

To associate business processes with responsibilities, use the same procedure outlined in the following topics, which describe how to associate business services with responsibilities:

- "Associating a Business Service with a Responsibility" on page 305
- "Associating a Responsibility with a Business Service" on page 306

For further information about business processes and workflows, see *Siebel Business Process Framework: Workflow Guide*.

Clearing Cached Responsibilities

A particular responsibility is cached when a user logs in who has that responsibility. Users have access only to those views that were defined for applicable responsibilities at the time they logged in, even though additional views might have been added by an administrator since that time.

If you add, delete, or modify a responsibility in the Responsibilities view (Responsibilities List View), you can clear the cache in order to instruct the Siebel application to read updated values from the database. Clearing the cache makes these changes available to users who log in subsequently or who log out and log in again. The Siebel Server does not have to be restarted.

To clear cached responsibilities

1. Navigate to the Administration - Application screen, then the Responsibilities view.

2. In the Responsibilities list, click Clear Cache.

About 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 shows the same data for all users.

There are often circumstances where you require greater flexibility when determining what data is 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 require more restrictive visibility than your employees.

In order to meet this business requirement, Siebel Business 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 definition
- Use the visibility Auto All property
- Use the Special Frame Class and User Properties

NOTE: This topic provides configuration background information. It does not provide detailed instructions for working in Siebel Tools. For information about using Siebel Tools, see *Configuring Siebel Business Applications*.

Setting Visibility of the Pick List Object Definition

Developers can override the visibility set at the business component level by setting a different visibility type on the Pick List object definition, 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.

For example, you might want partners to be able to add new fund requests and associate those fund requests with campaigns in which they participate. However, you want partners to see only campaigns to which they have access. You can configure a special picklist for this use, and set the visibility on that picklist to Sales Rep, so that partners can only select from accessible campaigns when associating to a fund request.

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 a Siebel application.

About Using the Special Frame Class and User Properties

The developer can use a special frame class and user properties 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 shows positions only for the user’s organization. If users are running Siebel Partner Manager, the applet shows the positions for the user’s own organization and for the suborganizations (or child organizations) of that organization. This allows users to select positions for the partners they manage.

In order to override the pop-up visibility set at the business component level, the developer must make the following changes:

- If the applet whose visibility is to be overridden is an association applet, change the frame class of the applet to CSSSWEFrameListVisibilityAssoc.
- If the applet whose visibility is to be overridden is a pick applet, change the frame class of the applet to CSSSWEFrameListVisibilityPick.
- If the applet whose visibility is to be overridden is an MVG applet, change the frame class of the applet to CSSSWEFrameListVisibilityMvg.
- 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
- Set the business component user property Popup Visibility Auto All to FALSE.

The developer can also set visibility on an applet based on whether the user has access to a view or not. The developer must change the frame class of the applet to CSSSWEFrameListVisibilityPick and add the following user property to the applet:

- Name: `Override Visibility View: [`*`View Name`*`]`
- Value: [*`Visibility Type`*] where the developer can choose from the standard visibility types

For example, to override Campaign Pick Applet popup visibility to All if the user has access to the Campaign Administration List view, add the user property with the following values:

- Name: `Override Visibility View:` *`Campaign Administration List`*
- Value: *`All`*

About Configuring Drilldown Visibility

Drilldown visibility can occur within the same business object or between different business objects. The following topics provide more details on each scenario.

Configuring Drilldown Visibility Within the Same Business Object

If the original view and drilldown view are both based on the same business object, and visibility is unspecified in the drilldown view, whatever visibility is in effect in the original view is continued in the drilldown view.

If the drilldown view of a drilldown object has a different Visibility Applet Type setting from the original view, drilling down on a record takes the user to the first visible record of the destination view. It does not to the drilldown record.

Configuring Drilldown Visibility Between Different Business Objects

If the original view and drilldown view are based on different business objects, moving from the original view to the drilldown view might require that you configure visibility in the drilldown view to something other than its standard setting.

If you have to configure visibility in the drilldown view, note that two types of drilldown object exist:

- ID-based drilldown object
- Bookmark-based drilldown object

The drilldown object is ID-based when it has values specified for the Business Component and Source Field properties. Otherwise, it is a bookmark-based drilldown object.

The visibility rules in the drilldown view are the same for the two types of drilldown object, with the following exception; for an ID-based drilldown, setting the Visibility Type property of an applet's drilldown object overrides the Visibility Applet Type setting of the drilldown view. For example, assume you configure a drilldown object with a visibility type of All. It overrides other visibility types (for example, Sales Rep visibility) on the drilldown view when the user drills down.

The Visibility Type property in a drilldown object only overrides the drilldown view Visibility Applet Type property once, that is, when you drill down. If you navigate to another view in the screen and then return to the drilldown view, the original visibility of the drilldown view is applied. The visibility is refreshed every time you navigate to a different view in the same screen after drilling down.

For example, assume that you navigate to a view with personal access control in the same screen after drilling down; the drilldown record is no longer visible. If you then navigate back to your original drilldown view (with Sales Rep visibility) the drilldown record remains invisible. If you navigate to a third view with All visibility, you can see your drilldown record again.

Visibility Rules for the Drilldown Object Type

If the drilldown view is a detail view that does not have visibility specified, and the drilldown object does not have visibility specified, visibility on the drilldown view's screen applies in the following order (assuming that the business component is configured for visibility):

- All
- Organization
- Manager
- Sales Rep

NOTE: You can only specify visibility on an ID-based drilldown object.

For more information about the Drilldown object type, see *Siebel Object Types Reference*.

Visibility Rules for the Link Object Type

After you drill down to another screen, the thread bar is updated. The current view displays its records using a master-detail relationship, based on the value of the link property Visibility Rule Applied in the original view (before the drilldown).

If Visibility Rule Applied is set to Never, no additional visibility rules apply. The thread context's master-detail relationship determines the records visible in the view, regardless of the visibility setting for the current view. If you change the view using the viewbar, the thread context is retained. Records can be displayed that normally (without the thread context) are not visible in this new view.

If Visibility Rule Applied is set to Always, additional visibility rules apply. Siebel Business Applications might display an error message when a user performs a drilldown to notify the user that he or she does not have the appropriate privileges to see the detail records.

For more information about the Link object type, see *Siebel Object Types Reference*.

Example of Visibility in a Drilldown Between Different Business Objects

The following example illustrates how the visibility rules described above apply when a user drills down from the Opportunity business object to the Quote business object. In the Opportunity Quote View, a user drills down on the Name field of an entry in the Opportunity Quote List Applet to the Quote Detail View. In the screen (Quotes Screen) of Quote Detail View, the visibility type of all views accessible by the user are checked. Visibility is applied in the following order:

- If an accessible view has visibility equal to All, this visibility applies after the user drills down to Quote Detail View.
- If an accessible view has visibility equal to Organization, this visibility applies after the user drills down to Quote Detail View.
- If the user's position equals Manager and an accessible view has visibility equal to Manager, Manager visibility applies after the user drills down to Quote Detail View.
- If an accessible view has visibility equal to Sales Rep or Personal, this visibility applies after the user drills down to Quote Detail View.

An error message appears if the user does not have the appropriate visibility to view the record in the Quote Detail view.

Party Data Model

The S_PARTY table is the base table for all of the parties listed in Table 26 on page 251: Person (Contact), User, Employee, Partner User, Position, Account, Division, Organization, Partner Organization, Household, User List, and Access Group.

For each party record stored in the S_PARTY table, the value of the PARTY_TYPE_CD column denotes the party type. Along with the party type, extension tables provide the primary differentiation between the different parties.

For information about how joins are used to draw data from multiple tables into a single business component—such as is done for Employee, Account, and other business components for party-type data, see *Configuring Siebel Business Applications*.

In Figure 13 on page 316, the base table and extension tables that make up the party data model are shown within the Party boundary (the dark box). The tables shown outside of the Party boundary are used to define relationships among parties. topics that follow illustrate how the party data model applies to various particular parties.

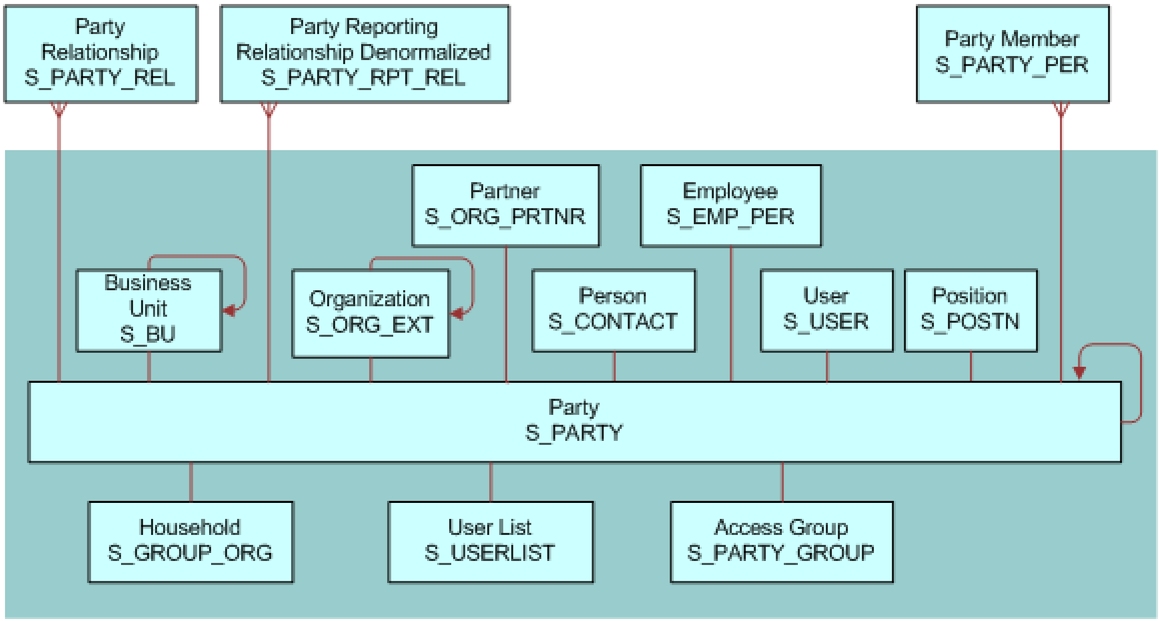


Figure 13. Party Data Model

How Parties Relate to Each Other

Parties have some required relationships, as described below.

- 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 (INT_ORG_FLG = “Y”) and it has an associated S_BU record.
- 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.
- Persons (contacts), users, employees, partner users are instances of the Person party type.
- Typically, you associate each employee and partner user with one or more positions. The employee or partner user has only one active position at one time. The employee or partner user is automatically associated with one division and one organization at a time—the division and organization associated with the active position.

  CAUTION: Merging employee records is not recommended. You can disrupt party relationships to a significant extent and get unexpected results.

- For purposes of granting visibility to data, associations of parties of type Person with other types of parties are stored using the S_PARTY_PER table. For example, accounts are associated with contacts, users are associated with positions, and so on. A user associated with a position can see data for accounts or opportunities assigned to the position (when this is the active position). Relationships stored in S_PARTY_REL also affect data routing for mobile users.
- For purposes of storing ad hoc, informational relationships between parties, such associations are stored using the S_PARTY_REL table. For example, a company and its accounting firm might both be stored as accounts. Assuming that your application provides the capability to define this relationship, it can be stored in the S_PARTY_REL table.
- Ad hoc and informational relationships between parties are stored in the table S_PARTY_REL. For example, a company and its accounting firm might both be stored as accounts. The relationship between these two accounts can be stored in the S_PARTY_REL table, assuming that your application has been configured to define these relationships.

Person (Contact) Data Model

In Figure 14 on page 317, the base table and extension table (S_CONTACT) that define a Person, or Contact, are shaded. A Person is the simplest representation of an individual in the database.

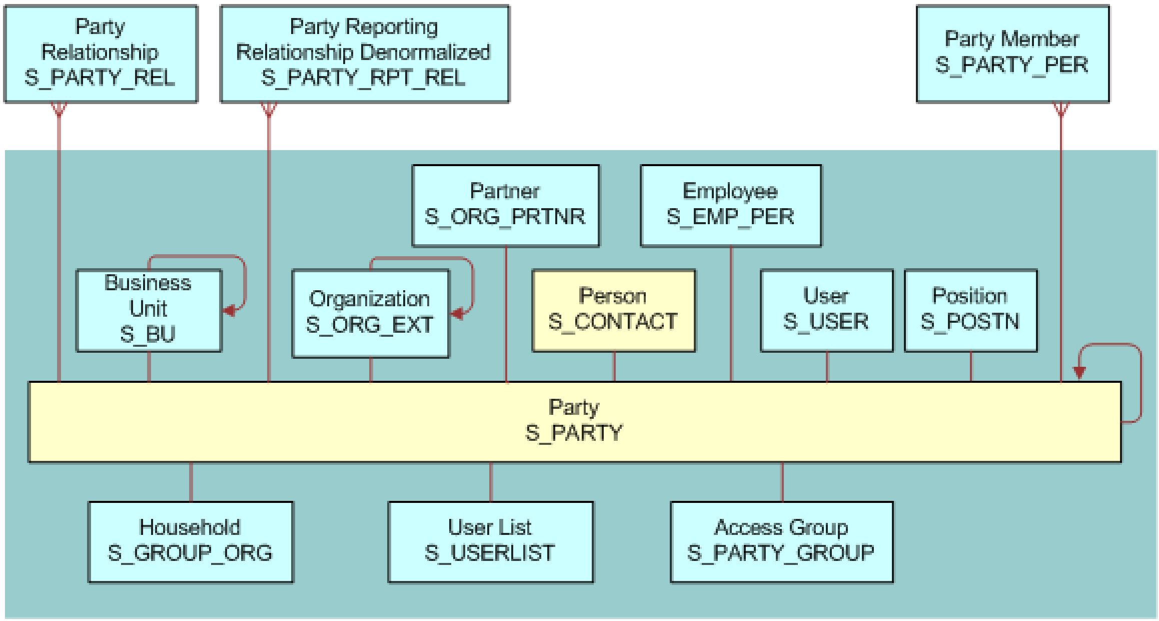


Figure 14. Person (Contact) Data Model

User Data Model

In Figure 15 on page 318, the base table and extension tables (S_CONTACT and S_USER) that define a User are shaded. A User is a Person with the following added qualities:

- The S_USER table contains a login for this user.
- The S_PER_RESP intersection table (not shown) specifies a responsibility for this user.
- It is possible to promote a contact to a user. For example, adding a User ID value for a person in the All Persons view in the Administration - User screen causes the person to appear as a user in the Users view.

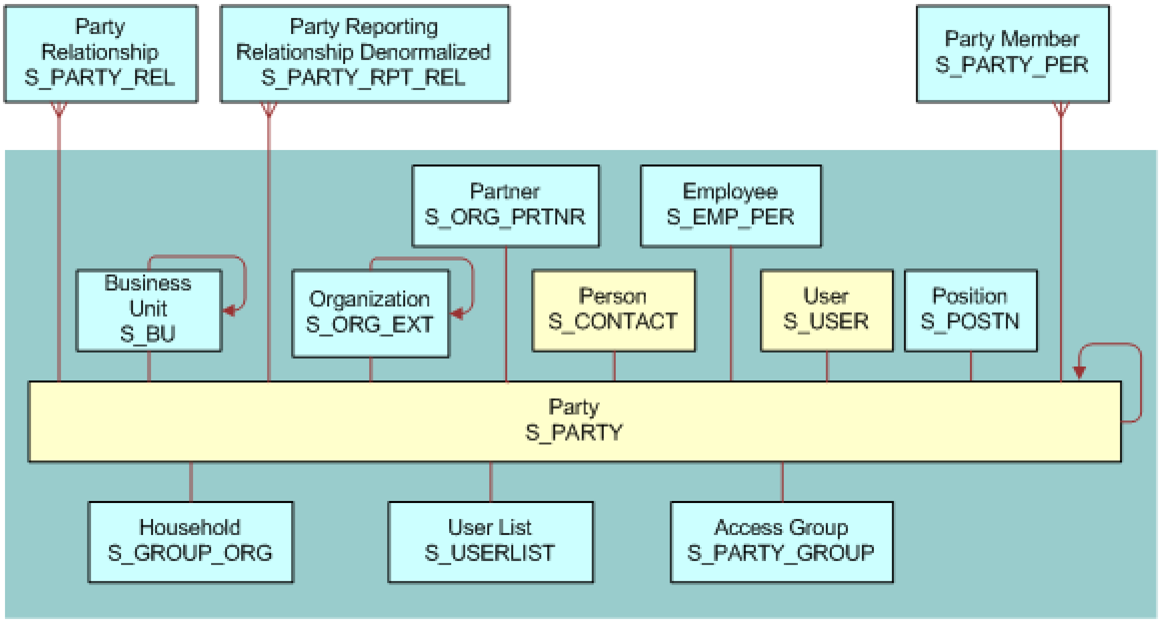


Figure 15. User Data Model

Employee Data Model

In Figure 16 on page 319, the base table and extension tables (S_CONTACT, S_USER, and S_EMP_PER) that define an Employee are shaded. Internal Employees and Partner Users are each represented as Employee records.

An Employee is a User with the following added qualities:

- S_EMP_PER provides employee data for this user.
- A position defined using the S_POSTN table is typically (but not necessarily) associated with an employee.
    - If the organization to which the position belongs is not a partner organization, then the employee is an internal employee.

- If the organization is a partner organization, then the employee is a partner user.

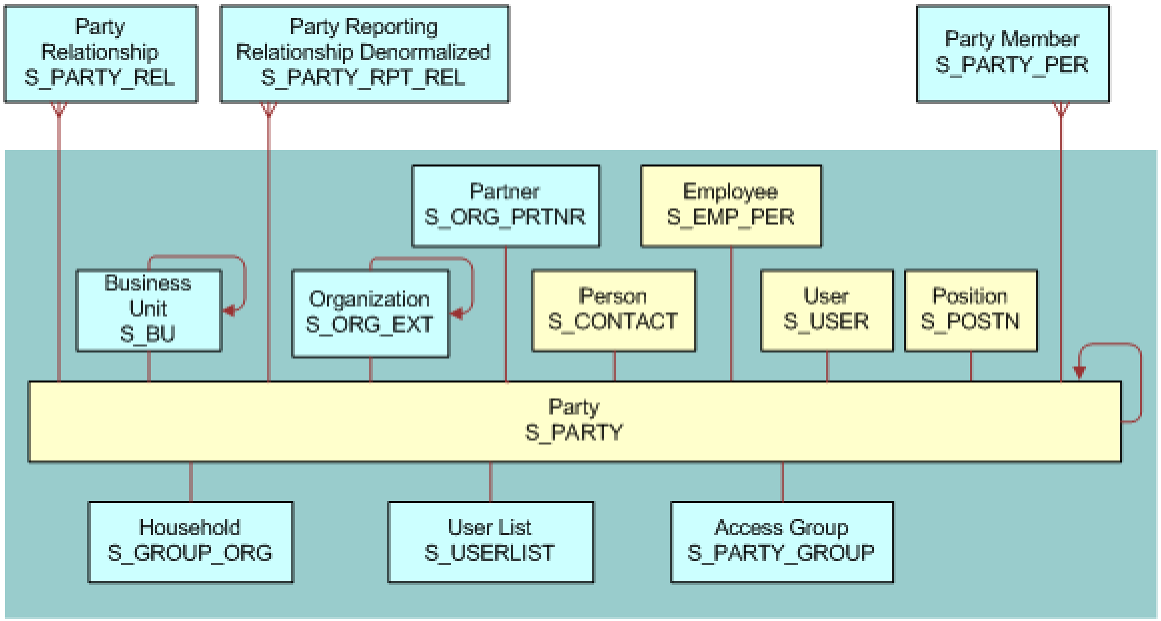


Figure 16. Employee Data Model

Position Data Model

In Figure 17 on page 320, the base table and extension table (S_POSTN) that define a Position are shaded.

In positions, as in other areas of Siebel Business Applications, 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).

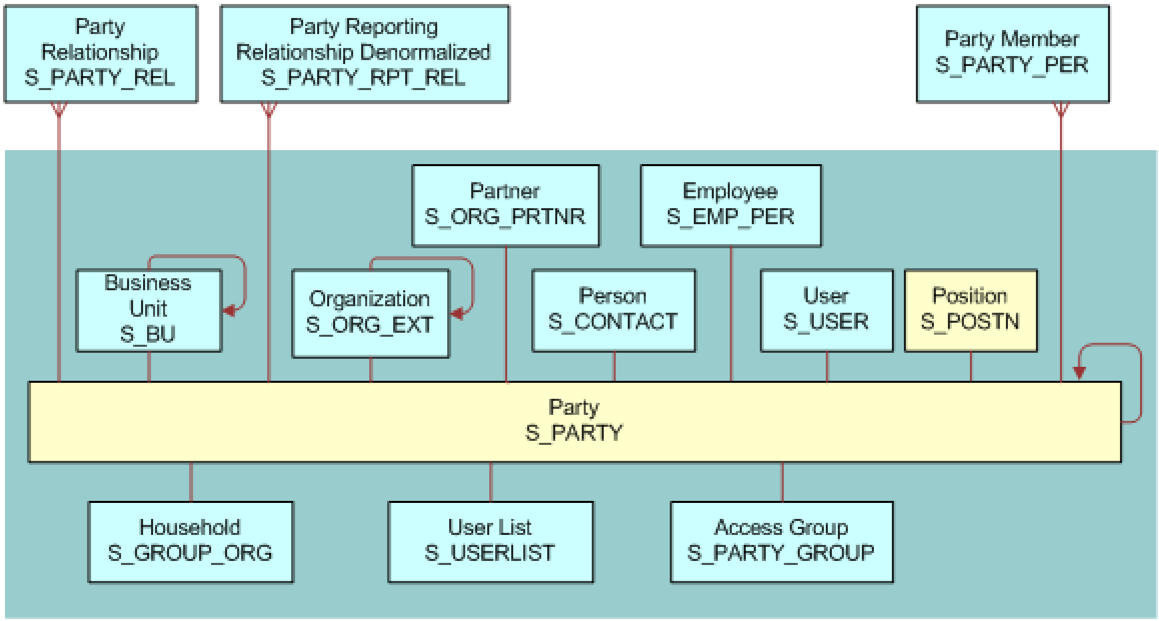


Figure 17. Position Data Model

Account Data Model

In Figure 18 on page 321, the base table and extension table (S_ORG_EXT) that define an Account are shaded.

(Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.)

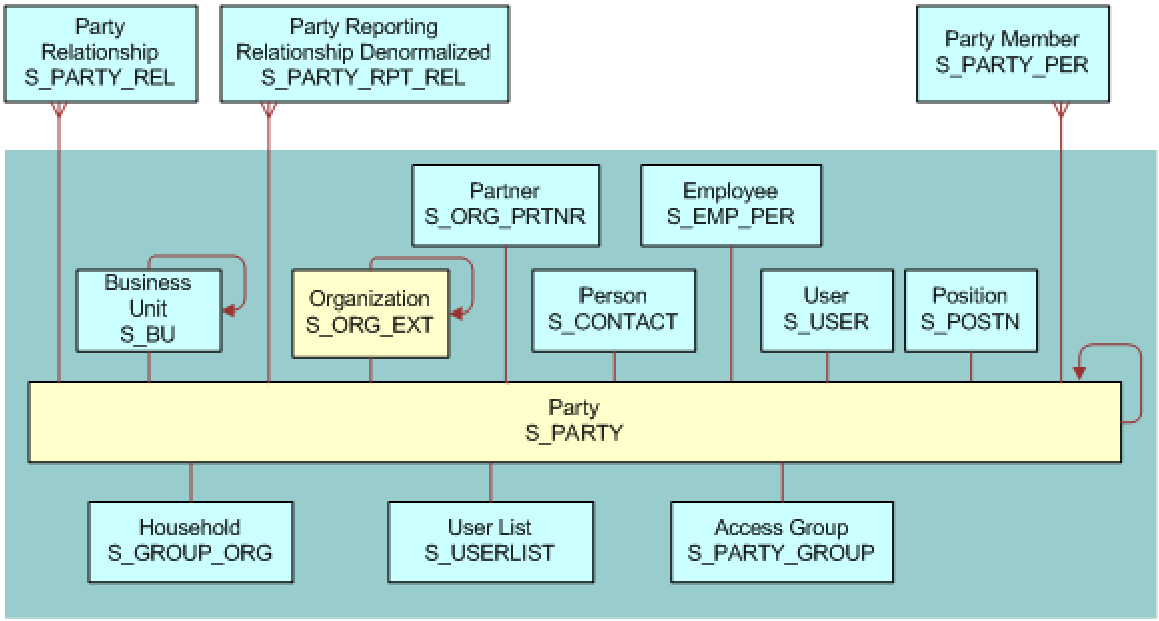


Figure 18. Account Data Model

Division Data Model

In Figure 19 on page 322, the base table and extension table (S_ORG_EXT) that define a Division are shaded.

In S_ORG_EXT, the flag INT_ORG_FLG = Y specifies that a division is an internal organization. (For an account, this flag is set to N.)

(Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.)

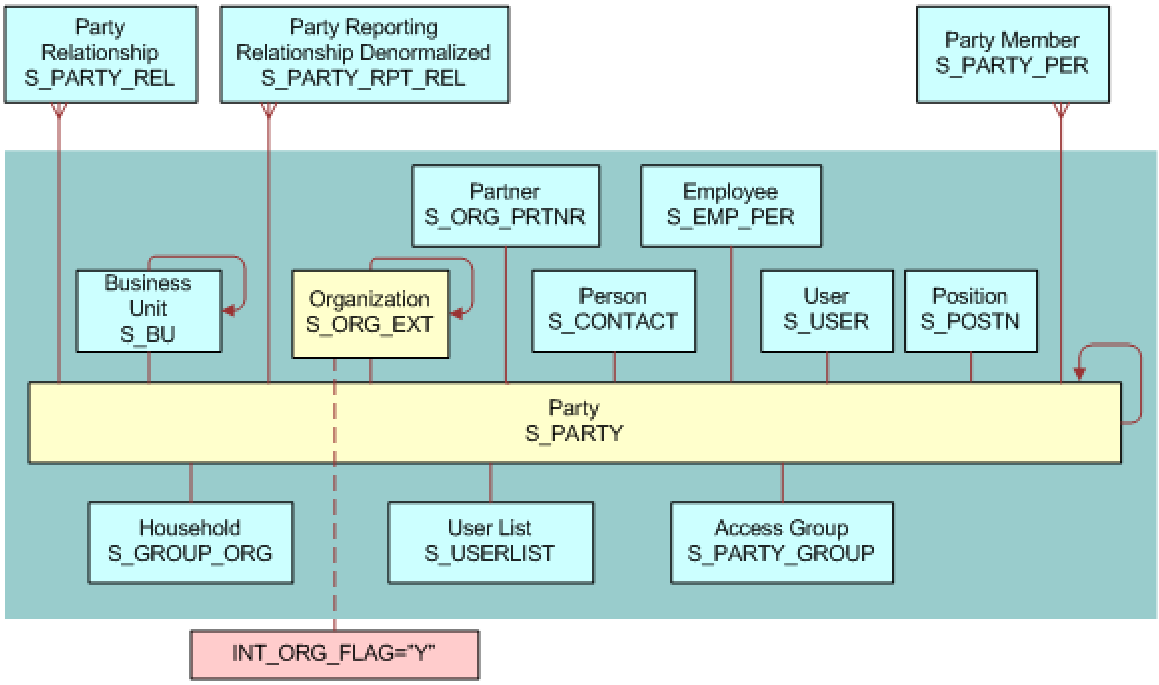


Figure 19. Division Data Model

Organization Data Model

In Figure 20 on page 323, the base table and extension tables (S_ORG_EXT and S_BU) that define an Organization are shaded.

An Organization, sometimes known as a business unit, is also a Division, but has a record in the S_BU table.

(Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.)

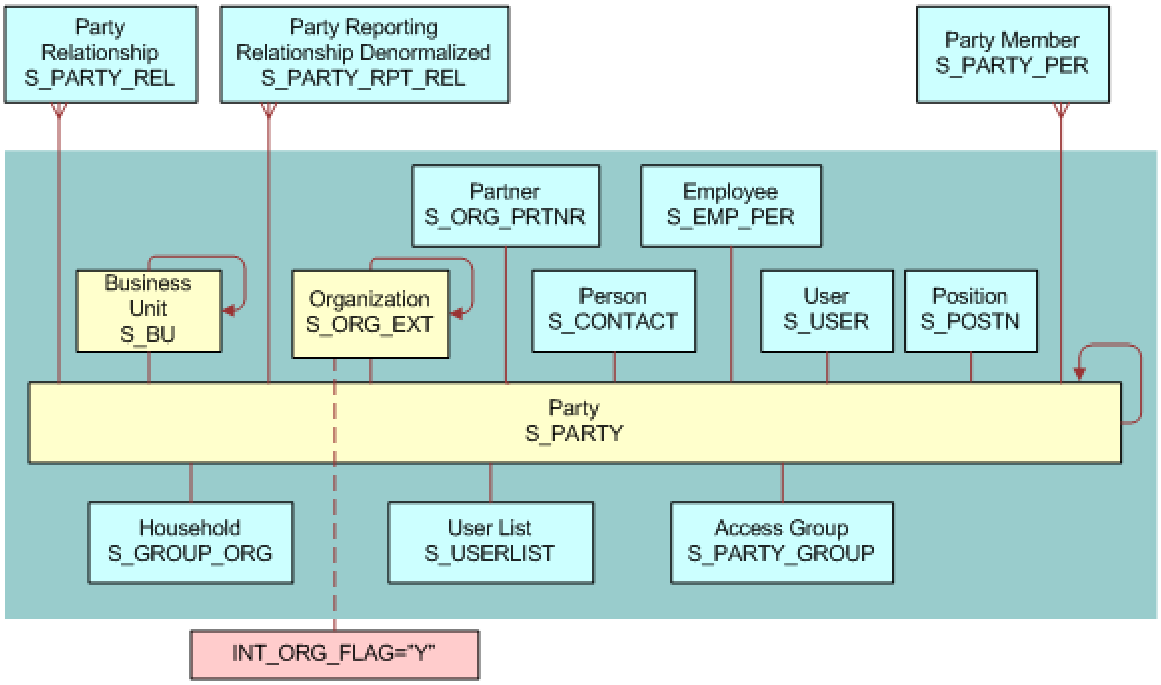


Figure 20. Organization Data Model

Partner Organization Data Model

In Figure 21 on page 324, the base table and extension tables (S_ORG_EXT, S_BU, and S_ORG_PRTNR) that define a Partner Organization are shaded.

A Partner Organization is the same as an Organization but the flag PRTNR_FLG in S_ORG_EXT qualifies it as a Partner Organization.

(Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.)

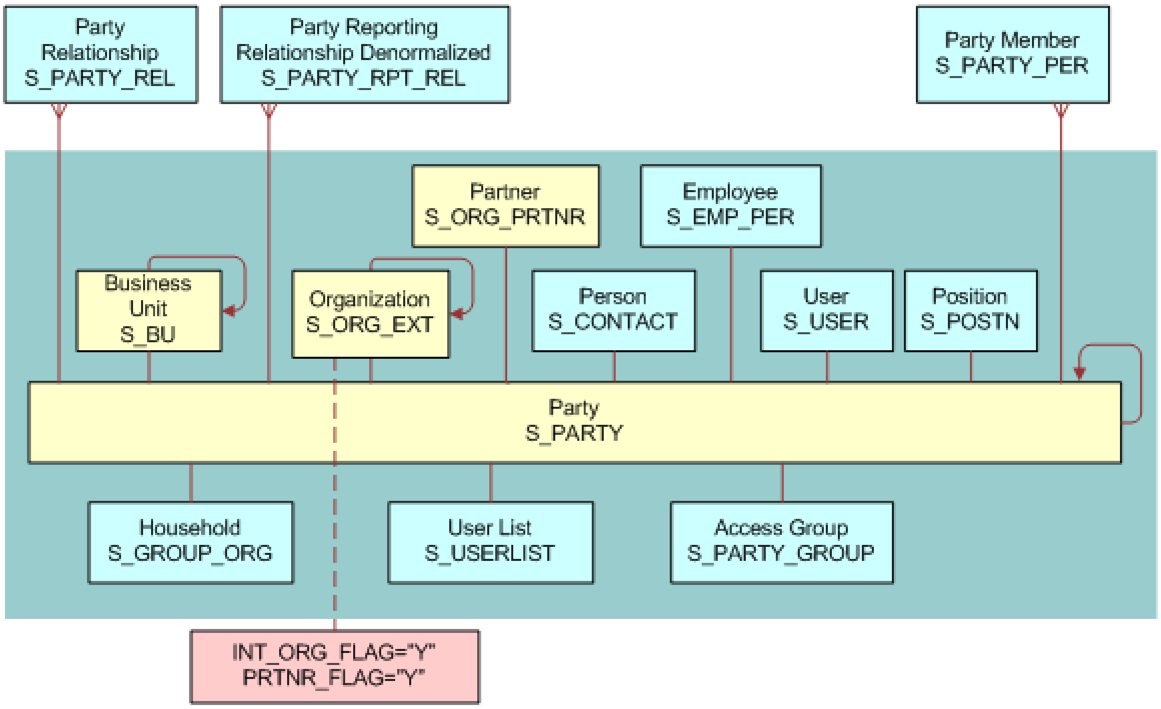


Figure 21. Partner Organization Data Model

Household Data Model

In Figure 22 on page 325, the base table and extension table (S_ORG_GROUP) that define a Household are shaded.

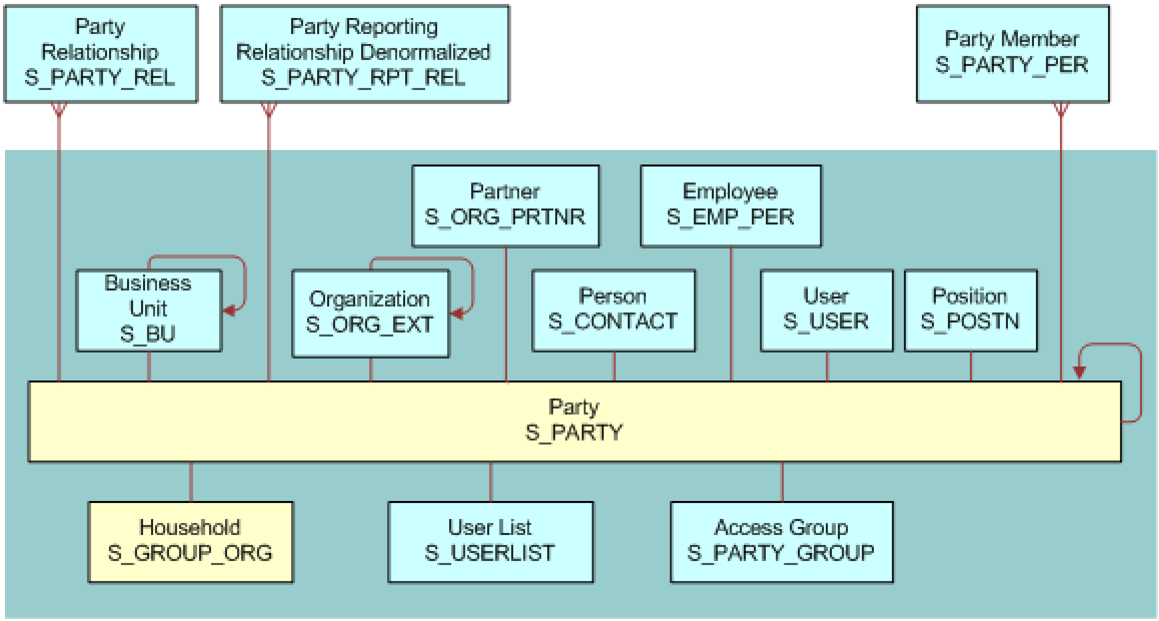


Figure 22. Household Data Model

User List Data Model

In Figure 23 on page 326, the base table and extension table (S_USERLIST) that define a User List are shaded.

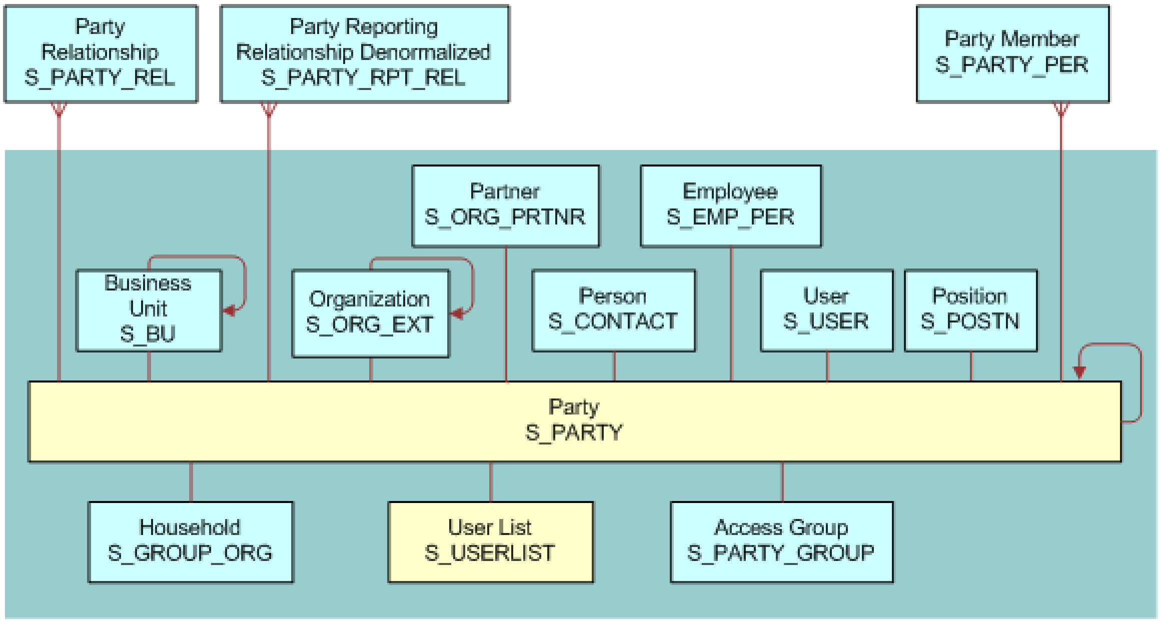


Figure 23. User List Data Model

Access Group Data Model

In Figure 24 on page 327, the base table and extension table (S_PARTY_GROUP) that define an Access Group are shaded.

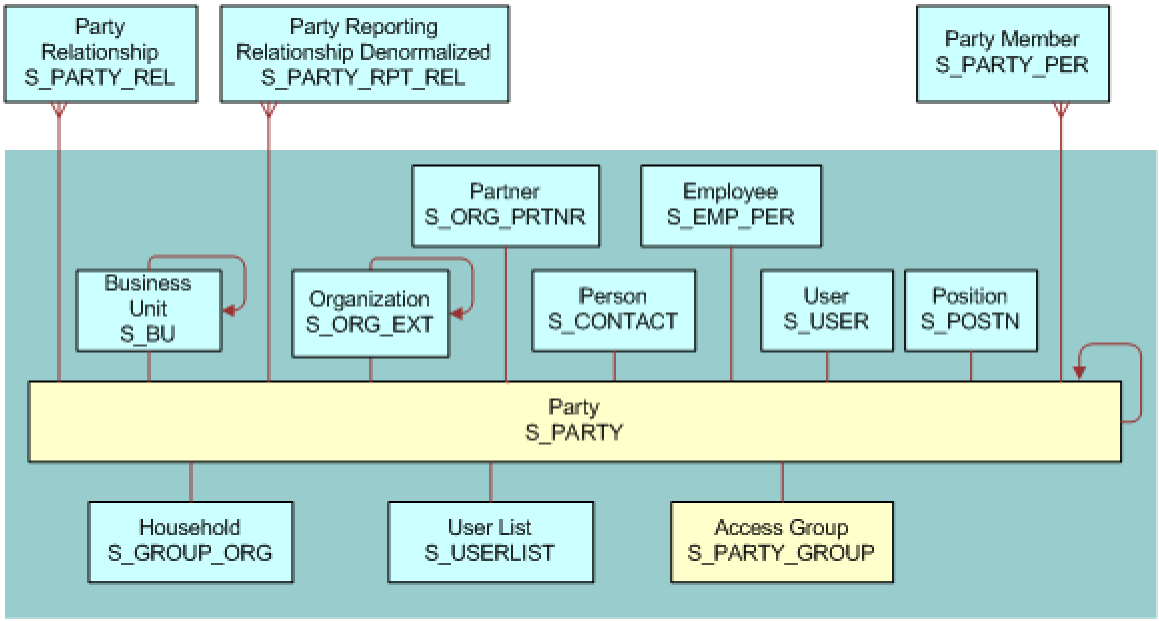


Figure 24. Access Group Data Model

A Troubleshooting Security Issues

This appendix provides troubleshooting tips and information about security-related issues that can occur in Siebel Business Applications. It includes the following topics:

- User Authentication Issues on page 329
- User Registration Issues on page 330
- Access Control Issues on page 332

User Authentication Issues

This topic describes problems that can occur when authenticating users.

User is Unable to Work in the Administration - Server Configuration / Management Screen

The server administration component performs its own authentication by verifying that the Siebel user ID it gets from the Siebel Application Object Manager (AOM) is the user name for a database account. An 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.

When you use external authentication, server administrators might not be able to access the Administration - Server Configuration or Administration - Server Management screen. Alternatively, if the system is configured to use the audit trail feature, some audit trail problems can occur.

To allow administrator users to work in server administration and management screens (and avoid audit trail problems), for each user in this relatively small group, use database authentication instead of external authentication. Administrator users can log into the application using either a different AOM or a Siebel Developer Web Client—in each case, database authentication must be configured.

Alternatively, authentication for a secondary data source such as the Siebel Gateway Name Server can be configured.

For more information about database authentication, see "Configuring Database Authentication" on page 112 and related sections.

Adding Users or Changing Passwords Is Not Reflected in the Directory

If you add users or change passwords in Siebel Business Applications and the changes are not reflected in the directory, make sure the PropagateChange parameter is set to TRUE for the security adapter. For more information, see "Siebel Gateway Name Server Parameters" on page 341.

Responsibilities in the Directory Conflict with Responsibilities in Siebel Business Applications

It is recommended that you assign user responsibilities in the directory or by using Siebel Business Applications, but not both. For more information, see "Configuring Roles Defined in the Directory" on page 172.

Upgrading Siebel Application Appears to Disable Checksum Validation

You must recalculate the security adapter's CRC checksum value whenever you upgrade your Siebel Business Applications. For more information, see "Configuring Checksum Validation" on page 165.

"Web Authentication Failed" Error Message Appears in Application Log File

If your installation is configured for Web SSO (without anonymous browsing) and the ProtectedVirtualDirectory parameter is not set, this message might appear.

To fix this error, set the ProtectedVirtualDirectory parameter in the eapps.cfg file to the same value as the application directory. For example:

```
[/eSales]
ProtectedVirtualDirectory=/eSales
```

User Registration Issues

This topic describes problems that can occur when registering users.

Workflows Do Not Appear in the Business Process 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 param lang=`*LANGUAGE*, where *LANGUAGE* is your three-letter database language code. Restart the server.

When I Click New User, Either Nothing Happens or an Error Message 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 for Self-Registration" on page 216.
- Using Server Manager, connect to the server and run `list param lang` to verify. If the language code is incorrect, you can run `change param lang=`*LANGUAGE*, where *LANGUAGE* 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 might be new to the database but might 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 must to be restarted.

In the Administration - Server Management screen, restart only the necessary AOMs. Restarting the server will also work.

When I Click Next in a User Registration View, Nothing Happens

There might 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

1. In the Administration - Runtime Events screen, click the Events view.
2. 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.

3. 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.
4. 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 SecThickClientExtAuthent system preference is not set to TRUE.
- The Siebel Server has not been restarted since setting the system preferences. For information about the system preference related to user authentication, see "Setting a System Preference for Developer Web Clients" on page 153.

Check to see if the user exists in the Person view in the Administration - User 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 topic describes problems related to access control.

Employee User Has Trouble Logging into a Siebel Customer Application

It is not recommended to use an Employee login account to access a customer application (such as Siebel Sales). Instead, give the user a separate login account for the application.

Cannot Delete Division Records

You cannot delete division records because business components throughout your Siebel Business 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 cannot 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 for Views and Responsibilities" on page 277.

Unexpected Refresh Causes Loss of Data

When you enter records on particular views (for example, *Service Request List View*), records can appear lost if the underlying business component is re-queried before a user is assigned to the access list. This event can occur if the associated detail applet (for example, *Service Request Entry* applet) expands or collapses to show or hide additional fields. By default, collapsing or expanding a detail applet results in the record being committed and the business component being requeried.

You can override the default behavior described above by setting the user property RestrictedFieldActivation to FALSE. Setting RestrictedFieldActivation to FALSE means that the business component is not re-queried if the detail applet expands or collapses. You can set RestrictedFieldActivation to FALSE in one of the two following locations:

- In the [InfraUIFramework] section of the client configuration file.
- In the applet. To set the value of RestrictedFieldActivation in the applet, you add it to the user properties of the applet in Siebel Tools.

CAUTION: It is not recommended to set RestrictedFieldActivation = FALSE in the [InfraUIFramework] section of a configuration file as it can degrade the scalability of your Siebel deployment. You are advised to set the value of RestrictedFieldActivation in the applet using Siebel Tools.

In addition to specifying the applet, you can also specify the view mode where you disable an automatic re-query of the business component when a detail applet collapses or expands. To specify the view mode, add the following entry to the user properties of the applet in Siebel Tools:

`NoRestrictedFieldActivationMode`*`number`*`r` *`valueOfVisibilityMode`*

For example, the following entries override the default behavior in the Personal and Manager view modes:

```
NoRestrictedFieldActivationMode1 Personal
```

```
NoRestrictedFieldActivationMode2 Manager
```

B Configuration Parameters Related to Authentication

This appendix describes the configuration parameters that are applicable to implementing a security adapter. It includes the following topics:

- Parameters in the eapps.cfg File on page 335
- Siebel Gateway Name Server Parameters on page 341
- Siebel Application Configuration File Parameters on page 348

In general, parameters values related to security adapter configuration must be verified by your LDAP or ADSI administrator, or database administrator. Many values shown are examples only and might not be suitable for your deployment.

Parameters in the eapps.cfg File

The eapps.cfg file contains parameters that control interactions between the Siebel Web Engine and the Siebel Web Server Extension (SWSE), for all Siebel Business Applications deploying the Siebel Web Client.

The eapps.cfg file is located in the *SWEAPP_ROOT*\bin directory after you apply a SWSE logical profile, where *SWEAPP_ROOT* is the directory in which you installed the SWSE.

The eapps.cfg file includes sections such as [swe], [defaults], and [connmgmt] and sections for individual Siebel Business Applications, such as [/prmportal_enu] and [/callcenter_enu]. Each parameter value in the [defaults] section is used by all individual applications, unless you override the parameter's value with an entry in an application's own section.

The following list is a portion of a sample eapps.cfg file. This sample includes some parameters that might not coexist. They are provided so you can see a range of authentication-related parameters. In the eapps.cfg sample, the AnonUserName and AnonPassword values in the [/prmportal_enu] section are used by Siebel Partner Portal instead of the values provided in the [defaults] section.

```
[swe]
Language = enu
Log = all
LogDirectory = D:\sba80\SWEApp\log
ClientRootDir = D:\sba80\SWEApp
WebPublicRootDir = D:\sba80\SWEApp\public\enu
SiebEntSecToken = fJq&29&58hJaY(A8!Z
IntegratedDomainAuth = FALSE

[defaults]
EncryptedPassword = TRUE
AnonUserName = GUESTCST
AnonPassword = fhYt8T*9N4e8&Qay
StatsPage = _492394stats.swe
SingleSignOn = TRUE
TrustToken = mR*739DAPw*94%O2
UserSpec = REMOTE_USER
UserSpecSource = Server
DoCompression = TRUE
SessionTimeout = 900
GuestSessionTimeout = 300

[/prmportal_enu]
AnonUserName = guestcp
AnonPassword = aGr^92!8RWnf7Iy1
ProtectedVirtualDirectory = /p_prmportal_enu
ConnectString = siebel.TCPIP.None.None://172.20.167.200:2320/SBA_80/
eChannelObjMgr_enu
SiebEntSecToken = ^s*)Jh!#7^s*)Jh!#7

[connmgmt]
CACertFileName = d:\siebel\admin\cacertfile.pem
CertFileName = d:\siebel\admin\certfile.pem
KeyFileName = d:\siebel\admin\kefile.txt
KeyFilePassword = ^s*)Jh!#7
PeerAuth = FALSE
PeerCertValidation = FALSE
```

Typically, password encryption is in effect for the eapps.cfg file, as determined by the setting EncryptedPassword = TRUE. In this case, values for SiebEntSecToken, AnonPassword, and TrustToken are encrypted. For more information, see "Managing Encrypted Passwords in the eapps.cfg File" on page 45.

NOTE: It is recommended that you set the value for StatsPage to a value other than the default value (_stats.swe). For further information on this parameter, see 478289.1 (Article ID) on My Oracle Support. This document was formerly published as Siebel Alert 1124.

You can edit the parameters in the eapps.cfg file manually using a text editor or you can configure and apply a SWSE logical profile using the Siebel Configuration Wizard. When you edit configuration files, do not use a text editor that adds additional, nontext characters to the file. For information on using the Siebel Configure Wizard to configure SWSE parameters, see *Siebel Installation Guide* for the operating system you are using.

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

Authentication-Related Parameters

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

- **AnonUserName.** This parameter specifies the user name required for anonymous browsing and initial access to the login pages. The user name selected requires access to views intended for anonymous browsing, but must otherwise be the name of a restricted user.
- **AnonPassword.** The password corresponding to the value entered for AnonUserName.

- **ClientCertificate.** When this parameter is set to TRUE in a Web SSO implementation, the user is authenticated through a digital certificate.

  See also "Digital Certificate Authentication" on page 195.

- **EncryptedPassword.** When this parameter is set to TRUE, the password for the anonymous user and the Web update password are interpreted as encrypted passwords. This parameter is added to the eapps.cfg file (with a value of TRUE) when you apply a SWSE logical profile using the Siebel Configuration Wizard for SWSE. However, if the parameter is not defined in the file, this is equivalent to a value of FALSE.

  For more information, see "Managing Encrypted Passwords in the eapps.cfg File" on page 45.

- **EncryptSessionId.** When this parameter is set to TRUE (the default), the session ID will be encrypted. When it is FALSE, the session ID is not encrypted. For a Siebel Web Client, the session ID is used in the session cookie (in cookie-based mode) or in the application URL (if cookie-based mode is not enabled).

  For more information about cookies, see "About Using Cookies with Siebel Business Applications" on page 204.

- **GuestSessionTimeout.** The time, in seconds, that a connection open for anonymous browsing can remain idle before it times out. The default is 300 seconds (5 minutes).

  Guest sessions are used for anonymous browsing. They permit users to navigate portions of the site without logging in. In contrast to anonymous sessions, guest sessions are associated with an individual Siebel Web Client. These sessions are opened when an unregistered user starts navigating the site, and the sessions remain open until the Web client logs out or times out due to inactivity.

  When deciding how long guest user timeout is to be, the primary consideration is whether or not anonymous browsing is being used. If anonymous browsing is being used, guest user timeouts must be greater than the average time users require to deliberate their next action. In other words, this is the time allowed between user actions.

  Both guest and anonymous sessions use the AnonUserName and AnonPassword parameters to log in. For more information on setting this parameter, see *Siebel Performance Tuning Guide*.

- **SessionTimeout.** The time, in seconds, from the user's last browser request until the user's connection times out. The default is 900 seconds (15 minutes). Table 30 offers guidelines for setting this parameter.

  Standard sessions are those where users log in using their registered user name and password. Otherwise, standard sessions share many of the same characteristics as guest sessions.

  Table 30. Guidelines for Setting Session Timeouts

Session Type	Condition	Recommended Setting
Anonymous session	■ Large numbers of users logging in within a short period of time (login spikes) ■ Frequent logins and logouts	Greater than 30 minutes.
Guest	■ Long intervals between user actions ■ Login view is used for logins ■ Logout occurs on a logout view	Greater than 30 minutes. Less than 5 minutes. Less than 5 minutes.
Regular	■ Employee applications ■ Customer applications ■ High security requirements ■ High continuity (low interaction) with the browser ■ Lightly loaded system	Greater than 30 minutes. 1-15 minutes. Less than 5 minutes. Greater than 30 minutes. Greater than 30 minutes.

  Session timeout refers to session inactivity. That is, if session timeout is set to 3600 seconds, then it requires one hour of session inactivity for that session to time out. Session inactivity means no request is made to the Siebel Server on that session. Any act that sends a ping request to the Siebel Server, such as message broadcasting, resets the session timeout period. If the update interval is less than the SessionTimeout set in the eapps.cfg file, the session never times out.

  If you use the Siebel Portal Framework to implement portal views, note that Siebel Business Applications time out if user activity in the portal view exceeds the time that is specified by SessionTimeout. Note also that, by default, portal views send a ping status request to their server every 120 seconds (2 minutes) to keep their session alive. For more information about the Siebel Portal Framework, see *Siebel Portal Framework Guide*. For more information about setting the SessionTimeout parameter, see *Siebel Performance Tuning Guide*.

- **SingleSignOn.** The SWSE operates in Web SSO mode when this parameter is TRUE. For more information, see Chapter 7, "Web Single Sign-On Authentication."

- **SubUserSpec.** In a Web SSO environment that implements digital certificate authentication, a value of CN specifies that the Siebel user ID is to be extracted from the certificate's CN (Common Name) attribute. For more information, see "Configuring the User Specification Source" on page 196.

- **TrustToken.** In a Web SSO environment, this token string is a shared secret between the SWSE and the security adapter. It is a measure to protect against spoofing attacks. This setting must be the same on both the SWSE and the security adapter.

  For more information, see Chapter 7, "Web Single Sign-On Authentication."

- **UserSpec.** In a Web SSO implementation, this variable name specifies where the SWSE looks for a user's user name 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 or AIX, use the value CERT_SUBJECT, a variable that contains the certificate name. For example, UserSpec/SubUserSpec is "`CERT_SUBJECT"/"CN"`. For other UNIX operating systems, use the value `"REMOTE_USER"` for the UserSpec parameter. The SubUserSpec setting is disregarded.

  For more information, see "Configuring the User Specification Source" on page 196.

- **UserSpecSource.** In a Web SSO implementation, this parameter specifies the source from which the SWSE derives the user credentials:

  - **Server.** If credentials are derived from the usual Web server user name field
  - **Header.** If credentials are derived from the variable within the HTTP request header.

  For more information, see "Configuring the User Specification Source" on page 196.

The following parameter can be defined in the section for each individual Siebel application. Do not define this parameter in the [defaults] section.

- **ProtectedVirtualDirectory.** 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.

  For more information, see "Creating Protected Virtual Directories" on page 184.

  For example, if you used the suggested name for the protected virtual directory for Siebel eService, enter:

  ```
  [/eservice_enu]
  ProtectedVirtualDirectory = /p_eservice
  ```

  If your Web SSO implementation is not configured for anonymous browsing, set this value to the same directory as your application. For example:

  ```
  [/eservice_enu]
  ProtectedVirtualDirectory = /eservice
  ```

  Otherwise, a Web Authentication Failed message might appear in the application's log file.

  NOTE: You use examples like those above to secure an entire application. However, if some parts of the application do not require authentication, you must be able to authenticate users when they access a secured part of the application. In this case, set the parameter to an alias where the Web SSO credentials are passed. Siebel Business Applications redirect the authentication request.

The following parameter in the eapps.cfg file can be defined in the [swe] section of the file.

- **IntegratedDomainAuth.** To support Windows Integrated Authentication for Web SSO, set this parameter to TRUE. This setting causes SWSE to strip out the domain name from HTTP headers, which allows the application to integrate with Windows Integrated Authentication.

SSL-Related Parameters

The following parameters can be included in the [connmgmt] section of the eapps.cfg file, when you are using SSL to encrypt SISNAPI communications between the Web server and the Siebel Server. For more information, see "Configuring SSL Encryption for SWSE" on page 78.

- **CACertFileName.** Identifies the trusted authority who issued the certificate.
- **CertFileName.** Specifies the name of the ASN/PEM certificate file.
- **KeyFileName.** Specifies the name of the PEM private key file.
- **KeyFilePassword.** Specifies the password to decrypt the private key file.
- **PeerAuth.** Enables peer authentication during SSL handshake. PeerAuth is FALSE by default. Set PeerAuth to TRUE to authenticate certificates from the Siebel Server. The SWSE requires the certifying authority's certificate to authenticate the certificate from the Siebel Server.
- **PeerCertValidation.** Independently verifies that the hostname of the SWSE computer matches the hostname presented in the certificate.

Siebel Gateway Name Server Parameters

Parameters for the Siebel Gateway Name Server can be set at one or more of the Enterprise, Siebel Server, or component levels. They are set in the Administration - Server Configuration screen of a Siebel employee application, such as Siebel Call Center.

- Parameters you set at the Enterprise level configure all Siebel Servers throughout the enterprise.
- Parameters you set at the Siebel Server level configure all applicable components on a specific Siebel Server.
- Parameters you set at the component level configure all the tasks, or instances, of a specific component.
- Parameters you set for an enterprise profile (named subsystem) configure the applicable security adapter.

For purposes of authentication, most of the components of interest are AOMs, such as the Call Center Application Object Manager or the eService Application Object Manager. The Synchronization Manager component also supports authentication.

A particular parameter set at a lower level overrides the same parameter set at a higher level. For example, if Security Adapter Mode is set to LDAP at the Enterprise level, and Security Adapter Mode is set to ADSI at the component level for the eService Application Object Manager component, then the ADSI security adapter is used for Siebel eService.

Parameters configured for Siebel security adapters are configured for the enterprise profile (for GUI Server Manager) or named subsystem (for command-line Server Manager). For more information about configuring security adapters, see Chapter 6, "Security Adapter Authentication."

NOTE: You can set parameters on the Siebel Gateway Name Server using Siebel Server Manager or you can do so using the Siebel Configuration Wizard. For information on editing Gateway Name Server parameters using the Siebel Configuration Wizard, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 134. For information on using Siebel Server Manager to edit Gateway Name Server parameters, see *Siebel System Administration Guide*.

Parameters for Database Authentication

The following parameters are for database authentication, and are defined for named subsystems of type InfraSecAdpt_DB (that is, they might be set for the DBSecAdpt named subsystem or a similar security adapter with a nondefault name):

- **CRC (alias DBSecAdpt_CRC).** Use this parameter to implement checksum validation, in order to verify that each user gains access to the database through the correct security adapter. This parameter 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 parameter.

  For more information, see "Configuring Checksum Validation" on page 165.

- **DataSource Name (alias DataSourceName).** Specifies the data source for which you are specifying password hashing parameters.

- **Propagate Change (alias DBSecAdpt_PropagateChange).** Set this parameter to TRUE to allow administration of the current user's password in the database through Siebel Business Applications.

  If this parameter is set to TRUE (the default setting):

  - Users can change their passwords from within Siebel Business Applications on the User Profile screen (navigate to Tools, User Preferences, and then User Profile) and the change is propagated to the database.
  - An administrator can change the password associated with his or her own login ID using the Administration - User screen in the Siebel Web Client, and the change is propagated to the database. The administrator cannot change other users' passwords from the Administration - User screen.

- **Security Adapter Dll Name (alias DBSecAdpt_SecAdptDllName).** Specifies the DLL that implements the security adapter API required for integration with Siebel Business Applications. The file extension does not have to be explicitly specified. For example, sscfsadb.dll implements the Siebel database security adapter in a Windows implementation, and libsscfsadb.so does so in a UNIX implementation. If the DLL name for the adapter is used in a UNIX implementation, it is converted internally to the actual filename DLL.

The following parameters are also for database authentication environments, and are defined for named subsystems of type InfraDataSource (that is, they might be set for the ServerDataSrc named subsystem or another data source). The named subsystem is specified as the value for the `DataSourceName` parameter for the database security adapter.

- **Hash User Password (alias DSHashUserPwd).** Specifies password hashing for user passwords. Uses the hashing algorithm specified using the DSHashAlgorithm parameter. For details, see "About Password Hashing" on page 157.
- **User Password Hash Algorithm (alias DSHashAlgorithm).** Specifies the password hashing algorithm to use, if DSHashUserPwd is TRUE. The default value, RSASHA1, provides hashing using the RSA SHA-1 algorithm. The value SIEBELHASH specifies the password hashing mechanism provided by the mangle algorithm from Siebel Business Applications (supported for existing customers only). For details, see "About Password Hashing" on page 157.

Parameters for LDAP or ADSI Authentication

The following parameters are for LDAP or ADSI authentication, and are defined for named subsystems of type InfraSecAdpt_LDAP (that is, they might be set for the named subsystems LDAPSecAdpt or ADSISecAdpt, or a similar security adapter with a nondefault name):

- **Application Password (alias ApplicationPassword).** Specifies 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 an ADSI directory, the password is stored using Active Directory user management tools; it is not stored in an attribute.

- **Application User (alias ApplicationUser).** Specifies the user name of a record in the directory with sufficient permissions to read any user's information and do any necessary administration.

  This user provides the initial binding of the LDAP or ADSI security adapter with the AOM when a user requests the login page, or else anonymous browsing of the directory is required. You must implement an application user.

  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.

- **Base DN (alias BaseDN).** Specifies the Base Distinguished Name, which 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"
  ```

  `where`

  - "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 Active Directory server might be

  ```
  BaseDN = "ou=people, DC=qatest, DC=siebel, DC=com"
  ```

  Domain Component (DC) entries are the nested domains that locate this server. Therefore, adjust the number of DC entries to represent your architecture. You cannot distribute the users of a single Siebel application in more than one base DN.

- **CRC (alias CRC).** Use this parameter to implement checksum validation, in order to verify that each user gains access to the database through the correct security adapter. This parameter 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 parameter.

  For more information, see "Configuring Checksum Validation" on page 165.

- **Credentials Attribute Type (alias CredentialsAttributeType).** Specifies the attribute type that stores a database account. For example, if CredentialsAttributeType is set to dbaccount, then when a user with user name 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* and password=*P*, where *U* and *P* are credentials for a database account. There can be any amount of white space between the two key-value pairs and no space within each pair. The keywords username and password 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.

- **Hash DB Cred (alias HashDBPwd).** Specifies password hashing for database credentials passwords. For details, see "About Password Hashing" on page 157.
- **Hash User Password (alias HashUserPwd).** Specifies password hashing for user passwords. Uses the hashing algorithm specified using the HashAlgorithm parameter. For details, see "Process of Configuring User and Credentials Password Hashing" on page 159.
- **Password Attribute Type (alias PasswordAttributeType).** Specifies the attribute type under which the user's login password is stored in the directory.

  The LDAP entry must be userPassword. However, if you use the LDAP security adapter to authenticate against Microsoft Active Directory, set the value of this parameter to either unicodePWD or userPassword, depending on the code page used by the directory server.

  Active Directory does not store the password in an attribute so this parameter is not used by the ADSI adapter. You must, however, specify a value for the Password Attribute Type parameter even if you are using the ADSI adapter. Specify a value of either userPassword or unicodePWD, depending on the code page used by the directory server. In general, specify a value of userPassword if an ASCII code page is used by the directory server, and specify a value of unicodePWD if a Unicode code page is used.
- **Password Expire Warn Days (ADSI only) (alias PasswordExpireWarnDays).** Specifies the number of days to display a warning message before a password expires.

  You can only specify a value for this parameter when using an ADSI directory. You can specify a value when the security adapter in use is the ADSI Security Adapter or the LDAP Security Adapter.
- **Port (alias Port).** Specifies the port on the server computer that is used to access the LDAP server. Typically, use 389, the default value, for standard transmission or use 636 for secure transmission.

  This parameter is used by the LDAP security adapter only. (For ADSI, you set the port at the directory level, so this parameter is not used with the ADSI security adapter.) You must, however, specify a value for the Port parameter even if you are using the ADSI adapter; specify either port 389 or 636.
- **Propagate Change (alias PropagateChange).** Set this parameter to TRUE to allow administration of the directory through Siebel Business Applications. When an administrator then adds a user or changes a password from within Siebel Business Applications, or a user changes a password or 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.

- **Roles Attribute Type (alias RolesAttributeType).** Specifies the attribute type for roles stored in the directory. For example, if RolesAttributeType is set to Roles, then when a user with user name 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.

  For details, see "Configuring Roles Defined in the Directory" on page 172.

- **Security Adapter Dll Name (alias SecAdptDllName).** Specifies the DLL that implements the security adapter API required for integration with Siebel Business Applications. The file extension does not have to be explicitly specified. For example, sscfldap.dll implements the LDAP security adapter in a Windows implementation. On supported UNIX operating systems, the file name can be libsscfldap.so or libsscfldap.sl. If the DLL name for the LDAP security adapter is used in a UNIX implementation, it is converted internally to the actual filename.

- **Server Name (alias ServerName).** Specifies the name of the computer on which the LDAP or ADSI server runs, for example ldapserver.siebel.com.

  You must specify the fully qualified domain name of the LDAP server, not just the domain name. For example, specify ldapserver.oracle.com, not oracle.com.

  For ADSI, if SSL is configured between the Siebel Server computer and the Active Directory server computer, you must specify the fully qualified domain name of the Active Directory server. If the Siebel Server and Active Directory server are in the same domain, you can specify the Active Directory server's complete computer name or its IP address.

- **Shared Credentials DN (alias SharedCredentialsDN).** Specifies the absolute path (not relative to the BaseDN) of an object in the directory that has the shared database account for the application. If it is empty, the database account is looked up in the user's DN as usual. If it is 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 the value of CredentialsAttributeType.

  For example, if SharedCredentialsDN is set as follows:

  ```
  "uid=HKIM, ou=people, o=oracle.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.

- **Shared DB Password (alias SharedDBPassword).** Specify the password to connect to the Siebel database. Specify a value for this parameter if you store the password as a parameter rather than as an attribute of the directory entry for the shared database account. To use this parameter, you must use an LDAP directory. For more information, see "Configuring the Shared Database Account" on page 167.

- **Shared DB Username (alias SharedDBUsername).** Specify the username to connect to the Siebel database. You must specify a valid Siebel user name and password for the SharedDBUsername and SharedDBPassword parameters. Specify a value for this parameter if you store the username as a parameter rather than as an attribute of the directory entry for the shared database account. To use this parameter, you must use an LDAP directory. For more information, see "Configuring the Shared Database Account" on page 167.

- **Siebel Username Attribute Type (alias SiebelUsernameAttributeType).** If the UseAdapterUsername parameter is set to 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 user name passed in is assumed to be the Siebel user ID.
- **Single Sign On (alias SingleSignOn).** (TRUE or FALSE) If TRUE, the security adapter is used in Web SSO mode, instead of using security adapter authentication.
- **SSL Database (alias SslDatabase).** Specifies whether a Secure Sockets Layer (SSL) is used for communication between the LDAP security adapter and the directory. If empty, SSL is not used. If not empty, its value must be the absolute path of the file ldapkey.kdb. This file, which is generated by IBM GSK iKeyMan, contains a certificate for the certificate authority that is used by the LDAP server.
- **Trust Token (alias TrustToken).** 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 AOM accepts that the request has come from the SWSE, that is, from a trusted Web server. This parameter's default value is an empty string.
- **Use Adapter Defined Username (alias UseAdapterUsername).** (TRUE or FALSE) 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 UseAdapterUsername is FALSE.
- **User Password Hash Algorithm (alias HashAlgorithm).** Specifies the password hashing algorithm to use, if HashUserPwd is TRUE or HashDBPwd is TRUE. The default value, RSASHA1, provides hashing using the RSA SHA-1 algorithm. The value SIEBELHASH specifies the password hashing mechanism provided by the mangle algorithm from Siebel Business Applications (supported for existing customers only). For details, see "About Password Hashing" on page 157.
- **Username Attribute Type (alias UsernameAttributeType).** Specifies the attribute type under which the user's login name is stored in the directory. For example, if UsernameAttributeType is set to uid, then when a user attempts to log in with user name 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 is set to TRUE), then you must set the OM - Username BC Field 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 "Configuring Adapter-Defined User Name" on page 169.

Parameters for Custom Security Adapter Authentication

The following parameters are for custom security adapter authentication *only*, and are defined for the named subsystem InfraSecAdpt_Custom:

- **Config File Name (alias ConfigFileName).** Specifies the file name that contains custom security adapter configuration parameters. These settings would be other than those defined in this section.

- **Config Section Name (alias ConfigSectionName).** Specifies the name of the section, in the file specified using the ConfigFileName parameter, that contains custom security adapter configuration settings.

The following parameters are for custom security adapter authentication, and are defined for the named subsystem InfraSecAdpt_Custom. For more information about these parameters, see the descriptions for similar parameters applicable to LDAP or ADSI security adapters, in "Siebel Gateway Name Server Parameters" on page 341.

- CRC (alias CustomSecAdpt_CRC)
- Hash DB Cred (alias CustomSecAdpt_HashDBPwd)
- Hash User Password (alias CustomSecAdpt_HashUserPwd)
- Propagate Change (alias CustomSecAdpt_PropagateChange)
- Security Adapter Dll Name (alias CustomSecAdpt_SecAdptDllName)
- Single Sign On (alias CustomSecAdpt_SingleSignOn)
- Trust Token (alias CustomSecAdpt_TrustToken)
- Use Adapter Defined Username (alias CustomSecAdpt_UseAdapterUsername)
- User Password Hash Algorithm (alias CustomSecAdpt_HashAlgorithm)

Parameters for AOM

The following parameters are defined for the Enterprise, Siebel Server, or AOM component:

- **AllowAnonUsers.** (TRUE or FALSE) Unregistered users are not allowed access to the Siebel application if this parameter value is FALSE.
- **DisableReverseProxy.** If you deploy IBM Tivoli Access Manager WebSEAL to authenticate users of Siebel Business Applications with high interactivity in a Web Single Sign-On deployment, set DisableReverseProxy to TRUE to disable reverse proxy support. You must disable implicit reverse proxy support as IBM Tivoli Access Manager WebSEAL acts as a reverse proxy server. The default value for DisableReverseProxy is FALSE.
- **SecureLogin.** (TRUE or FALSE) If TRUE, the login form completed by the user is transmitted over Secure Sockets 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.** When SecureBrowse is set to TRUE, all views in the application are navigated over SSL. When SecureBrowse is set to FALSE, views in the application whose Secure attribute is set to TRUE are navigated over SSL.

  NOTE: Siebel customer applications support switching between secure and nonsecure views but employee applications (such as Siebel Call Center) do not. For more information, see "Configuring a Siebel Web Client to Use SSL" on page 199.

  For information about the Secure attribute for a view, see *Configuring Siebel Business Applications*.
- **OM - Proxy Employee (alias ProxyEmployee).** User ID of the proxy employee. For information about the proxy employee, see "Seed Data" on page 353.

- **OM - Username BC Field (alias UsernameBCField).** This parameter is used only if you implement an adapter-defined user name. 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.

  For information, see "Configuring Adapter-Defined User Name" on page 169.

Siebel Application Configuration File Parameters

A configuration file exists for each Siebel application for each language. The parameters in the file determine how the user interacts with the AOM 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 Siebel Web Client, application configuration files are located in the *SIEBSRVR_ROOT*\bin\LANGUAGE subdirectory. For example, eservice.cfg is provided for Siebel eService, for implementation in U.S. English, in the *SIEBSRVR_ROOT*\bin\ENU directory.

  Most of the security-related parameters applicable to Siebel Servers (and, consequently, Siebel Web Clients) are stored in the Siebel Gateway Name Server, not in the application configuration file.

- **Configuration file on the Siebel Mobile Web Client or Developer Web Client.** For users connecting through the Siebel Mobile Web Client or Developer Web Client, the configuration file is located in the *SIEBEL_CLIENT_ROOT*\bin\LANGUAGE subdirectory on the client. For example, eservice.cfg is provided for Siebel eService, for implementation in U.S. English, in the *SIEBEL_CLIENT_ROOT*\bin\ENU directory.

  - The Siebel Mobile Web Client connects directly to the local database; it bypasses the Siebel Server.

  - The Siebel Developer Web Client connects directly to the server database; it bypasses the Siebel Server.

For more information about working with configuration files, see *Siebel System Administration Guide*.

In a given configuration file, some parameters might not appear by default. Others might 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 or Siebel client.

NOTE: The parameter values that reference directory attributes that you provide for the Siebel LDAP and ADSI security 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.

Parameters in [InfraUIFramework] Section

The following parameters apply to Siebel Mobile Web Clients and Siebel Developer Web Clients. For a description of the equivalent parameters applicable to Siebel Web Clients, see "Siebel Gateway Name Server Parameters" on page 341.

- **DisableReverseProxy.** If you deploy IBM Tivoli Access Manager WebSEAL to authenticate users of Siebel Business Applications with high interactivity in a Web Single Sign-On deployment, set DisableReverseProxy to TRUE to disable reverse proxy support. You must disable implicit reverse proxy support as IBM Tivoli Access Manager WebSEAL acts as a reverse proxy server. The default value for DisableReverseProxy is FALSE.
- **SecureLogin.** (TRUE or FALSE) If TRUE, the login form completed by the user is transmitted over Secure Sockets 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.** When SecureBrowse is set to TRUE, all views in the application are navigated over SSL. When SecureBrowse is set to FALSE, views in the application whose Secure attribute is set to TRUE are navigated over SSL.

  NOTE: Siebel customer applications support switching between secure and nonsecure views, but employee applications (such as Siebel Call Center) do not. For more information, see "Configuring a Siebel Web Client to Use SSL" on page 199.

  For information about the Secure attribute for a view, see *Configuring Siebel Business Applications*.

Parameters in [InfraSecMgr] Section

The following parameters are located in the [InfraSecMgr] section of the application configuration file. These parameters apply to Siebel Mobile Web Client and Developer Web Clients.

- **SecAdptMode.** Specifies the security adapter mode.
  - For database authentication, specify `DB`. (DB is the default value for SecAdptMode.)
  - For LDAP authentication, specify `LDAP`.
  - For ADSI authentication, specify `ADSI`.
  - For a custom security adapter, specify `CUSTOM`.
- **SecAdptName.** Specifies the name of the security adapter.
  - For database authentication, specify `DBSecAdpt`. For Mobile or Developer Web Client configuration, the section [DBSecAdpt] is created in the configuration file. (`DBSecAdpt` is the default value for SecAdptName.)

  - For LDAP authentication, specify LDAPSecAdpt (or another name of your choice). For Developer Web Client configuration, the section [LDAPSecAdpt] is created by default in the configuration file if you configure LDAP using the Siebel Configuration Wizard.
  - For ADSI authentication, specify ADSISecAdpt (or another name of your choice). For Developer Web Client configuration, the section [ADSISecAdpt] is created by default in the configuration file if you configure ADSI using the Siebel Configuration Wizard.
  - For a custom security adapter, specify a name such as SecAdpt_Custom. You must add the applicable section to the file yourself. For example, [SecAdpt_Custom].

- **UseRemoteConfig.** This parameter applies *only* to the Siebel Developer Web Client. It specifies 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 [LDAPSecAdpt] in an application's configuration file.

  You must provide the path in universal naming convention (UNC) format—that is, for example, in a form like server\vol\path\ldap_remote.cfg. For detailed information about using this parameter, see "Security Adapters and the Siebel Developer Web Client" on page 173.

If you implement a custom, 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.

Parameters in [DBSecAdpt] Section

The following parameters are located in the [DBSecAdpt] section (or equivalent) of the application configuration file, if you are configuring the database security adapter. Each authentication-related parameter in an application's configuration file is interpreted by the security adapter for database authentication.

These parameters apply to Siebel Mobile Web Client and Developer Web Client only. For more information, see the descriptions for equivalent parameters applicable to Siebel Web Client and other authentication contexts, in "Siebel Gateway Name Server Parameters" on page 341.

- **DBSecAdpt_CRC.** Use this parameter to implement checksum validation, in order to verify that each user gains access to the database through the correct security adapter. This parameter 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 parameter.

  For more information, see "Configuring Checksum Validation" on page 165.

- **DBSecAdpt_PropagateChange.** Set this parameter to TRUE to allow administration of credentials in the database through Siebel Business Applications. When an administrator then adds a user or changes a password from within Siebel Business Applications, or a user changes a password or self-registers, the change is propagated to the database.

  For Siebel Developer Web Client, the system preference SecThickClientExtAuthent. must also be set to TRUE. For details, see "Setting a System Preference for Developer Web Clients" on page 153

- **DBSecAdpt_SecAdptDllName.** Specifies the DLL that implements the security adapter API required for integration with Siebel Business Applications. The file extension does not have to be explicitly specified. For example, sscfsadb.dll implements the database security adapter in a Windows implementation.

- **DataSourceName.** Specifies the data source applicable to the specified database security adapter.

Parameters in the Data Source Section

The following parameters are located in the data source section of the application configuration file, such as [ServerDataSrc] (for Siebel Developer Web Client) or [Local] (for Siebel Mobile Web Client).

- **DSHashAlgorithm.** Specifies the password hashing algorithm to use, if DSHashUserPwd is TRUE. The default value, RSASHA1, provides hashing using the RSA SHA-1 algorithm. The value SIEBELHASH specifies the password hashing mechanism provided by the mangle algorithm from Siebel Business Applications (supported for existing customers only). For details, see "About Password Hashing" on page 157.
- **DSHashUserPwd.** Specifies password hashing for user passwords. Uses the hashing algorithm specified using the DSHashAlgorithm parameter. For details, see "Process of Configuring User and Credentials Password Hashing" on page 159.
- **IntegratedSecurity.** Applicable only to Siebel Developer Web Client, with Oracle or Microsoft SQL Server database. For details, see "Security Adapters and the Siebel Developer Web Client" on page 173.

Parameters in [LDAPSecAdpt] or [ADSISecAdpt] Section

The following parameters are located in the [LDAPSecAdpt] or [ADSISecAdpt] section (or equivalent) of the application configuration file, according to whether you are configuring the LDAP security adapter or the ADSI security adapter. Each authentication-related parameter in an application's configuration file is interpreted by the security adapter (for LDAP or ADSI authentication).

Some parameters apply only to LDAP implementations, or only to ADSI implementations. Some parameters apply only in a Web SSO authentication environment.

For more information, see the descriptions for equivalent parameters applicable to Siebel Web Client and other authentication contexts in "Siebel Gateway Name Server Parameters" on page 341.

- ApplicationPassword
- ApplicationUser
- BaseDN
- CRC
- CredentialsAttributeType
- HashAlgorithm
- HashDBPwd
- HashUserPwd
- PasswordAttributeType
- PasswordExpireWarnDays
- Port
- PropagateChange
- RolesAttributeType
- SecAdptDllName
- ServerName
- SharedCredentialsDN
- SiebelUsernameAttributeType
- SingleSignOn
- SslDatabase
- TrustToken
- UseAdapterUsername
- UsernameAttributeType

The parameter, EncryptApplicationPassword, can be set in the [LDAPSecAdpt] or [ADSISecAdpt] sections of an application configuration file only; it is not a Siebel Gateway Name Server parameter. Set EncryptApplicationPassword to TRUE if you want to store the encrypted value of the ApplicationPassword parameter in the application configuration file. Use the encryptstring utility to generate the encrypted value of the ApplicationPassword parameter. For information on using the encryptstring utility, see "Encrypting Passwords Using the encryptstring Utility" on page 46.

C Seed Data

This appendix describes seed data provided for your Siebel Business Applications that is relevant to the content of this guide, and provides information about how to use this data. It includes the following topics:

NOTE: In the tables in this appendix, the term *customer applications* represents the group of Siebel Sales, Siebel eService, Siebel Customer, Siebel Training, Siebel Events, and Siebel Marketing.

Seed Employee

One Employee record is provided as seed data at installation, as described in Table 31 on page 353. 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 Siebel Gateway Name Server parameter.

For information about associating the proxy employee with an application, see "Siebel Gateway Name Server Parameters" on page 341. For information about organization access control, see "Access Control Mechanisms" on page 256.

Table 31. Proxy Employee Seed Data Field Values

Last Name	First Name	User ID	Responsibility	Position	Organization
Employee	Proxy	PROXYE	None	Proxy Employee	Default Organization

Seed Users

Table 32 on page 354 describes nonemployee User records provided as seed data.

Table 32. 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	Self-registered Partner Agent	Siebel Partner Portal

Seed Responsibilities

Responsibility records are provided as seed data, as described in Table 33 on page 354. 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.

For all responsibilities provided in seed data, see those listed in the Siebel application.

Table 33. 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

Table 33. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
MgmtSrvr-Admin	Default Organization	Views for a user of the Siebel Management Framework. Assign this responsibility to Siebel users who require access to the Siebel Management Server.	Siebel Management Framework
MgmtSrvr-Deploy&Execute	Default Organization	Views for a user of the Siebel Management Framework. Assign this responsibility to Siebel users who require access to ADM functionality.	Siebel Management Framework
MgmtSrvr-Monitor	Default Organization	Views for a user of the Siebel Management Framework. Assign this responsibility to Siebel users who require access to the Siebel Management Server, Siebel Management Agent(s), or the Siebel Diagnostic Tool.	Siebel Management Framework
Unregistered Partner Agent	Default Organization	Views provided for anonymous browsing	Siebel Partner Portal
Self-Registered Partner Agent	Default Organization	Limited set of views provided for a user who self-registers	Siebel Partner Portal
Partner Relationship Manager	Default Organization	Views for Siebel Partner Portal partner relationship manager	Siebel Partner Portal
Partner Operations Manager	Default Organization	Views for Siebel Partner Portal partner operations manager, including views for administering users	Siebel Partner Portal
Partner Sales Manager	Default Organization	Views for Siebel Partner Portal partner sales manager	Siebel Partner Portal
Partner Sales Rep	Default Organization	Views for Siebel Partner Portal partner sales rep	Siebel Partner Portal
Partner Service Manager	Default Organization	Views for Siebel Partner Portal partner service manager	Siebel Partner Portal
Partner Service Rep	Default Organization	Views for Siebel Partner Portal partner service rep	Siebel Partner Portal
Registered Customer - Wireless	Default Organization	Views provided for a registered eService user on a wireless device	eService

Table 33. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
Web Training Manager	Default Organization	Views that allow an administrator to see his or her direct reports' course and curriculum enrollment information	Training
Training Administrator	Default Organization	Views that allow administration of courses and enrollees	Training

The following procedure describes how to list the views associated with a responsibility.

To see the views included in a responsibility

1. Navigate to the Administration - Application screen, then the Responsibilities view.
2. 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 must not be assigned to any individual user. The login credentials are:

- Login: LDAPUSER
- Password: LDAPUSER

NOTE: It is recommended that an administrator change the password. For more information, see Chapter 3, "Changing or Adding Passwords."

D Addendum for Siebel Financial Services

This appendix outlines the differences in the implementation of user authentication, user administration, and basic access control in Siebel Financial Services applications and the implementation that is documented in other sections of this book. It includes the following topics:

- Siebel Financial Services Applications on page 357
- User Authentication for Siebel Financial Services on page 359
- User Registration and Administration for Siebel Financial Services on page 361
- Basic Access Control for Siebel Financial Services on page 364
- Configuration File Names for Siebel Financial Services Applications on page 366
- Seed Data for Siebel Financial Services on page 367

Siebel Financial Services Applications

The applications listed in Table 34 on page 358 are specific to Siebel Financial Services applications or are applications that have functionality that is adapted for Siebel Financial Services. The applications are listed as they are named in Siebel Tools.

For some applications, options are listed that, along with functionality modules, determine the screens and views that are licensed to you. A given application can be referred to by one or more product names, as listed in the Products column. Information is categorized for employee, partner, and customer applications.

Table 34. Siebel Financial Services Applications

Tools Application Object Name	Users	Options	Products
Siebel Financial Services	Employees	Siebel Sales Siebel eService Siebel Call Center Siebel Partner Manager	Siebel Finance Siebel Insurance Siebel Healthcare
Siebel Financial Services ERM	Employees	Not applicable	Siebel Employee Relationship Management
Siebel Financial Services Marketing	Employees	Siebel Marketing only	Siebel Finance Siebel Insurance Siebel Healthcare
Siebel Financial Partner Relationship Management (PRM)	Partners	Not applicable	Siebel PRM for Finance Siebel Agent Portal Siebel Healthcare Group Portal Siebel Healthcare Provider Portal
Siebel eBanking	Customers	Not applicable	Siebel eBanking
Siebel Financial eBrokerage	Customers	Not applicable	Siebel eBrokerage
Siebel Financial eService	Customers	Not applicable	Siebel Insurance/ Healthcare eService Siebel Healthcare Member Portal
Siebel Financial eEnrollment	Customers	Not applicable	Siebel Healthcare Enrollment Portal
Siebel FINS eSales	Customers	Not applicable	Siebel Sales
Siebel Financial eCustomer	Customers	Not applicable	Siebel Customer
Siebel eEvents Management	Customers	Not applicable	Siebel Events Manager for Finance

NOTE: Siebel Healthcare Group Portal is used as a customer product; that is, users are typically your customers. Technically, Siebel Healthcare Group Portal is a product label for the Siebel Financial partner application. You provide users with their own positions and organizations, unlike users of customer applications.

User Authentication for Siebel Financial Services

This topic contains information for Siebel Financial Services applications that differs from information in other sections of this guide, or that otherwise warrants mention.

LDAP and ADSI Security Adapter Authentication

Security adapter authentication is a prerequisite if you want to implement self-registration or external administration of users. However, not all Siebel Business Applications provide self-registration and external administration of users as default functionalities.

For information about the applications in this group that provide self-registration and external administration of users as default functionalities, see "User Registration and Administration for Siebel Financial Services" on page 361.

About Implementing LDAP and ADSI Security Adapter Authentication

Implementation of LDAP or ADSI security adapter authentication is the same for Siebel Financial Services applications as described in other sections of this guide, with the following exceptions.

Parameters for Siebel Financial Services applications are listed primarily in the eapps_fins.cfg file. The eapps.cfg file is also included, as documented in other sections of this guide. The eapps.cfg file has an include line that points to the eapps_fins.cfg file. Consider references throughout this topic to the eapps.cfg file to be references to the eapps.cfg file and the eapps_fins.cfg file.

About Setting Up Security Adapter Authentication

The Responsibility and New Responsibility that are assigned to the seed anonymous user GUESTCST are intended for use with Siebel Financial Services customer applications. These responsibilities differ from the responsibilities assigned to GUESTCST for Siebel customer applications that are not specific to financial services, as documented in other sections of this guide.

If you deploy either Siebel Events Manager for Finance or Siebel customer applications that are not specific to financial services concurrently with any other Siebel Financial Services customer applications, then you must create a separate anonymous user.

The new anonymous user is used for Siebel Events Manager for Finance and for the Siebel customer applications that are not specific to financial services; that is, the applications documented in other sections of this guide. Assign this anonymous user the responsibilities listed for the GUESTCST user in "Seed Users" on page 354.

When you add TESTUSER to the database, enter the Responsibility and New Responsibility fields with an appropriate responsibility for a typical registered user for the application you are setting up. For information about the seed responsibilities provided for specific applications, see "Seed Data for Siebel Financial Services" on page 367 and "Seed Data" on page 353.

About Implementing Web SSO Authentication

Implementation of Web SSO authentication is the same for Siebel Financial Services applications as described in other sections of this guide with the following exceptions.

Parameters for Siebel Financial Services applications are listed primarily in the eapps_fins.cfg file. The eapps.cfg file is also included, as documented in other sections of this guide. The eapps.cfg file has an include line that points to the eapps_fins.cfg file. Consider references throughout this topic to the eapps.cfg file to refer to the eapps.cfg file and the eapps_fins.cfg file.

Setting Up Web SSO

The Responsibility and New Responsibility that are assigned to the seed anonymous user GUESTCST are intended for use with Siebel Financial Services customer applications. These responsibilities differ from the responsibilities assigned to GUESTCST for Siebel customer applications that are not specific to financial services, as documented in other sections of this guide.

If you deploy either Siebel Events Manager for Finance or Siebel customer applications that are not specific to financial services concurrently with any other Siebel Financial Services customer applications, then you must create a separate anonymous user.

The new anonymous user is used for Siebel Events Manager for Finance and for the Siebel customer applications that are not specific to financial services; that is, the applications documented in other sections of this guide. Assign this anonymous user the responsibilities listed for the GUESTCST user in "Seed Users" on page 354.

When you add TESTUSER to the database, enter the Responsibility and New Responsibility fields with an appropriate responsibility for a typical registered user for the application you are setting up. For information about the seed responsibilities provided for specific applications, see "Seed Data for Siebel Financial Services" on page 367 and "Seed Data" on page 353.

Parameters in the eapps.cfg and eapps_fins.cfg Files

In addition to the eapps.cfg file, the Siebel Web Engine also uses the eapps_fins.cfg file to control interactions between Siebel Financial Services applications and the Siebel Web Engine. The topic defining the Application Object Manager (AOM) and authentication parameters for an application appears once, in either the eapps.cfg file or in the eapps_fins.cfg file.

Table 35 on page 361 lists the sections in the eapps.cfg file and in the eapps_fins.cfg file, which are provided for Siebel Financial Services applications.

Table 35. Sections in eapps.cfg and eapps_fins.cfg Files

Tools Application Object Name	Section in eapps.cfg	Section in eapps_fins.cfg
Siebel Financial Services	None	[/fins]
Siebel Financial Services ERM	None	[/finserm]
Siebel Marketing	[/marketing]	None
Siebel Financial PRM	None	[/finsechannel]
Siebel eBanking	None	[/finsebanking]
Siebel Financial eBrokerage	None	[/finsebrokerage]
Siebel Financial eService	None	[/finseservice]
Siebel Financial eEnrollment	None	[/finseenrollment]
Siebel FINS eSales	None	[/finsesales]
Siebel Financial eCustomer	None	[/finsecustomer]
Siebel eEvents for Finance	[/eevents]	None

Siebel Application Configuration File Parameters

For names of application configuration files for specific applications, see "Configuration File Names for Siebel Financial Services Applications" on page 366.

User Registration and Administration for Siebel Financial Services

This topic contains information for Siebel Financial Services applications that differs from the information in the topic on registering and administering users in other sections of this guide, or that otherwise warrants mention.

Seed Data

The Responsibility and New Responsibility that are assigned to the seed user GUESTCST are intended for use with Siebel Financial Services customer applications. These responsibilities differ from the responsibilities assigned to GUESTCST for Siebel customer applications that are not specific to financial services, as documented in other sections of this guide.

If you deploy either Siebel Events Manager for Finance or Siebel customer applications that are not specific to financial services concurrently with any other Siebel Financial Services customer applications, then you must create a separate anonymous user. The new anonymous user is used for Siebel Events Manager for Finance and for the Siebel customer applications that are not specific to financial services; that is, the applications documented in other sections of this guide. Assign this anonymous user the responsibilities listed for the GUESTCST user in "Seed Users" on page 354. For information about seed data specific to Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 367.

Unregistered Users and Anonymous Browsing

Anonymous browsing is default functionality for the following Siebel Financial Services applications:

- Siebel Employee Relationship Management
- Siebel Events Manager for Finance
- Siebel Finance PRM
- Siebel eBanking
- Siebel eBrokerage
- Siebel Finance eSales
- Siebel Healthcare Enrollment Portal

In addition to the GUESTCST and GUESTCP seed user records provided as anonymous users, a seed user record with user ID GUESTERM is provided as the anonymous user for Siebel Financial Services ERM.

For information about seed data specific to Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 367.

Self-Registration

User self-registration is default functionality for the Siebel Financial Services applications listed in this topic.

NOTE: Although self-registration is provided as default functionality for some Siebel Financial Services applications, it is not common in the industry for users to self-register for financial services. More commonly, internal administrators register users by using the Siebel Financial Services application.

- Siebel Finance PRM
- Siebel Events Manager for Finance
- Siebel eBanking
- Siebel eBrokerage
- Siebel Finance eSales

A user can self-register in Siebel Finance PRM as a company or as an individual. By self-registering, the user requests to become a partner and becomes a prospective partner.

An internal administrator uses the Administration - Partner screen in Siebel Finance to promote a prospective partner to approved partner and then to registered partner.

For information about using the Administration - Partner screen, see *Siebel Partner Relationship Management Administration Guide*.

Internal Administration of Users

Internal administration of users is the same for Siebel Financial Services applications as described in other sections of this guide, with the following exception.

You can administer partner users in the Administration - Partner screen in Siebel Financial Services. For information about using the Administration - Partner screen, see *Siebel Partner Relationship Management Administration Guide*.

External Administration of Users

Delegated administration is default functionality of Siebel Financial PRM. Although delegated administration is provided as default functionality of Siebel Financial PRM, it is not common in the finance industry for external administrators to register customer or partner users. More commonly, internal administrators register users by using the Siebel Financial Services application.

Access Considerations

Seed responsibilities that provide user administration views for delegated administrators are described in "Seed Data" on page 353. The seed responsibilities for delegated administrators do not include views specific to Siebel Financial Services applications. For a delegated administrator to access appropriate financial services views and user administration views, the delegated administrator must be assigned responsibilities in one of the following ways:

- Assign at least two seed responsibilities to the delegated administrator—one for a regular user of the Siebel application, and the appropriate responsibility for delegated administrators of the application.
- Create a single responsibility that includes all the views you want delegated administrators to have, then assign the responsibility to the delegated administrators.

For information about assigning responsibilities to users, see the topics on internal administration of users and external administration of users in other sections of this guide.

Maintaining a User Profile

Maintaining a user profile is the same for Siebel Financial Services applications as described in other sections of this guide, with the exception of editing personal information.

Depending on the Siebel customer application, the user can click My Profile or My Accounts to access the User Profile form.

Basic Access Control for Siebel Financial Services

Basic access control for Siebel Financial Services applications is implemented as described other sections of this guide, with the following exceptions.

Access Control Mechanisms

The following information affects access control to Opportunities in any view that uses personal, position, or organization access control.

If an opportunity's Secure field is checked, then only positions on the sales team have visibility of the opportunity in any view that applies person, position, or organization access control. For example, in the All Opportunities view, users on the sales team can see a secure opportunity, but other users in the same organization cannot. In the My Team's Opportunities view, a manager cannot see a secure opportunity on which a direct report is a primary unless the manager is also on the sales team. Any activities or events related to a secure opportunity are also hidden from any user who is not on the sales team.

Secure opportunity access control is provided by the following search specification on the Opportunity business component:

```
[Secure Flag] = 'N' OR EXISTS([Sales Rep Id] = LoginId())
```

Access-Group Access Control

Households can also be used in combination with other party types to form an access group. In all access control contexts, households must be included in lists of the party types that can be members of access groups.

Administration of Access-Group Access Control

The procedures for associating an access group with a catalog or category differ from the documentation in other sections of this guide.

Associating an Access Group with a Catalog

The following procedure describes how to associate an access group with a catalog for Siebel Financial Services. 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. Navigate to the Administration - Catalog screen, then the Catalogs view.
2. Select a catalog from the Catalogs list.
3. Click the Access Groups view tab.

   The Access Groups list appears, which shows the access groups associated with this catalog.

4. In the Access Groups list, add a new record.

   A pop-up list appears that contains access groups.

5. Select an access group, and then click Add.

   The access group appears in the Access Groups list.

6. Complete the following fields for the access group you add, using the guidelines provided in the following table, and then step off of the access group record to save the record.

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 descendant categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendant categories.

You can disassociate an access group from a catalog similarly.

Associating an Access Group with a Category

The following procedure describes how to associate an access group with a category for Siebel Financial Services. 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. Navigate to the Administration - Catalog screen, then the Catalogs view.
2. Drill down on a catalog name in the Catalogs list.

   The Categories list for the catalog appears.

3. Click the Access Groups view 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. Complete the following fields for the access group you add, using the guidelines provided, and then step off of the access group record to save the record.

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 descendant categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendant categories.

You can disassociate an access group from a category similarly. When an access group is disassociated from a category, it is automatically disassociated from all of the category’s descendant categories.

Configuration File Names for Siebel Financial Services Applications

This topic contains information for Siebel Financial Services applications that differs from the information relating to Siebel application configuration file names in other topics in this guide, or that otherwise warrants mention.

Table 36 on page 366 contains the names of application configuration files that are used by Siebel Financial Services applications.

Table 36. Siebel Financial Services Application Configuration File Names

Tools Application Object Name	Configuration File Name
Siebel Financial Services	fins.cfg
Siebel Financial Services ERM	finserm.cfg
Siebel Financial Services Marketing	finsmarket.cfg
Siebel Financial PRM	finscw.cfg
Siebel eBanking	finsebanking.cfg
Siebel Financial eBrokerage	finsebrokerage.cfg
Siebel Financial eService	finseservice.cfg
Siebel Financial eEnrollment	finseenrollment.cfg
Siebel FINS eSales	finsesales.cfg

Table 36. Siebel Financial Services Application Configuration File Names

Tools Application Object Name	Configuration File Name
Siebel Financial eCustomer	finsecustomer.cfg
Siebel eEvents Management	eevents.cfg

Seed Data for Siebel Financial Services

This topic contains information for Siebel Financial Services applications that differs from the information in "Seed Data" on page 353 or that otherwise warrants mention.

The seed data related to user access is also provided with Siebel Financial Services applications.

In this topic, the term "Siebel Financial Services customer applications" represents the group denoted as customer applications in Table 34 on page 358.

Seed Users

Table 37 on page 367 shows modifications to the seed nonemployee User records that are provided with Siebel Financial Services applications.

The GUESTCP seed user record, which is documented in "Seed Data" on page 353, functions as the anonymous user for Siebel Financial PRM, the partner application in Siebel Financial Services. The responsibility assocuated with the GUESTCP seed user record provides views for anonymous browsing, and the responsibility in its New Responsibility field provides views for users who self-register.

Table 37. User Seed Data Field Values

Last Name	First Name	User ID	Responsibility	New Responsibility	Used by These Applications
Customer	Guest	GUESTCST	Unregistered Customer	Registered Customer	Siebel Financial Services customer applications
Guest	ERM	GUESTERM	ERM AnonUser	None	Siebel Financial Services ERM

Seed Responsibilities

Table 38 on page 368 lists additional seed responsibilities that are provided with Siebel Financial Services applications. Although the seed responsibilities are also included with Siebel Financial Services applications, those responsibilities do not include views specific to Siebel Financial Services applications.

No additional seed responsibilities are provided for registered partner users of Siebel Financial PRM. You must build responsibilities for registered partner users based on their various business roles. You can create new responsibilities, or you can copy and modify seed responsibilities for partner users.

Table 38. Seed Responsibilities

Name	Organization	Description and Comments	Used by These Applications
Unregistered Customer	Default Organization	Views provided for anonymous browsing.	Siebel Financial Services customer applications, except Siebel Events Manager for Finance. For Siebel Events Manager for Finance, use Web Anonymous User instead.
Registered Customer		Views for a typical registered user. Associate Default Organization with this responsibility before assigning this responsibility to a user.	Siebel Financial Services customer applications, except Siebel Events Manager for Finance. For Siebel Events Manager for Finance, use Web Registered User instead.
ERM AnonUser	Default Organization	Views provided for anonymous browsing.	Siebel Financial Services ERM.
ERM User	Default Organization	Views for a typical registered user.	Siebel Financial Services ERM.
ERM Manager	Default Organization	Views for employee management. Assign this responsibility to a manager in addition to a responsibility that contains views for a regular user.	Oracle's Siebel Financial Services ERM.

For information about creating and modifying responsibilities, see Chapter 10, "Configuring Access Control."

Index