Security Guide for Siebel eBusiness Applications

Version 7.7, Rev. A
May 2005

Siebel Systems, Inc., 2207 Bridgepointe Parkway, San Mateo, CA 94404

Printed in the United States of America

Contents

Chapter 5: Communications and Data Encryption

Chapter 6: Security Adapter Authentication

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 Security Guide for Siebel eBusiness Applications, Version 7.7, Rev. A

Table 1 lists changes described in this version of the documentation to support release 7.7 of the software.

Table 1. New Product Features in Security Guide for Siebel eBusiness Applications, Version 7.7, Rev. A

Topic	Description
"Firewall and Proxy Server Support" on page 38	This topic describes how to deploy an application in a reverse proxy Web server configuration.
"Configuring Data Encryption" on page 60	This topic now describes how to upgrade data encrypted using the Standard Encryptor encryption (based on mangle algorithm) of previous releases to the RC2 encryption standard.

What's New in Security Guide for Siebel eBusiness Applications, Version 7.7

Table 2. New Product Features in Security Guide for Siebel eBusiness Applications, Version 7.7

Topic	Description
"Managing Encrypted Passwords in the eapps.cfg File" on page 34	Passwords stored in the eapps.cfg file are now encrypted. The encryptstring.exe utility can be used for manual encryption of such passwords.
"Firewall and Proxy Server Support" on page 38	Siebel high interactivity applications can now support reverse proxy Web server configurations.
"Role of Siebel Server Load Balancing in Networking Security" on page 41	Siebel Servers can load-balance Siebel Servers, using either Siebel load balancing or a third-party load balancer. See also the *Deployment Planning Guide*.
"Port Numbers" on page 41	Application Object Managers (AOMs) now use static ports.
"Configuring Secure Communications" on page 50	The SSL Configuration Utility (for SISNAPI) is now integrated with the Siebel Software Configuration Utility (for Enterprise or SWSE). It can also run as a stand-alone utility.
"Configuring Data Encryption" on page 60	The Siebel Strong Encryption Pack now includes AES data encryption at three levels: 128-bit, 192-bit, and 256-bit. Multiple upgrade scenarios are supported for higher levels of data encryption. The Key Database Manager utility now supports AES encryption. Business component field configuration now supports AES encryption through the AES Encryptor business service. The mangle algorithm has been removed from internal code references.
Chapter 6, "Security Adapter Authentication"	Parameters for security adapters have moved from configuration files to Siebel Gateway Name Server and are configured through Siebel Server Manager. (Configuration files are still used for Mobile and Dedicated Web Client.) Security adapters and authentication manager are no longer part of AOM; security adapters are defined as enterprise profiles (named subsystems). Database authentication now uses the security adapter framework (the database security adapter is the default). Some security-related configuration parameters and system preferences from previous releases are now obsolete.

Table 2. New Product Features in Security Guide for Siebel eBusiness Applications, Version 7.7

Topic	Description
"Installing LDAP Client Software" on page 82	Deploying any LDAP security adapter now requires installation of IBM LDAP client software provided by Siebel Systems.
"Using the LDAP/ADSI Configuration Utility" on page 103	The LDAP/ADSI Configuration Utility is enhanced.
"Configuring Password Hashing" on page 125	Password hashing (for users or credentials) is now configured and performed through the security adapter. The hashpwd.exe utility replaces encrypt.exe and provides support for the RSA SHA-1 hashing algorithm. Customers can migrate passwords to RSA SHA-1 algorithm. (The prior mangle algorithm is still available for existing customers.)
"Configuring the Application User" on page 131	The application user is no longer optional when using LDAP/ADSI security adapters.
"Authentication for Mobile Web Client Synchronization" on page 141	Mobile Web Client synchronization using Synchronization Manager can now optionally use security adapter authentication. The Database authentication option for Mobile Web Client now uses the database security adapter. See also *Siebel Remote and Replication Manager Administration Guide*.
Chapter 7, "Web Single Sign-On Authentication"	Microsoft Windows Integrated Authentication can now be deployed as a Web Single Sign-On (Web SSO) alternative.
"Cookies and Siebel Applications" on page 168	Configuration parameters in the eapps.cfg file for session tracking and cookie management are now modified.
"About Single- and Multiple-Organization Access Control" on page 225	Lists of Values can now be configured for multiple-organization visibility.
"Managing Tab Layouts Through Responsibilities" on page 268 "Managing Tasks Through Responsibilities" on page 271 "Clearing Cached Responsibilities" on page 272	Default tab layouts and tasks are now configured through responsibilities. (Tab layouts feature added in version 7.5.3.) Views can be specified to be read-only for responsibilities you associate them with. Administrators can clear cached responsibilities. Roles (Siebel application feature) are now obsolete. Capabilities for roles are now included in responsibilities.

Security-Related Changes for Version 7.7 Not Covered in This Book

The following security-related changes for Version 7.7 are not covered in the *Security Guide for Siebel eBusiness Applications*. They are described in other books on *Siebel Bookshelf*.

- **Local database password management and local database encryption.** Mobile users can now change their local database password independent of the password used for synchronization with Siebel Remote server. The local database password can now be hashed using the RSA SHA-1 algorithm.

  The local database for mobile users can now be encrypted using standard Sybase encryption for SQL Anywhere.

  For details, see *Siebel Remote and Replication Manager Administration Guide*.

- **SSL for email integrations.** Communications with email servers can now use SSL.

  For details, see *Siebel Communications Server Administration Guide*.

- **Null password warnings.** Siebel Enterprise Server configuration now requires users to specify passwords; null passwords are not allowed.

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

- **UserNameToken supported for Web services.** Siebel EAI now supports the UserNameToken element, a security mechanism included in the WS-Security specification. This feature allows Siebel applications to send and receive credentials through Web services in a standards-compliant manner.

  For details, see *Integration Platform Technologies: Siebel eBusiness Application Integration Volume II*.

2 About Security for Siebel Applications

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

General Security Concepts

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

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

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

Classifications of security services include:

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

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

Industry Standards for Security

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

NOTE: For more information about third-party products supported or validated for use with Siebel eBusiness Applications, see *System Requirements and Supported Platforms* on Siebel SupportWeb.

Supported standards include:

- **LDAP/ADSI.** Siebel Systems provides preconfigured integration with Lightweight Directory Access Protocol (LDAP) and Active Directory Services Interface (ADSI) for user authentication purposes. For more information, see "Security Adapters for LDAP/ADSI Authentication" on page 19 and Chapter 6, "Security Adapter Authentication."
- **SSL encryption and authentication.** Protection of communications between Siebel eBusiness Application components (that is, Siebel Servers and Web servers) by using the Secure Sockets Layer (SSL) capabilities of supported Web servers. For more information, see "Configuring Secure Communications" on page 50.

  Communications between Siebel Servers and directory servers can use SSL. For more information, see "Configuring Secure Communications for Security Adapter" on page 133.

  Communications between Siebel Servers and email servers can use SSL. For more information, see *Siebel Communications Server Administration Guide*.
- **X.509 certificates.** Siebel 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 159.
- **RSA SHA-1 password hashing.** Siebel user passwords can be hashed using the RSA SHA-1 algorithm. For more information, see "Configuring Password Hashing" on page 125.
- **RSA communications encryption.** Communication between Siebel components can be encrypted using RSA encryption algorithms. For more information, see "Configuring Secure Communications" on page 50.
  - For supported UNIX platforms, Windows platforms, or cross-platform environments, Siebel Systems supports RSA Bsafe. RSA Bsafe is FIPS 140-1 certified.
  - For supported Windows platforms, Siebel Systems supports Microsoft Crypto. (If the Siebel Server and the Web server are installed on the same machine running Microsoft Windows, then you cannot use Microsoft Crypto. You can use it only when these components run on different Microsoft Windows machines.)
- **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 "Configuring Data Encryption" on page 60.

To augment the security of your Siebel applications deployment, Siebel Systems has alliances with other leading security providers. Providers are listed as security software partners in the Alliances section of the Siebel Web page.

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 Systems has developed 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 Systems supports these types of user authentication:

- Siebel-provided database security adapter, for database authentication
- Siebel-provided LDAP or ADSI security adapters, for LDAP/ADSI authentication
- Web Single Sign-On (Web SSO)

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

These authentication mechanisms apply whether users access the Siebel application from within a LAN or WAN, or remotely. Figure 1 on page 18 shows a logical view of the three primary types of user authentication within a Siebel site.

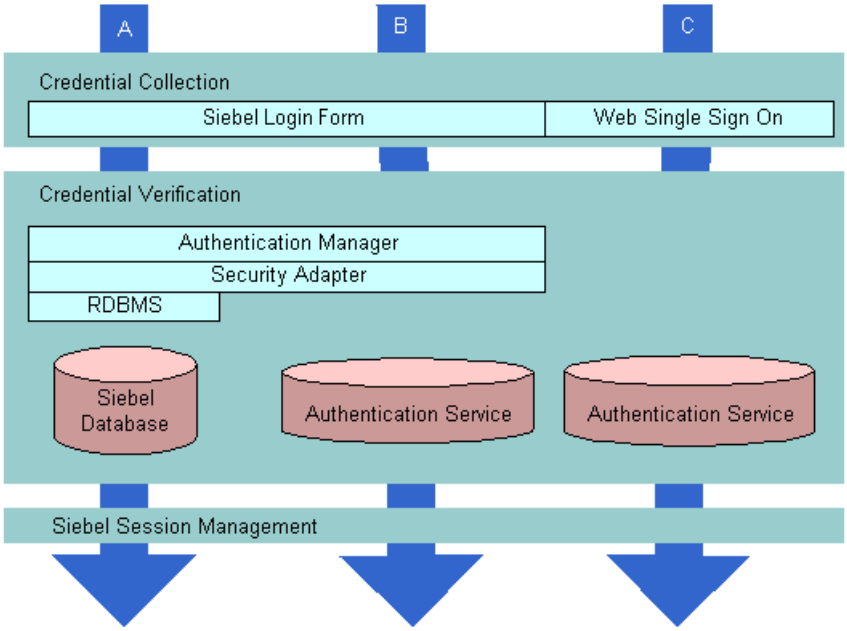


Figure 1. Logical Diagram of User Authentication Methods Within a Siebel Site

Security Adapter for Database Authentication

Siebel Systems provides 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 the Siebel application. The database administrator (DBA) must add all user database accounts. Database authentication deployment supports password hashing for protection against hacker attacks.

Any Siebel application can use database authentication, which is configured as the default. However, some functionality provided by Siebel Systems, 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.

NOTE: The exact valid character set for a Siebel username and password depends on the underlying authentication system. For database authentication, refer to documentation from your RDBMS vendor.

Security Adapters for LDAP/ADSI Authentication

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

NOTE: The exact valid character set for a Siebel username and password depends on the underlying authentication system. For LDAP/ADSI authentication, refer to documentation from your vendor, such as one of those listed below.

Siebel Systems customers can therefore verify user credentials with security standards such as Lightweight Directory Access Protocol (LDAP) or Active Directory Services Interface (ADSI).

Siebel Systems has developed security adapters for leading authentication services:

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

For information on supporting additional security vendors, see "Security Adapter SDK" on page 19.

Web Single Sign-On

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

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

NOTE: The exact valid character set for a Siebel username depends on the underlying authentication system. For Web SSO, refer to documentation from your vendor.

Siebel Systems has alliances with leading security providers for Web SSO integration. Providers are listed as security software partners in the Alliances section of the Siebel Web page.

Security Adapter SDK

Siebel Systems 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 may 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 the Siebel application.

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

Starting in Version 7.7, the underlying SDK is based on an IBM SDK (rather than a Netscape SDK).

The Siebel Security Adapter SDK is described in *Siebel Security Adapter Software Developers Kit 7*, available on Siebel SupportWeb.

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 20 shows the types of encryption available for communications within the Siebel environment.

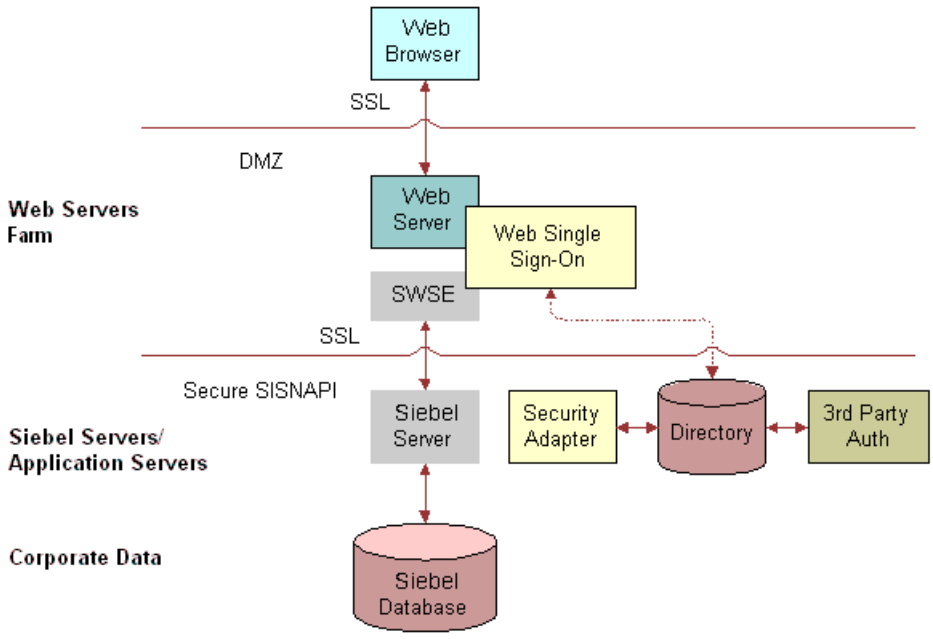


Figure 2. Encryption of Communications in the Siebel Environment

Client Browser to Web Server

Siebel applications run using the Siebel Web Client in a standard Web browser. When a user accesses a Siebel application, 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 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 the Siebel application will use SSL, in the following scenarios:

- Use SSL only on the login view to protect password transmission. See "Login Features" on page 163.
- Use SSL for additional specific views *(option available for standard interactivity applications only)*. See "Configuring Secure Views" on page 163.
- Use SSL for the entire application. See "Configuring Secure Views" on page 163.

Web Server to Siebel Server

Siebel software components communicate over the network using a Siebel TCP/IP-based protocol called SISNAPI (Siebel Internet Session API). Customers have the option to secure SISNAPI using 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 "Configuring Secure Communications" on page 50.

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 applications allow customers to encrypt sensitive information stored in the database so that it cannot be viewed without access to the Siebel application. Customers can configure Siebel software to encrypt a field of data before it is written to the database and decrypt the same data when it is retrieved. This prevents attempts to view sensitive data directly from the database. Siebel applications support data encryption using AES and RC2 algorithms.

For more information, see "Configuring Data Encryption" on page 60.

Controlling Access to Data

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

- View-level access control to manage which 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 unified administration for access to millions of content items for millions of 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 application a user can access, based on the functions assigned to that user. In Siebel applications, these functions are called *responsibilities*.

Responsibilities define the collection of views to which a user has access. An employee assigned to one responsibility may not have access to parts of the Siebel applications associated with another set of responsibilities. For example, typically a system administrator has 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 that need to view particular data records to access that information.

Siebel 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.

Auditing for Data Continuity

Siebel Systems supports various degrees of auditing.

- At the simplest level, each data record has created and last updated fields (when and by whom). With additional configuration, you can generate an activity for additional levels of auditing. This is best used when there are limited needs for auditing (just a few areas to track).
- Siebel applications can maintain an audit trail of information that tells when business component fields have been changed, who made the change, and what has been changed. 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 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 44.

Secure Physical Deployment to Prevent Intrusion

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

In Siebel application 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 Systems also supports 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 the Siebel application for users (such as employees) who require remote access.

Siebel eBusiness 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 need to be opened on the firewall between the Web server and the Siebel Server.

Siebel Systems architecture 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 need for failover and catastrophic recovery management. For more information, see *Deployment Planning Guide*.

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

Security for Mobile Solutions

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

Siebel Systems provides security for customers using these devices to access Siebel 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 products 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 59 and "Authentication for Mobile Web Client Synchronization" on page 141.

  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 applications through browser-enabled mobile devices. Siebel Wireless views rendered in XML or HTML are sent through the Siebel-supported Web server 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 including Triple DES (Data Encryption Standard) encryption through the RIM Mobile Data Service.

When using Siebel applications on the RIM BlackBerry wireless handheld, data is passed over the wireless data network and routed using the secure BlackBerry Enterprise Server with Mobile Data Service. All data traveling between the BlackBerry handheld and the corporate infrastructure is Triple-DES encrypted. The data remains encrypted along the entire path from source to destination.

Mobile Device User Authentication

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

Security Settings for the Web Browser

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

For detailed information about browser settings used in deploying Siebel clients, see *Siebel System Administration Guide*.

NOTE: For more information about settings in your Web browser, see the documentation that came with your browser, and see *System Requirements and Supported Platforms* on Siebel SupportWeb.

Bibliography of Security References

For more information about managing security on your network and industry trends in security, the following books and Web sites are available.

Books

Stallings, William. *Cryptography and Network Security: Principles and Practice*, Second Edition, 1999. Prentice Hall, http://www.prenhall.com.

Garfinkel, Simon with Gene Spafford. *Web Security, Privacy & Commerce*, Second Edition, January 2002. O'Reilly & Associates, Inc., http://www.oreilly.com.

Northcutt, Stephen, et al. *Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems*, First Edition, July 2002. New Riders Publishing, http://www.newriders.com.

Web Sites

Useful Web sites for Security Consortiums and Security Standards Commitees include:

- CERT Coordination Center, Carnegie Mellon University, http://www.cert.org.
- Sun Microsystems' Security page, http://wwws.sun.com/software/security/.

- Microsoft Security & Privacy home page, http://www.microsoft.com/security/.

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

Roadmap for Configuring Security

This section provides a general overview of tasks you can perform to take advantage of security resources for Siebel eBusiness Applications. Use this section 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 software 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 *Deployment Planning Guide* and 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 SADMIN password.
   - 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 application 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 44. See also *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 59.

   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 default passwords. It includes the following topics:

NOTE: For information about configuring and using hashed user passwords and database credentials passwords through your security adapter, see "Configuring Password Hashing" on page 125.

Changing Default Passwords

The Siebel Database Server installation script and the seed data provided with Siebel eBusiness 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 sections that follow include procedures for changing account passwords. Before you change default passwords, review the following points:

- For end users, the availability of the Password and Verify Password fields in the Siebel application (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 LDAP/ADS Directory" on page 80.

    In addition, the `Propagate Change` parameter (alias `PropagateChange`) must be `TRUE` for the LDAP or ADSI security adapter (default is `TRUE`). For Siebel Dedicated 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 `TRUE` for the parameter defined in the Name Server, `FALSE` for the same parameter defined in application configuration files for the Dedicated Web Client. For more information, see Chapter 6, "Security Adapter Authentication."

- The procedures in this section 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.

Changing System Administrator Passwords on Microsoft Windows

The Siebel Database Server installation script creates a Siebel administrator account that you can use to perform administrative tasks. The default user ID and password for this account are SADMIN and SADMIN (case-sensitive). You should change the password for this account.

You may also need to change the password for the Siebel service owner account, which is the Windows user 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 may cause the password to be truncated. For example, the password abcde''f may be truncated to abcde.

For more information about setting up these accounts for initial use, see the *Siebel Installation Guide* for the operating system you are using.

Changing Password for Siebel Service Owner Account

Use the procedure below to modify the password for the Siebel service owner, which is the Windows user 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, which is the user that starts the Siebel Server system service.

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

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

   a. Choose Start > Programs > Administrative Tools > Services.

   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.

NOTE: 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 Password for Siebel Administrator Database Account

Use the procedure below to modify the password for the Siebel administrator database account. You must also change the corresponding password parameter for the Siebel Enterprise.

To change the password for the Siebel administrator database account

1 Change the Siebel administrator's password for the Enterprise, using Siebel Server Manager.

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

b From the application-level menu, choose Navigate > Site Map > Administration - Server Configuration > Enterprises.

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 application (all users must log out).

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

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

4 Stop and restart the Siebel Server system service.

For details, see *Siebel System Administration Guide*.

Changing the Siebel Administrator Password on UNIX

The Siebel Database Server installation script creates a Siebel administrator account that you can use to perform administrative tasks. The default user ID and password for this account are SADMIN and SADMIN (case-sensitive). You should change the password for this 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 may cause the password to be truncated. For example, the password abcde"f may be truncated to abcde.

For more information about setting up this account for initial use, see the *Siebel Installation Guide* for the operating system you are using.

To change the password for the Siebel administrator database account

1. End all client sessions and shut down the Siebel Server. Use the following command to shut down the server:

   SIEBSRVR_ROOT/bin/stop_server all

   NOTE: In order to stop all Siebel Servers in the Siebel Enterprise, you must run this command on all Siebel Server machines.

2. Use Server Manager to change the password in the Siebel Gateway Name Server.

   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, refer to your RDBMS documentation on changing passwords.

4. Stop and restart the Siebel Gateway Name Server.

   $SIEBEL_ROOT/gtwysrvr/bin/stop_ns

   $SIEBEL_ROOT/gtwysrvr/bin/start_ns

5. Restart all Siebel Servers. Perform this step for each applicable Siebel Server.

   $SIEBEL_ROOT/siebsrvr/bin/start_server all

6. Connect to the Server Manager and verify the password change:

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

   You should be able to log in as SADMIN with the new password.

Changing the Table Owner (DBO) Password

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

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

A corresponding parameter is configured for the Siebel Enterprise, named Table Owner (alias TableOwner). Siebel application modules such as 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 applications, the Table Owner password does not need 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 may sometimes need to be provided manually. For example, both the Table Owner name and password are required when a task is started for the Generate New Database or Generate Triggers server components.

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 may also need 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. From the application-level menu, choose Navigate > Site Map > Administration - Server Configuration > Enterprises.
   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. If you have Siebel Dedicated Web Client users, also change the value for the `TableOwnPass` parameter in the [ServerDataSrc] section of each application configuration file, such as uagent.cfg for Siebel Call Center. This step must be done for each user's Siebel client installation.
3. Change the password in the database.

   For more information on changing passwords, refer to your RDBMS documentation.
4. 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. From the application-level menu, choose Navigate > Site Map > Administration - Server Management > Servers.
   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 Call Center 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. From the application-level menu, choose Navigate > Site Map > Administration - Server Configuration > Enterprises.
   b. Click the Component Definitions tab.
   c. Select the component that initiated the failed task.

      For example, if Call Center 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 Object Manager component definition, that may be the reason for the failed tasks. If so, respecifying the correct values should solve the problem.
3. Restart the Siebel Server machine, and check again if any tasks failed.

Adding a Password for Updating Web Server Static Files

As part of the installation hardening process, it is recommended that administrators define a password for updating cached images and other Siebel application-related static files on the Web server.

Each time the Siebel administrator restarts the Web server, the Siebel Web Server Extension (SWSE) contacts the Siebel Server and refreshes these static files. Administrators may find that entering a URL command is a more efficient way to refresh the files, particularly when multiple Web servers are deployed.

NOTE: Setting a password allows only Siebel administrators to refresh the cached static files on your Web server by accessing updated files originally placed on the Siebel Server. If you do not set a password, any unauthorized user could invoke the SWE command UpdateWebImages to update these files.

To add the Web update password, do one of the following:

- You can use the Web Update Protection Key screen that appears when you install and configure the SWSE. For more information, see the *Siebel Installation Guide* for the operating system you are using.
- You can add or change the password later on, by editing the value of the `WebUpdatePassword` parameter in the eapps.cfg file. This file is located in *SWEAPP_ROOT*\bin directory, where *SWEAPP_ROOT* is the directory in which you installed the SWSE.

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

If password encryption for the eapps.cfg file is in effect (`EncryptedPassword = TRUE`), then SWSE configuration automatically stores the specified Web update protection key as an encrypted value for the `WebUpdatePassword` parameter. If you manually edit the eapps.cfg file, then you must use the encryptstring utility to generate an encrypted version of the password to store in the file.

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 the"Managing Encrypted Passwords in the eapps.cfg File" on page 34.

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

To edit the eapps.cfg file to configure the Web update password

1. The Web public root directory (the location of Web file caching for Siebel applications) is set automatically when you run the SWSE configuration utility. 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 machine), add a parameter like this:

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

   where *SWEAPP_ROOT* is the SWSE installation directory, such as D:\sea77\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.

   NOTE: 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 Web update protection key (Web update password) can be set using the SWSE configuration utility. Or, you can specify it by adding a line in each application section of the eapps.cfg file. For example, to specify a Web update password for Siebel eService, add a parameter like this:

```
[/eservice_enu]
WebUpdatePassword = abcdef
```

NOTE: Typically, password encryption is in effect for the eapps.cfg file, as described in "Managing Encrypted Passwords in the eapps.cfg File" on page 34.

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

Passwords stored in the eapps.cfg file are encrypted. 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 application-specific sections of the eapps.cfg file. The value for the WebUpdatePassword parameter (Web update protection key) is also encrypted.

For more information about the WebUpdatePassword parameter, see "Adding a Password for Updating Web Server Static Files" on page 32.

After you have 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.

NOTE: 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 295.

Encrypting Passwords Using the encryptstring Utility

Using the Siebel Enterprise configuration utility to change an anonymous user password, or the Web update protection key, automatically saves the password in encrypted form.

If, however, you need to manually add an encrypted value for the corresponding parameters in the eapps.cfg file (`AnonPassword` or `WebUpdatePassword`), 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 may be something like fhYt8T9N4e8se4X3VavTjQXwAEqm. (*The specific value that is output will change each time you use the encryptstring utility*.)

CAUTION: Although the anonymous user has limited privileges, it is generally recommended to use more secure passwords for production deployments of your Siebel applications. The section "Changing Default Passwords" on page 27 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, as described earlier in this section.

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 Siebel Strong Encryption Pack" on page 60.

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:

NOTE: For more information on some of these topics, see the *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 machines on the local network, can have a significant impact on network security.

Figure 3 on page 38 shows the basic components included in a Siebel Systems network.

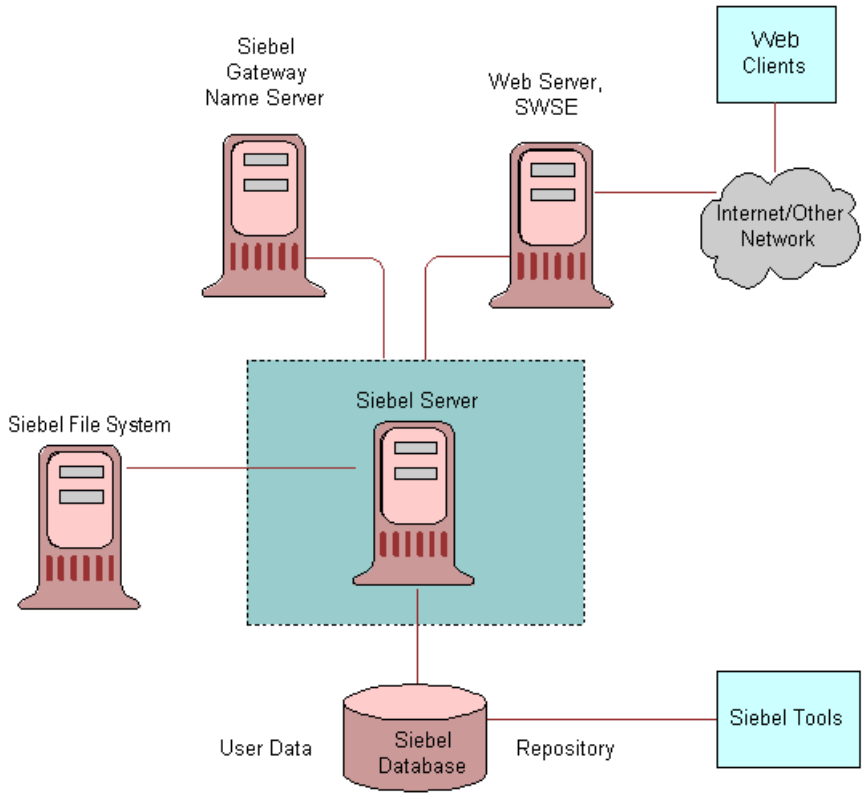


Figure 3. Siebel Network Components

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 eBusiness 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.

  NOTE: You do not need 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 Systems does not support the translation of port numbers or protocol switching. An example of protocol switching is changing from HTTP to HTTPS or vice versa.
  - Siebel Systems does support rewriting of the hostname and of the IP addresses of the Web servers.
  - The reverse proxy server and Web server must run on the same port.
  - 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 and vice versa.
- **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 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 section 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 machine. Sometimes called the DMZ (demilitarized zone), this zone is where the external network first interacts with the Siebel environment.

  NOTE: 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, it should reside 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. Access to this zone should be limited 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, or between the Siebel Database and the Siebel File System. Figure 4 on page 40 shows the recommended placement for firewalls in Siebel networks.

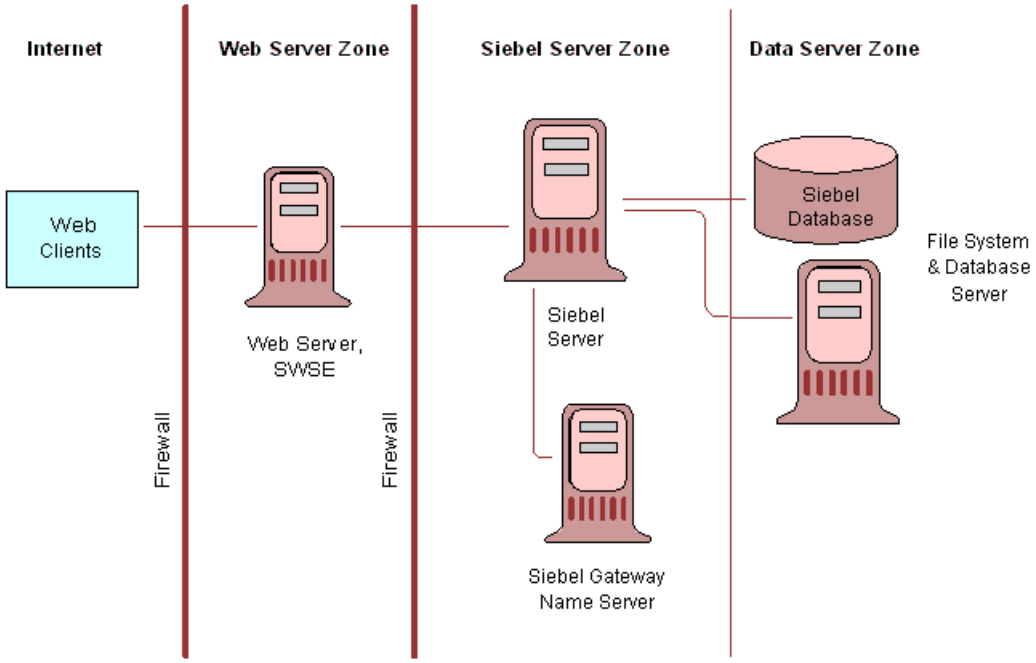


Figure 4. Firewalls in Siebel Networks

Deploying Siebel Applications Accessed Through a Firewall

When deploying Siebel 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 may be supported.) For more information, see "Parameters in the eapps.cfg File" on page 295.

- 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 applications. For more information, see "Cookies and Siebel Applications" on page 168.
- 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 Networking 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 the *Deployment Planning Guide*.

Port Numbers

Network traffic going to 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 applications, see the *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/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/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/ADS directory server to use with your Siebel 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.
- To allow users to access Siebel 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 should reside.

  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 needs to 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 and OS/390: 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 UPD run on top of IP.

- Siebel Mobile Client users who need 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

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

Physical Security of the Client Device

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

Most leading handheld devices, such as those made by HP/Compaq and RIM, have user-enabled passwords. RIM, for instance, allows users to select whether or not a password is required when the device is turned on. Siebel Systems 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.

For example, mFormation Inc. provides the ability to monitor the wireless network continuously and to delete contents of devices remotely when necessary, preventing unauthorized access to data even when a device falls into the wrong hands.

Database Server Access

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

To restrict privileges to Siebel Server processes, assign an operating system account specific to the Siebel Server. This account should only have access to files, processes, and executables required by Siebel applications. The Siebel Server account should not be the root administrator.

On UNIX systems, the .rhosts file allows remote, root administrators to access other machines. 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 Database Server and contains physical files used by Siebel 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 application environment, only the Siebel Service owner should have access rights to the Siebel File System directory. The Siebel Server processes and components use the Siebel Service owner account to operate.

NOTE: For Siebel Dedicated Web Client, access to the Siebel File System may be achieved either through FSM or through direct connection from each individual client. For more information, see the *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 applications can maintain an audit trail of information that indicates when business component fields have been changed, who made the change, and what has been changed.

Audit Trail is a configurable feature that creates a history of the changes that have been made to various types of information in various Siebel applications. An audit trail is a record showing who 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 *Applications Administration Guide*.

Securing Siebel Reports Server

This section describes securing communication between the Siebel Reports Server, the AOM, and the Siebel Web Client. Note the following considerations:

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

For more information, see the *Siebel Installation Guide* for the operating system you are using, the *Deployment Planning Guide*, and the *Siebel Reports Administration Guide*.

Siebel Reports Server Components

The Siebel Reports Server consists of the following components:

- **Actuate iServer.** Manages all services that support the administration, viewing, printing, scheduling, and authentication of reports. All report properties are stored in the Actuate Encyclopedia.
- **Actuate Management Console.** The browser-based interface that manages one or more Actuate iServers and Encyclopedias. (Replaces the Actuate Administrator Desktop.)
- **Actuate Active Portal.** Provides access to reports in the Actuate Encyclopedia. Users can generate, view, print and share reports.
- **Actuate e.Report Designer Professional (Optional).** Used by professional developers to build new reports or customize existing reports. The Actuate Basic Language and Actuate Foundation Class Library supports adding advanced reporting capabilities.
- **Actuate e.Report Designer (Optional).** Lets you design and build reports using its graphical user interface. This application complements e.Report Designer Professional and is used by business users to design and distribute a variety of reports. No programming is required. This application supports both modifying complex reports and using components from libraries.

Configuring Siebel Reports Server for Security

Areas of Siebel Reports Server that can be configured for security include the following:

- Communication between Siebel Web Client and Actuate Active Portal
- Communication with the AOM

Communication Between Siebel Web Client and Actuate Active Portal

This communication takes place during report viewing. When the Siebel Web Client communicates with Actuate Active Portal, a cookie that contains the encrypted Reports Server login parameters is passed through the HTTP headers. Because the login parameters are encrypted, this part of the communication is secure by default. The report itself is delivered in DHTML through Actuate Active Portal to the Siebel Web Client.

To make this part of the communications secure, enable SSL by setting the following parameter:

```
Actuate Server Network Protocol Name = HTTPS
```

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

For more information about cookies and Siebel applications, see "Cookies and Siebel Applications" on page 168.

Communication with the AOM

Report generation is initiated through the Siebel Reports Adapter for Actuate (which is part of the Siebel Web Services Framework), by using a SOAP call to Active Portal. A connection is established to the Actuate iServer using the supplied user credentials from the Siebel application. The iServer establishes a separate session to the Application Object Manager to obtain data for report generation. This communication is encrypted.

Set the desired encryption type (RSA or MSCRYTPO) for the `Actuate Server Connect String` parameter. For example:

```
Actuate Server Connect String = RSA
```

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

Securing Siebel Document Server

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

For more information about Siebel Document Server, see *Applications Administration 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. Only the user that authenticates as the Siebel Server service should have access to the file system and have execute permissions on the Siebel Document Server.
- Microsoft provides some standard utilities in the Resource kit to lock down security on a generic Microsoft Windows machine. 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. Macro security should be set to high so that untrusted macros cannot be executed by the document server. This should not be an issue as there should not be a need for macros inside of 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 machine 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 application 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 eBusiness 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 Systems limits 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 Siebel Strong Encryption Pack" on page 60.

To make sure that information remains private, Siebel eBusiness 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 eBusiness Applications use the Secure Sockets Layer, version 3.0 (SSL) capabilities of supported Web server platforms to secure transmission of data between the Web browser and the Web server.

  Siebel eBusiness 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 Secure Views" on page 163 and "Login Features" on page 163.

- **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 system platforms. 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 need to install the Siebel Strong Encryption Pack. For more information on the Siebel Strong Encryption Pack, see "About Siebel Strong Encryption Pack" on page 60.

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

- **SSL encryption for connection to LDAP/ADS.** Secure Sockets Layer (SSL) can be used for connection to certified LDAP or ADS 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 eBusiness 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 the Siebel application.

  Customers can configure Siebel software to encrypt field 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.

  Sensitive data can be encrypted by using AES (Advanced Encryption Standard) or RC2 encryption, at various key lengths. Encryption can be enabled for business component fields using Siebel Tools. For more information, see "Configuring Data Encryption" on page 60.

  NOTE: Field-level encrypted data should not be replicated to mobile users using Siebel Remote, because it cannot be decrypted and viewed on the Mobile Web Client. The local database for the Mobile Web Client can, however, be encrypted, if it is based on the encrypted template. For details, see *Siebel Remote and Replication Manager Administration Guide*.

- **RC4 encryption**. Siebel eBusiness Applications use RC4 encryption to encrypt passwords stored in the siebns.dat file and to encrypt the auto-login credential cookie. For more information about encrypted passwords in the siebns.dat file, see "About Password Encryption" on page 35. For more information about the Auto-Login Credential Cookie, see "Auto-Login Credential Cookie" on page 170.

- **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 eBusiness Applications. For more information, see "Configuring Password Hashing" on page 125.

Figure 5 on page 49 shows some of the types of encryption available in the Siebel application environment.

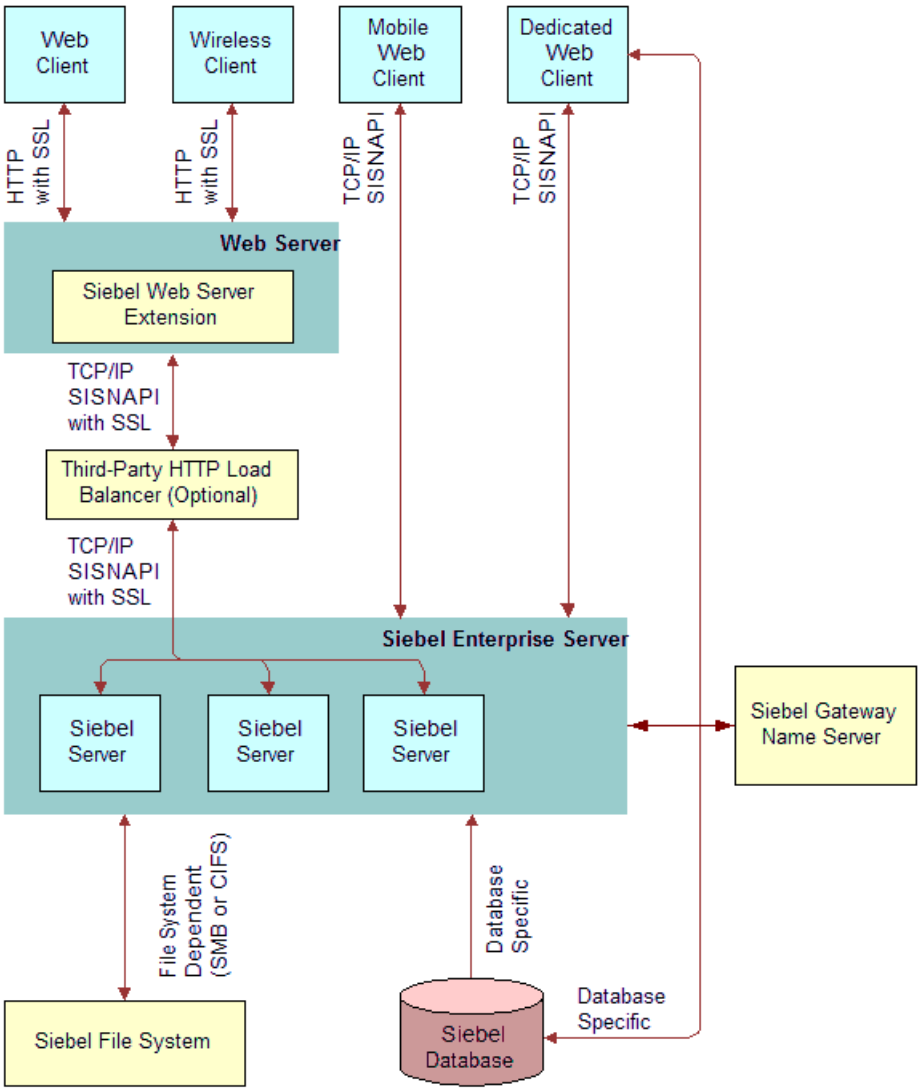


Figure 5. Communications Encryption in the Siebel Application Environment

Configuring Secure Communications

The following sections describe how to set up encryption for communication between components in the Siebel environment. Encryption may be configured for data traffic between the Web server, Siebel Server, and Siebel Web Client.

NOTE: Encryption options described in this section are not used to encrypt data in the database, as described in "Configuring Data Encryption" on page 60. Also, these encryption options are not used for communication with the database—for such encryption, check with your database vendor.

Configuring Encryption for Siebel Enterprise and SWSE

When you configure your Siebel Enterprise or Siebel Web Server Extension (SWSE) following 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 eBusiness Applications. It also corresponds to the value of the Siebel Enterprise parameter `Encryption Type`.

The Siebel Software Configuration Utility appears when you first install the Siebel Enterprise or SWSE. For information about running this utility, see the *Siebel Installation Guide* for the operating system you are using.

Using this utility, you can specify to use Secure Sockets Layer (SSL), Microsoft Crypto, or RSA encryption. (For SSL, you specify None, then specify whether to deploy SSL.)

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/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.

In the Siebel Software Configuration Utility, the Encryption Type screen displays the options for configuring the encryption type. You can choose one of the following options:

- **NONE.** Specify this option if you will use Secure Sockets Layer (SSL) instead of Microsoft Crypto or RSA encryption, or if you will not use encryption.
- **MSCRYPTO.** The Microsoft Crypto encryption protocol for communications between Siebel components (option available on Microsoft Windows platforms only).
- **RSA.** A required protocol if you are using the RSA Security Systems 128-bit strong encryption feature for Siebel components.

NOTE: For Siebel installations that include both UNIX and Microsoft Windows platforms, it is recommended to use an encryption method supported across platforms, such as SSL or RSA.

If you specified None for the encryption type, the utility prompts you for whether you want to deploy SSL in the enterprise (for the Siebel Enterprise or for SWSE).

- If you specify to deploy SSL, then additional screens appear for configuring SSL (these screens are part of the SSL configuration utility). For details, see the following sections:
  - "Configuring SSL Encryption for Siebel Enterprise or Siebel Server" on page 51
  - "Configuring SSL Encryption for SWSE" on page 55

  When you are done configuring SSL for the Siebel Enterprise or SWSE, you return to the Siebel Software Configuration Utility. (To complete SSL configuration for all Siebel Servers, you may subsequently need to run the SSL configuration utility separately one or more times.)
- If you do not specify to deploy SSL, then the SSL configuration screens do not display and you continue with the main Siebel Software Configuration Utility.

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, key exchange is handled through a standard SSL handshake.

Configuring SSL Encryption for Siebel Enterprise or Siebel Server

This section describes how you can 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.

Configuring at the Enterprise level applies to all Siebel Servers in the enterprise. In general, some of the settings should be configured differently at the Siebel Server level.

Configuring SSL communications between Siebel Servers and the Web server also requires that you configure SWSE to use SSL, as described in "Configuring SSL Encryption for SWSE" on page 55.

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 may 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.

Performing the procedure below adds parameters to the Siebel Gateway Name Server. If you also configure the SWSE for SSL, Name Server parameters mentioned in this procedure (short names) correspond to parameters added to the [connmgmt] section of the eapps.cfg file. Name Server parameters mentioned in this procedure can alternatively be set using Siebel Server Manager.

About Certificates and Private Key Files Used for SSL Authentication

When you configure SSL authentication for each Siebel Server and SWSE, you specify parameter values that indicate the names of certificate files, certificate authority files, and private key files on the Siebel Server and SWSE machines.

The certificate files you use for this purpose can be issued by and obtained from third-party certificate authorities. Certificate files must use either ASN (Abstract Syntax Notation) or PEM (Privacy Enhanced Mail) 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. Certificate files on each machine must be unique and belong to that machine if `PeerAuth = TRUE` on the remote machine. Certificate authority files identify the third-party certificate authority who issued the certificate. Private key files must use PEM format.

NOTE: The ASN format is also referred to as the DER format. The file extension (.asn) remains the same.

Certificate files and private key files are typically installed on each Siebel Server machine and SWSE machine for which you configure SSL.

You need not authenticate or encrypt communications between components on the same machine.

Running the SSL Configuration Utility for Siebel Server

This section describes running the SSL configuration utility for Siebel Server—that is, the Siebel Software Configuration Utility (Siebel Server SSL). Use this procedure to configure the Siebel Enterprise or to configure individual Siebel Servers.

NOTE: While performing the procedure below, if you specify to configure SSL for the Siebel Enterprise rather than an individual Siebel Server, all Siebel Servers in the Enterprise inherit all settings. These settings include the key filename and password and certificate filenames. You can run the utility again later to separately configure individual Siebel Servers, at which time you can specify unique key filenames or passwords or unique certificate filenames. In order to completely configure SSL for your Siebel Servers, you must run this utility multiple times.

The prompts for the SSL configuration utility are the same whether you run it in GUI mode or console mode. However, some user interface elements are different in these two modes.

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 run the SSL configuration utility separately later on a UNIX platform, it will run in console mode.

To enable SSL encryption for the Siebel Server

1. Before you begin, obtain and install the necessary certificate files you will need if you will configure SSL authentication.
2. If you are running the main Siebel Software Configuration Utility to configure the Siebel Enterprise or specific Siebel Servers, start the SSL configuration utility by specifying that you want to deploy SSL for the Enterprise, as described in "Configuring Encryption for Siebel Enterprise and SWSE" on page 50.
3. Alternatively, to run the SSL configuration utility directly on a Siebel Server machine, start the SSL configuration utility directly, as described below:

   - For Microsoft Windows platforms, open an MS-DOS window and enter the following command (utility runs in GUI mode):

     ```
     SIEBSRVR_ROOT\bin\ssincfgw.exe -l language -f
     SIEBSRVR_ROOT\admin\sslSiebsrvr.scm -logevents all
     ```

     where:

     - *SIEBSRVR_ROOT* is the Siebel Server installation directory
     - *language* is the language in which you want to run the SSL configuration utility (for example, ENU for U.S. English)

   - For UNIX platforms, enter the following commands (utility runs in console mode):

     ```
     cd SIEBSRVR_ROOT
     ```

     For Bourne shell or Korn shell:

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

     (Make sure there is a space between the initial period (`.`) and `./siebenv.sh`.)

     For C shell:

     ```
     source siebenv.csh
     ```

     ```
     cd SIEBSRVR_ROOT/bin
     ```

     ```
     ./icfg - l language -f SIEBSRVR_ROOT/admin/sslSiebsrvr.scm -logevents all
     ```

     where:

     - *SIEBSRVR_ROOT* is the Siebel Server installation directory
     - *language* is the language in which you want to run the SSL configuration utility (for example, ENU for U.S. English)

4 If you are running the SSL configuration utility separately (as described in Step 3 on page 53), enter the hostname of the Siebel Gateway Name Server machine and the name of the Siebel Enterprise applicable to the component you want to configure.

NOTE: If you are running the SSL configuration utility as part of running the Siebel Software Configuration Utility (as described in Step 2 on page 53), the Siebel Gateway Name Server and Siebel Enterprise were already specified. This screen does not appear.

5 Specify the configuration type: whether to configure SSL for the Siebel Enterprise or for a Siebel Server. (The issues behind this choice are described in a note just before this procedure.)

6 If you are configuring a Siebel Server, specify the name of the Siebel Server.

NOTE: If you specify Siebel Server SSL, the settings apply to all components on the Siebel Server. You cannot specify settings at the component level.

7 Specify the names of the certificate file and of the certificate authority file.

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

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

The password you specify will be stored in encrypted form.

The equivalent parameters in the Name Server are `KeyFileName` (display name `Private key file name`) and `KeyFilePassword` (display name `Private key file password`).

9 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.

NOTE: 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 Name Server is `PeerAuth` (display name `Peer Authentication`).

10 Specify whether you require peer certificate validation.

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

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

11 If you were running the SSL configuration utility as part of running the Siebel Software Configuration Utility, you return to that process, as described in the *Siebel Installation Guide* for the operating system you are using.

12 If you were running the SSL configuration utility directly, then review the settings, finish configuration, and restart the server.

13 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 55.

Setting Additional Name Server Parameters for Siebel Server SSL

After configuring SSL for Siebel Servers as described earlier in this section, make the following configuration changes:

- 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.

Configuring SSL Encryption for SWSE

This section describes how to configure your SWSE to use Secure Sockets Layer (SSL) encryption and, optionally, authentication for SISNAPI communications with Siebel Servers.

Configuring SSL communications between Siebel Servers and the Web server also requires that you configure Siebel Enterprise or Siebel Server to use SSL, as described in "Configuring SSL Encryption for Siebel Enterprise or Siebel Server" on page 51.

Performing this procedure adds parameters to the eapps.cfg file in a new section called [connmgmt]. For example, the [connmgmt] section might look like this:

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

Names for eapps.cfg file parameters mentioned in this procedure correspond to Name Server parameters for Siebel Server.

After running this utility, 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
```

Running the SSL Configuration Utility for SWSE

This section describes running the SSL configuration utility for SWSE—that is, the Siebel Software Configuration Utility (Siebel Web Server Extension SSL).

The prompts for the SSL configuration utility are the same whether you run it in GUI mode or console mode. However, some user interface elements are different in these two modes.

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 run the SSL configuration utility separately later on a UNIX platform, it will run in console mode.

To enable SSL encryption for the SWSE

1. Before you begin, obtain and install the necessary certificate files you will need if you will configure SSL authentication.
2. If you are running the main Siebel Software Configuration Utility to configure SWSE, start the SSL configuration utility by specifying that you want to deploy SSL for the Enterprise, as described in "Configuring Encryption for Siebel Enterprise and SWSE" on page 50.
3. Alternatively, to run the SSL configuration utility directly on a Web server machine, start the SSL configuration utility directly, as described below:
   - For Microsoft Windows platforms, open an MS-DOS window and enter the following command (utility runs in GUI mode):

     ```
     SWEAPP_ROOT\bin\ssincfgw.exe -l language -f
     SWEAPP_ROOT\admin\sslEapp.scm -logevents all
     ```

     where:

     - *SWEAPP_ROOT* is the SWSE installation directory
     - *language* is the language in which you want to run the configuration utility (for example, ENU for U.S. English)
   - For UNIX platforms, if the current path is not in the library path, you need to add it so that the SSL configuration utility can run on the machine that hosts the SWSE. The following list describes the parameter values for the library paths on supported UNIX platforms:
     - Sun Solaris = `LD_LIBRARY_PATH`
     - HP-UX = `SHLIB_PATH`
     - IBM AIX = `LIBPATH`

     For example, on IBM AIX, with C shell execute the following command from *SWEAPP_ROOT,* where *SWEAPP_ROOT* is the SWSE installation directory if the environment variable was set previously:

     ```
     setenv LIBPATH ${LIBPATH}:.
     ```

     If the environment variable was not set previously, execute the following command:

```
setenv LIBPATH .
```

For IBM AIX with Bourne shell or Korn shell execute the following command from *SWEAPP_ROOT*, where *SWEAPP_ROOT* is the SWSE installation directory if the environment variable was set previously:

```
export LIBPATH=${LIBPATH}:.
```

If the environment variable was not set previously, execute the following command:

```
export LIBPATH=.
```

When the current path is in the library path, you execute the following command to start the SSL configuration utility:

```
./icfg - l language -f SWEAPP_ROOT/admin/sslEapp.scm -logevents all
```

4 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`.

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 will be stored in encrypted form.

The equivalent parameters in the eapps.cfg file are `KeyFileName` and `KeyFilePassword`.

6 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: The peer authentication parameter is ignored if SSL is not deployed between the SWSE and the Siebel Server. 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 is `PeerAuth`.

7 Specify whether you require peer certificate validation.

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

The equivalent parameter in the eapps.cfg file is `PeerCertValidation`.

8 If you were running the SSL configuration utility as part of running the Siebel Software Configuration Utility (as described in Step 2 on page 56), you return to that process, as described in the *Siebel Installation Guide* for the operating system you are using.

9 If you were running the SSL configuration utility directly (as described in Step 3 on page 56), then review the settings, finish configuration, and restart the Web server.

10 Repeat this procedure for each SWSE in your application environment, as necessary.

Make sure you also configure each Siebel Server in your environment, as described in "Configuring SSL Encryption for Siebel Enterprise or Siebel Server" on page 51.

Configuring Encryption for Web Clients

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

Siebel eBusiness Applications support the following 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.

  This type of client uses parameters stored in the Siebel Gateway Name Server for the Siebel Server, and uses configuration files located on the SWSE and on the Siebel Server. Encryption settings you make to the SWSE or Siebel Server are automatically recognized by this Web Client.

  For more information, see "Configuring Encryption for Siebel Enterprise and SWSE" on page 50.

- **Siebel Mobile Web Client.** This client is designed for local data access, without the need to be connected to a server. Periodically, the client must access the Siebel Remote server using a modem, WAN, LAN or other network to synchronize data.

  For information on setting encryption for transmissions between Mobile Web Client and Siebel Remote server, see "Configuring Encryption for Mobile Web Client Synchronization" on page 59. See also *Siebel Remote and Replication Manager Administration Guide*.

- **Siebel Dedicated 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 eBusiness Applications architecture reside on the user's personal computer.

- **Siebel Wireless Client.** A wireless-enabled mobile client with a Web browser and Internet service. For more information, see *Siebel Wireless Administration Guide.*

- **Siebel Handheld Client.** A streamlined version of the Siebel Mobile Web Client. Documentation for particular Siebel products 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 *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 eBusiness 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 eBusiness 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 "Cookies and Siebel Applications" on page 168.

Configuring Encryption for Mobile Web Client Synchronization

You can 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.

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 Dedicated 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 141.

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.

   NOTE: When you edit configuration files, do not use a text editor that adds additional, nontext characters 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 an application (using File > Synchronize > Database), 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 application 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*.

Configuring Data Encryption

You can encrypt sensitive data in the Siebel Database, such as customer credit card numbers, using various encryption alternatives provided by Siebel Systems. Standard Siebel eBusiness Applications provide the option for 56-bit RC2 encryption capabilities for data in the Siebel Database.

If you require stronger encryption capabilities, see "About Siebel Strong Encryption Pack" on page 60.

If you are upgrading from Releases 6.x or 7.0.x, which used the mangle algorithm encryption method (standard encryptor), see "Upgrading Encrypted Data to 56-bit RC2 Encryption" on page 68 for information on how to move your data to the RC2 encryption standard using a 56-bit encryption key.

About Siebel Strong Encryption Pack

More secure encryption alternatives are provided with the Siebel Strong Encryption Pack, which includes:

- 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 keyfile (if previously encrypted with a 56-bit or 128-bit RC2 encryption key) and then re-encrypts the keyfile with a longer key and a more secure algorithm.

- An installation guide

  This guide describes how to install the Siebel Strong Encryption Pack and upgrade data to the encryption levels supplied in the Siebel Strong Encryption Pack.

AES encryption and RC2 encryption are provided as Siebel business services. You configure AES or RC2 encryption for business component fields using Siebel Tools. For details, see "Configuring Business Component Encryption" on page 66.

The Siebel Strong Encryption Pack is available from Siebel Systems on separate distribution media, and requires a separate installation into your existing Siebel Server environment. For information on how to obtain the Siebel Strong Encryption Pack, see Technical Note 566 on Siebel SupportWeb.

CAUTION: If you are upgrading your encryption level, make sure you read "Upgrade Issues for Data Encryption" on page 65 before you install the Siebel Strong Encryption Pack.

How Data Encryption Works

When encryption is enabled for a business component field, unencrypted data from the field 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 keyfile.

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

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

The rest of this section describes how to use the Key Database Manager utility to add encryption keys and to change the keyfile password.

Requirements for Data Encryption

Encrypting field data is subject to the following restrictions and requirements.

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

- Because encryption and decryption have performance implications, only fields with data that is truly sensitive, such as credit card numbers and social security numbers, should be encrypted.

- Siebel Assignment Manager does not decrypt data before making assignments. Assignment rules should take this limit into consideration.
- 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 eBusiness Applications without the Strong Encryption Pack.
- Encrypted field data is retrieved, decrypted, and displayed when records are selected. However, users cannot query or sort on the unencrypted values for these fields. Indexing columns for encrypted fields offers no benefit, because only the encrypted values are indexed.
- Encrypted data requires up to 2.5 times more storage space in the database than unencrypted data. You must specify appropriate data length for the affected columns. For example, data 10 characters long may use 25 characters when encrypted, data 30 characters long may use 75 characters when encrypted, and so on.
- All business component fields that are mapped to the same database column must have encryption turned on and must use consistent user property settings as described in this section. Using different encryption algorithms or different key lengths for different fields is not supported.
- Any business component field that is to store encrypted data must be active.
- Field-level AES or RC2 encryption is not supported for Mobile Web Clients or Dedicated Web Clients.
- Siebel Systems does not provide AES or RC2 encryption for numeric data. However, you can use the encryptor for any information that is stored as strings in the database. To encrypt a calculated numeric field, map the field to a string field, and then set the encryption property of the string field to TRUE.

  The get-value and set-value methods for the calculated field will take care of the conversion between numeric data and string data. As long as the business component uses the calculated field, encryption and decryption is transparent to the application. The only limitation for this workaround is that sorting and direct queries cannot be performed on a calculated field.

Using Key Database Manager

The Key Database Manager utility allows you to add new encryption keys to the keyfile and to change the keyfile password. The Key Database Manager utility is named keydbmgr.exe on Microsoft Windows and keydbmgr on UNIX platforms. It is located in the bin subdirectory of the Siebel Server directory.

The Key Database Manager program is available on all supported Siebel Server platforms.

Running Key Database Manager

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

The Key Database Manager automatically determines which encryptor to use (RC2 Encryptor or AES Encryptor).

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

To run the Key Database Manager

1. Shut down any server components that are configured to use 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 the 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 3 on page 63.

3. When prompted, enter the keyfile password.
   - To add a new encryption key, see "Adding New Encryption Keys" on page 64.
   - To change the keyfile password, see "Changing the Keyfile Password" on page 64.

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

5. Restart any server components that were shut down in Step 1 on page 63.

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

Table 3 on page 63 lists the flags and parameters for the Key Database Manager utility.

Table 3. 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.

Adding New Encryption Keys

You can add new encryption keys to the keyfile. The AES Encryptor or RC2 Encryptor uses the latest key in the keyfile 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 keyfile.

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

To add new encryption keys

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 "Running Key Database Manager" on page 62.
3. To add an encryption key to the keyfile, enter *2*.
4. Enter some seed data to provide random data used in generating the new encryption key.

   The key must be at least 7 characters in length.
5. Exit the utility by entering *3*.

   When exiting the Key Database Manager utility, monitor any error messages that may be generated. If an error occurred, you may need to restore the backup version of the keyfile.
6. Distribute the new keyfile to all Siebel Servers by copying the file to the admin subdirectory in the Siebel Server directory.
7. Restart any server components that were shut down in Step 1 on page 64.

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

Changing the Keyfile Password

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

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

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

To change the keyfile password

1. 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 "Running Key Database Manager" on page 62.

3 To change the keyfile 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 may be generated. If an error occurred, you may need to restore the backup version of the keyfile.

7 Distribute the new keyfile 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 64.

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

Upgrade Issues for Data Encryption

The Siebel Strong Encryption Pack upgrades Siebel eBusiness Applications to 128-bit, 192-bit, or 256-bit encryption. For more information, see "About Siebel Strong Encryption Pack" on page 60.

Supported data encryption upgrade scenarios are outlined in the following list:

- Upgrade to 128-bit RC2 encryption from the following:
  - No encryption
  - Standard Encryptor encryption (based on mangle algorithm)
  - 56-bit RC2 encryption
- Upgrade to 128-bit AES encryption from the following:
  - No encryption
  - Standard Encryptor encryption (based on mangle algorithm)
  - 56-bit RC2 encryption
  - 128-bit RC2 encryption
- Upgrade to 192-bit AES encryption from the following:
  - No encryption
  - Standard Encryptor encryption (based on mangle algorithm)
  - 56-bit RC2 encryption
  - 128-bit RC2 encryption
  - 128-bit AES encryption
- Upgrade to 256-bit AES encryption from the following:

- No encryption
- Standard Encryptor encryption (based on mangle algorithm)
- 56-bit RC2 encryption
- 128-bit RC2 encryption
- 128-bit AES encryption
- 192-bit AES encryption

Configuring Business Component Encryption

This section describes how to use Siebel Tools to enable and disable encryption for business component fields.

For more information about performing some of the tasks described in this section, see *Configuring Siebel eBusiness Applications*.

Siebel Systems provides the AES Encryptor and the RC2 Encryptor to allow you to encrypt data fields. To use the AES Encryptor, you need to obtain the Siebel Strong Encryption Pack. For more information, see "About Siebel Strong Encryption Pack" on page 60.

For more information about using either the AES Encryptor or the RC2 Encryptor to add encryption keys to the keyfile and change the keyfile password, see "Configuring Data Encryption" on page 60.

Setting Encryption User Properties

Application developers can encrypt fields in a business component by setting the encryption user properties described here. When encryption is turned on, data written to the field is encrypted and data read from the field is decrypted.

To turn on encryption for business component fields

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

   For example, in the Quote business component, the Credit Card Number field has field user properties for encryption.

4 In the field user properties, set the following encryption values:

Field User Property	Value	Description
Encrypted	`Y`	■ `Y` indicates the field is encrypted. ■ `N` indicates the field is not encrypted.
Encrypt Service Name	`AES Encryptor` `RC2 Encryptor`	Sets the type of encryption to use for the field.
Encrypt Key Field	*KeyIndexField*	Specify the field on the business component where the encryption key index is stored. For the Credit Card Number field in the Quote business component, this user property is set to Credit Card Number Key Index.
Encrypt ReadOnly Field	*CalculatedField*	Specify a calculated field that determines whether the data in the encrypted field is read-only. Storing the data in read-only form may allow someone to recover it later. For example, for the Credit Card Number field in the Quote business component, this user property is set to the calculated field Credit Card Number - Read Only. ■ The calculated value of Credit Card Number - Read Only is Y (TRUE) if encryption or decryption fails—the field data is read-only. ■ The calculated value is N (FALSE) if encryption or decryption succeeds—the field data is editable. If you need to create an equivalent field for another business component, set it as calculated and do not specify a field value.

Table 4 on page 67 shows some examples of Key Index Fields for business components.

Table 4. Encryption Key Index Fields

Business Component	Field	Key Index Field
FS Invoice	Credit Card Number	Credit Card Number Key Index
Order Entry - Orders	Credit Card Number	Credit Card Number Key Index
Personal Payment Profile	Account Number	Account Number Key Index
Quote	Credit Card Number	Credit Card Number Key Index

Table 4. Encryption Key Index Fields

Business Component	Field	Key Index Field
Cfg Favorites Quote Item	Credit Card Number	(Create a new field)
Get Users Data	PayAccntNum	(Create a new field)

Encrypted Database Columns

Siebel Systems provides a number of database columns that are encrypted by default. Table 5 lists the database table columns encrypted by default in the Siebel Database.

Table 5. Encrypted Database Table Columns

Table	Table Column
S_ORDER	ACCNT_ORDER_NUM
	CC_NUMBER
S_PTY_PAY_PRFL	PAY_ACCNT_NUM
	VERIFICATION_NUM
S_SRC_PAYMENT	CC_NUM
S_SSO_SYS_USER	SSO_PASSWORD

Upgrading Encrypted Data to 56-bit RC2 Encryption

As of Release 7.5.x, the standard encryptor encryption method is no longer supported. If you are upgrading from Release 6.x or 7.0.x, you must upgrade to RC2 or AES encryption.

Data encrypted by the standard encryptor must be upgraded to the RC2 standard before it can be read by releases later than 7.0.x. Use the Encryption Upgrade utility (encryptupg.exe), located in the bin subdirectory of the Siebel Server directory, to upgrade unencrypted data, and data that was encrypted using the standard encryptor, to the RC2 encryption method.

This section describes how to upgrade to 56-bit RC2 encryption. If you want to upgrade to 128-bit RC2 encryption or AES encryption, see "About Siebel Strong Encryption Pack" on page 60.

CAUTION: For encryption with Unicode, you must use either AES or RC2 encryption, rather than the Standard Encryptor, which is no longer supported.

Perform the following procedures to upgrade your encryption method:

- Verify that all prerequisites are met. See "Prerequisites for Upgrading to 56-bit RC2 Encryption" on page 69.
- Make sure that the input file includes every column that you want to upgrade. See "Modifying the Input File" on page 69.

- If you customized business component fields to use the standard encryptor, verify that you have the correct user property definitions. See "Configuring Business Component Encryption" on page 66.
- Run the Key Database Manager utility to change the password or add a new key to the database. See "Using Key Database Manager" on page 62.

Prerequisites for Upgrading to 56-bit RC2 Encryption

In order to upgrade to the RC2 encryption method, the following prerequisites 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 of Release 6.x or 7.0.x, for each encrypted column that you want to upgrade, you need to create a new column to store the key index.
- 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 keyfile was created in the *SIEBEL_ROOT*/siebsrvr/admin directory when you installed the Siebel Server.)

Modifying the Input File

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. The input file is located in *SIEBEL_ROOT*/dbsrvr/bin directory. If you wish to execute the Encryption Upgrade Utility from the command line, place this file in the *SIEBEL_ROOT*/siebsrvr/bin directory.

The input file must include every column that you want to upgrade. The first line of the input file indicates a table name with brackets around it. The table name should be followed on subsequent lines by 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
```

After each table, skip a line, and continue with subsequent tables. Here is a sample input file:

```
[S_ORDER]
CC_NUMBER  S_ORDER  CCNUM_ENCRPKEY_REF

[S_DOC_ORDER]
CC_NUMBER  S_DOC_ORDER  CCNUM_ENCRPKEY_REF

[S_PER_PAY_PRFL]
PAY_ACCNT_NUM  S_PER_PAY_PRFL  CCNUM_ENCRPKEY_REF
```

To support upgrade of non-encrypted fields to RC2 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
```

Converting Encrypted Data to 56-bit RC2 Encryption

Follow the instructions below to convert data encrypted using the standard encryptor to 56-bit RC2 encryption.

NOTE: 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 convert to 56-bit RC2 encryption

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 69.
2. Run encryptupg.exe to convert to 56-bit RC2 encryption.

   From *SIEBEL_ROOT*\siebsrvr\bin, enter 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 encryption is no longer supported.

   - *ToEncryptionStrength* is the encryption strength that you want to upgrade to. Enter RC2 to upgrade to RC2 encryption.
   - *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 the standard encryptor of releases prior to 7.5.x to RC2 encryption:

```
encryptupg /f STAND /t RC2 /j d:\sea78\siebsrvr\bin\encryptupg.inp /l ENU /u sadmin
/p dbpw /c d:\sea78\siebsrvr\bin\enu\siebel.cfg
```

3 After the upgrade is complete, make sure that business components that contain encrypted fields specify the value for the RC2 encryption method in their user properties. For more information, see "Setting Encryption User Properties" on page 66.

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

Security Considerations for Unicode Support

Siebel eBusiness 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 may 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 a Siebel Application

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

Encrypted Data

Siebel eBusiness Applications provide either AES and RC2 encryption to encrypt field 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 "Configuring Data Encryption" on page 60.

6 Security Adapter Authentication

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

About User Authentication

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

- **Security adapter authentication.** Siebel applications provide a security adapter framework to support several different user authentication scenarios:
  - **Database authentication.** Siebel applications support authentication against the underlying database. In this architecture, the security adapter authenticates users against the Siebel Database. Siebel Systems provides a database security adapter (it is configured as the default security adapter).
  - **LDAP/ADSI authentication.** Siebel applications support authentication against LDAP-compliant directories or Microsoft Active Directory Server (ADS). In this architecture, the security adapter authenticates users against the directory. Siebel Systems provides a security adapter for LDAP and a security adapter for ADSI.
  - **Custom.** You can use a custom adapter you provide and configure the Siebel applications to use this adapter. For more information, see "Security Adapter SDK" on page 19.

- **Web Single Sign-On (Web SSO).** This approach uses an external authentication service to authenticate users before they access the Siebel application. In this architecture, a 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 may choose the approach for user authentication individually for each application in your environment, based on the specific application requirements. However, there are administrative benefits to using a consistent approach across all of your Siebel applications, because a consistent approach lowers the overall complexity of the deployment. Siebel Mobile Web Client can use only database authentication.

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 purposes of configuration parameters and procedures for setting their values, see Appendix B, "Configuration Parameters Related to Authentication."
- **Seed data.** When you install your Siebel eBusiness Applications, you are provided seed data that is related to authentication, user registration, and user access to Siebel applications. For detailed information on the seed data that is provided and for procedures for viewing and editing seed data, see Appendix C, "Seed Data."

Comparison of Authentication Strategies

Table 6 on page 75 highlights the capabilities of each authentication approach to help guide your decision. Several options are available for each basic strategy. X indicates that Siebel Systems supports the feature (with applicable third-party components). (X) indicates that Siebel Systems does not directly support the feature, but it may be supported by third-party components.

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

Table 6. Comparison of Authentication Approaches

Desired Deployment or Functionality	Database Security Adapter	LDAP/ ADSI Security Adapter	Web SSO	Comments
Does not require additional infrastructure components.	X			
Centralizes storage of user credentials and roles.		X	X	
Limits number of database accounts on the application database.		X	X	
Supports dynamic user registration. Users are created in real-time through self-registration or administrative views.		X	(X)	For Web SSO, user registration is the responsibility of the third-party authentication architecture. It is not logically handled by the Siebel architecture.
Supports account policies. You can set policies such as password expiration, password syntax, and account lockout.	X	X	(X)	Among supported RDBMS vendors for the Siebel Database, account policy (password expiration only) is supported *only* for supported IBM DB2 Universal Database platforms. For Web SSO, account policy enforcement is handled by the third-party infrastructure.
Supports Web Single Sign-On, the capability to log in once and access all the applications within a Web site or portal.			X	

About Siebel Security Adapters

When you install your Siebel eBusiness Applications, these security adapters are provided for user authentication:

- Database security adapter
- 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 the Siebel application.

An LDAP or ADS 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.

In general, the process of security adapter authentication includes the following principal stages:

- The user provides identification credentials.
- The user's identity is verified.
- The user's Siebel user ID and database account are retrieved from a directory, from the Siebel Database, or from another external source (for Web Single Sign-On).
- The user is granted access to the Siebel application and the Siebel Database.

For specific information about third-party directory servers supported by Siebel-provided security adapters, see *System Requirements and Supported Platforms* on Siebel SupportWeb for your Siebel application.

You can implement a security adapter other than one of those provided by Siebel Systems. To support the functionality described in this section for the Siebel adapters, the adapter you implement must support the Siebel Security Adapter Software Development Kit. For more information, see "Security Adapter SDK" on page 19.

Depending on how you configure your authentication architecture, the security adapter may 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 in the directory. If the user exists, the adapter retrieves the user's Siebel user ID, a database account, and, optionally, a set of roles which are passed to the Application Object Manager (AOM) to grant the user access to the Siebel application and the database. This adapter functionality is typical in a security adapter authentication implementation.

- **Without authentication (Web SSO mode).** The 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 the Siebel application 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 capability for a user's authentication on your Web site to serve for access to other applications on the Web site, including Siebel 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 the user is created in the Siebel Database.

Configuring Database Authentication

If you do not use LDAP/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 a Siebel application.

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 application 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 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 the Siebel application

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 may 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 Dedicated Web Client, parameters are configured by editing the application configuration file.

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 adatper (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 you should create a new database security adapter. Otherwise, settings you make will reconfigure the existing security adapter wherever it is used.

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 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 196.

The following option is available if you implement database authentication:

- **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 "Configuring Password Hashing" on page 125.

About LDAP/ADSI Security Adapter Authentication

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

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

Security adapter authentication provides a user with access to the Siebel application for which the security adapter is configured. Different Siebel applications may be configured to use different security adapters.

LDAP/ADSI Authentication Benefits

LDAP/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 application user interface by an internal administrator, a delegated administrator, or a self-registering user
- User self-registration
- Registration of users by delegated administrators through the Web site

LDAP/ADSI Authentication Process

The steps in the LDAP/ADSI security adapter authentication process are:

1. The user enters credentials to a Siebel application login form.

   These user credentials (a username and password) can vary depending on the way you configure the security adapter. For example, the username could be the Siebel user ID or an identifier such as an account or telephone number. The user credentials 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.

Requirements for LDAP/ADS Directory

If you are using LDAP or ADSI authentication, you must provide your own directory product, whether it is one of the directory servers supported by Siebel-provided security adapters or another directory of your choice. For specific information about third-party products supported by Siebel eBusiness Applications, see *System Requirements and Supported Platforms* on Siebel SupportWeb for your Siebel application.

- If you provide one of the Siebel-supported directory servers (that is, a supported LDAP directory or Microsoft ADS), then you can use a Siebel-provided security adapter, or you can create your own Siebel-compliant security adapter.
- If you provide a directory other than those supported by the Siebel-provided security adapters, then you are responsible for implementing a security adapter that will support this directory.

Data Requirements for Directory

Your LDAP/ADS directory must store, at a minimum, the following data for each user. Each piece of data is contained in an attribute of the directory.

- **Siebel user ID.** This attribute value must match the value in the user ID field for the user's Person record in the Siebel Database. It is used to identify the user's database record for access-control purposes.
- **Database account.** This attribute value must be of the form `username=`*U* `password=`*P*, where *U* and *P* are credentials for a database account. There may be any amount of white space between the two key-value pairs, and there must be no space within each pair. The keywords `username` and `password` must be lowercase.
- **Username.** This attribute value is the key passed to the directory that identifies the user. In a simple implementation, it may be the Siebel user ID, and so it may not need to be a separate attribute.
- **Password.** The storage of a user's login password differs between LDAP servers and ADS.
  - **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 an attribute.
    - If the user is authenticated by an authentication service, such as in a Web SSO implementation, a password attribute is not required.
  - **ADS.** ADS does not store the password as an attribute. The password can be entered at the directory level as a function of the client, or the ADSI security adapter can use ADS methods to create or modify a password.
    - If the user authenticates through the ADS 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.

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

An additional 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 applications. For more information, see "Configuring Roles Defined in Directory" on page 138.

User Privileges for Directory

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

NOTE: For ADSI authentication, it is recommended to use the Delegate Control Wizard to define privileges for users in the ADS directory.

You must create the following user:

- **Application user.** You must implement the application user, which is the only user that must be able to search and write records to the directory. For more information, see "Configuring the Application User" on page 131.

LDAP Security Adapter Requirements

If you are using LDAP authentication with any supported LDAP directory product, you must confirm that the IBM LDAP Client software that is provided by Siebel Systems is installed. If this LDAP Client is not yet installed, then you must manually install it.

- The LDAP Client software must be installed on the Siebel Server machine where the LDAP security adapter will function.
- In addition, if you require LDAP security adapter functionality from a Siebel Dedicated Web Client, you must install the LDAP client software on each such client computer.

For IBM LDAP Client installation instructions, see "Installing LDAP Client Software" on page 82.

ADSI Security Adapter Requirements

If you are running the Siebel Server on supported Microsoft Windows platforms and you are using ADSI authentication, you must meet the requirements described here. For more information about some of these issues, refer to your Microsoft Active Directory documentation.

- 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 may be met in multiple ways:
  - Including all systems as part of a single Microsoft Windows domain forest
  - Configuring trust relationships

- Configuring Secure Sockets Layer (SSL)

It is also recommended to place all Siebel Servers and Active Directory Servers in the same domain forest.

NOTE: To perform user management in the ADS directory through the Siebel client, it is strongly recommended that you configure ADS at the server level for SSL communications between the Active Directory client and server. This is different from SSL communications between the security adapter and the directory, which is configured through Siebel applications and is discussed in "Configuring Secure Communications for Security Adapter" on page 133.

- DNS servers on your network must be properly configured with DNS entries for ADS. 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 Dedicated Web Client deployments, you must install the ADSI client software on each such client computer, where applicable. This requirement does not apply universally across supported Microsoft Windows platforms.

  NOTE: For more information about ADSI client issues, search Microsoft's Web site for information about Active Directory Client Extensions.

To confirm successful installation of a Siebel-supported ADSI client

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 ADSI client are present in the subdirectory. For details, refer to your vendor documentation.
3. For each DLL, right-click on the file and choose Properties.
4. Click the Version tab to see the version number.

Installing LDAP Client Software

This section provides instructions for installing the IBM LDAP Client and IBM GSKit.

- IBM LDAP Client provides Siebel applications the ability to authenticate against supported LDAP directory servers, when used with the LDAP security adapter.
- IBM GSKit, optionally installed with IBM LDAP Client, enables Siebel applications to communicate with supported LDAP directory servers over SSL.

NOTE: The IBM installer program you run refers to the IBM Directory Server, IBM Directory Server Client, or Client SDK. In this document, the applicable client module is referred to as the IBM LDAP Client. Siebel eBusiness Applications use the IBM LDAP Client and GSKit software with all supported LDAP directory products, not just with IBM Directory Server.

Consider the following requirements for IBM LDAP Client installation into a Siebel environment:

- IBM LDAP Client *must* be installed on each Siebel Server machine for which LDAP authentication is to be supported, using the LDAP security adapter. IBM GSKit must also be installed if you are supporting SSL. The IBM LDAP Client software can be installed either before or after you install Siebel Server.
- For Siebel Dedicated Web Client deployments for which LDAP authentication is to be supported, the IBM LDAP client *must* be installed on each local client machine. IBM GSKit must also be installed if you are supporting SSL. The IBM LDAP Client software can be installed either before or after you install the Siebel Dedicated Web Client.

Installation is typically performed from a DVD provided by Siebel Systems. For information about installing Siebel Servers, Siebel Dedicated Web Clients, and other modules, see the *Siebel Installation Guide* for the operating system you are using.

This section also provides instructions for installing IBM GSK iKeyMan, a utility you use to generate certificate database files (CMS files). Certificate database files are required for Siebel applications to communicate with LDAP directory servers over SSL. IBM GSK iKeyMan can be installed on any machine using a supported platform. If you require this module, you only need to install it once per deployment.

NOTE: Statements in this section assume that you are installing the correct versions of the IBM software. For more information about third-party software, including supported version numbers for these IBM modules, see *System Requirements and Supported Platforms* on Siebel SupportWeb. Also refer to your vendor documentation.

Considerations for Secure LDAP Using 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.

- If IBM GSKit has been installed, the LDAP libraries dynamically loads the SSL libraries and uses 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.

NOTE: This installation guide assumes that SSL capability is, or will be, required for Siebel LDAP authentication. Therefore, the LDAP client installation process includes GSKit installation as its integral part. If you are absolutely sure that SSL will never be turned on for Siebel LDAP authentication, you do not need to install GSKit.

Use the following sections to install an IBM LDAP Client on different operating system platforms.

Installing the IBM LDAP Client and GSKit on Windows

This section describes different methods of installing the IBM LDAP Client and GSKit on Microsoft Windows platforms.

Installing with InstallShield GUI on Windows

Use the procedure below to install the IBM LDAP Client and GSKit on Windows platforms using the InstallShield GUI.

In the procedure below, if the installation program exits without displaying the language window after Step 6 on page 84, this might be caused by one of the following:

- Backlevel video drivers. Update your video drivers to correct this.
- Not enough space in the directory specified by the TEMP environment variable. Be sure that you have at least 100 MB of free space in this directory.

NOTE: If you use the InstallShield GUI to install, you must also use it to uninstall.

To install IBM LDAP Client and GSKit on Windows—InstallShield GUI

1. On the computer where you are installing the IBM LDAP Client, stop any programs that are running and close all windows.
2. Insert the DVD *Siebel eBusiness Applications, Base Applications for Windows*. Then, using Windows Explorer, navigate from the DVD root directory to the folder Windows\Server_Ancillary\ibmldap51.
3. Unzip the file that is stored there, such as by running the following command:

   ```
   unzip ids510fp2refresh-windows-client-us.zip
   ```

4. Navigate to the unzip directory, such as, for example:

   ```
   C:\Documents and Settings\Administrator\Local Settings\Temp\ids510fp2refresh-windows-client
   ```

5. Navigate to the ids_ismp subdirectory.
6. Run setup.exe.

   The language window is displayed.

7. Select the language you want to use during IBM LDAP Client installation. Click OK.

   This is the language used in the installation program, not in the IBM LDAP Client itself. You choose the language used in the IBM LDAP Client in Step 13 on page 85.

8. On the Welcome window, click Next.

   If you have a previous version of the IBM LDAP Client installed on your system, you are asked if you want to continue with the installation.

9 Click Yes to install over the previous version, or click No to exit the installation program.

10 After reading the software license agreement, click the option "I accept the terms in the license agreement." Click Next.

11 Any preinstalled components and corresponding version levels are displayed. Click Next.

12 To install to the default directory, click Next. To specify a different installation location, click Browse.

NOTE: Do not use special characters, such as hyphen (-) and period (.), in the name of the installation directory. If you do not use the default location, use a name such as ldap or ldapdir. Do not use a name such as ldap-dir or ldap.dir.

13 Select the language you want to use in the IBM LDAP Client software. Click Next.

14 Click Custom, and click Next.

A list of available components is displayed.

15 Select both displayed options: Client SDK (LDAP Client) and GSKit. Click Next.

NOTE: If you are sure that SSL will never be enabled for your LDAP Client, you can deselect GSKit here.

A window summarizing the components selected for installation and configuration is displayed.

16 If you want to change your selection, click Back. To begin installing, click Next.

17 After the files are installed, the Client README file opens. Click Next.

18 Specify whether to restart your computer now or later. Click Finish.

You have completed installation of IBM LDAP Client and IBM GSKit.

Installing with InstallShield Console on Windows

Use the procedure below to install the IBM LDAP Client and GSKit on Windows platforms using the InstallShield console. The steps for installing using the InstallShield console are similar to those for installing using the InstallShield GUI.

To install IBM LDAP Client and GSKit on Windows—InstallShield console

1 Perform Step 1 on page 84 through Step 5 on page 84.

2 In the ids_ismp directory, run the following command:

```
setup -is:javaconsole -console
```

3 Perform the remaining user interactions through the console rather than the GUI.

Installing with InstallShield Unattended Mode on Windows

Use the procedures below to install the IBM LDAP Client and GSKit on Windows platforms using the InstallShield unattended mode. Separate procedures are provided for installing IBM LDAP Client and IBM GSKit.

To install IBM LDAP Client on Windows—InstallShield unattended mode

1. Perform Step 1 on page 84 through Step 5 on page 84.
2. In the ids_ismp directory, run the following command:

   ```
   .\setup.exe -is:silent -options .\optionsFiles\InstallClient.txt
   ```

   This command installs the IBM LDAP Client to the directory C:\Program Files\IBM\LDAP.
3. To change the installation location, modify the file .\optionsFiles\InstallClient.txt.

   For example, if you want to install the LDAP Client under D:\Program Files\IBM\LDAP, edit the file to include the following:

   ```
   # install destination - this can be modified to install location
   -P product.installLocation="D:\Program Files\IBM\LDAP"
   ```

To install IBM GSKit on Windows—InstallShield unattended mode

1. Perform Step 1 on page 84 through Step 4 on page 84.
2. Navigate to the gskit subdirectory.
3. Run the following command:

   ```
   .\SETUP.EXE LDAP -s -f1 .\setup.iss
   ```

   This command installs IBM GSKit to the directory C:\Program Files\IBM\GSK6.
4. To change the installation location, modify the file setup.iss.

   For example, if you want to install GSKit under D:\Program Files\IBM\GSK6, edit the file to include the following:

   ```
   [SdAskDestPath-0]
   szDir=D:\Program Files\IBM\GSK6
   ```

To uninstall IBM GSKit on Windows—InstallShield unattended mode

- To uninstall IBM GSKit when it was previously installed with unattended mode, run the following command at the command line:

  ```
  gsk6BUI LDAP
  ```

Verifying Installation on Windows

Use the procedure below to verify that IBM LDAP Client and GSKit were successfully installed.

To verify installation on Windows

1. Choose Start > Settings > Control Panel > Add or Remove Programs.
2. Verify that entries are listed for the IBM LDAP Client, and for IBM GSKit.

3 Verify that appropriate libraries are installed:

   a Verify that ldap.dll exists under *installation_location*\LDAP\bin.

   b Verify that gsk6ssl.dll exists under *installation_location*\GSK6\lib.

Uninstalling with InstallShield on Windows

If you have used InstallShield to install IBM LDAP Client and GSKit, you must also use it to uninstall these components.

To uninstall the IBM LDAP Client and GSKit using InstallShield

1 Choose Start > Settings > Control Panel > Add or Remove Programs.

2 Select IBM Directory Server 5.1 (or the version appropriate to your installation).

Installing the IBM LDAP Client and GSKit on Solaris

This section describes different methods of installing the IBM LDAP Client and GSKit on Solaris platforms.

Installation When Non-IBM LDAP Files Exist on Your System

During the installation of the IBM LDAP Client on Solaris machines, you might encounter the following message:

```
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.
```

To relocate non-IBM LDAP files encountered during installation

1 Specify the new directory to which to move the non-IBM LDAP files:

```
(/usr/bin/ldapsparc) [?,q]
```

2 Press Enter to accept the default directory (/usr/bin/ldapsparc), or type a new path name and press Enter, or type q and press Enter to quit.

After relocating the files, you might see these additional messages:

```
## Processing system information.

WARNING: /usr/bin/ldapadd <no longer a linked file>

WARNING: /usr/bin/ldapdelete <no longer a regular file>

WARNING: /usr/bin/ldapmodify <no longer a regular file>
```

```
WARNING: /usr/bin/ldapmodrdn <no longer a regular file>

WARNING: /usr/bin/ldapsearch <no longer a regular file>

## Verifying package dependencies.

## Verifying disk space requirements.

## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being used by another
package:

/usr/bin/ldapadd

/usr/bin/ldapdelete

/usr/bin/ldapmodify

/usr/bin/ldapmodrdn

/usr/bin/ldapsearch

Do you want to install these conflicting files [y,n,?,q]
```

3 Type y and press Enter to continue the installation. The existing files are moved to the directory previously specified and the IBM LDAP Client files are installed in the /usr/bin directory.

Installing with Console Mode (Interactive) on Solaris

Use the procedures below to install the IBM LDAP Client and GSKit on Solaris platforms using the interactive console mode.

Separate procedures are provided for installing IBM LDAP Client and IBM GSKit.

To install IBM LDAP Client on Solaris—console mode

1 Login as root.

2 Insert the DVD *Siebel eBusiness Applications, Base Applications for Solaris*. Then navigate from the DVD root directory to the folder Solaris\Server_Ancillary\ibmldap51.

3 Copy the file ids510fp2refresh-solaris-client-us.tar to an empty directory that has at least 50 MB of available space.

4 Enter the following command:

```
tar -xvf ids510fp2refresh-solaris-client-us.tar
```

The directory ids510fp2refresh-solaris-client is created at the current location.

5 Navigate to the directory ids510fp2refresh-solaris-client.

6 Enter the following command:

```
pkginfo -d 'pwd'/ldap.client_rted.pkg
```

A list of installable software is displayed, such as:

```
application IBMldapc

IBM Directory Client
```

7 Enter the following command to begin installing:

```
pkgadd -d 'pwd'/ldap.client_rted.pkg
```

8 Respond to other prompts, as appropriate.

When installation is complete, a message similar to the following appears:

```
Installation of <IBMldapc> was successful.
```

To install IBM GSKit on Solaris—console mode

1 Perform Step 1 on page 88 through Step 5 on page 88.

2 Enter the following command:

```
uncompress gsk6bas.tar.Z
```

3 Enter the following command:

```
tar -xvf gsk6bas.tar
```

4 Enter the following command:

```
pkginfo -d 'pwd'
```

A list of installable software is displayed, such as:

```
application gsk6bas

Certificate and SSL Base Runtime (gsk6bas)
```

5 Enter the following command to begin installing:

```
pkgadd -d 'pwd'
```

Installing with Unattended Mode (Noninteractive) on Solaris

Use the procedure below to install the IBM LDAP Client and GSKit on Solaris platforms using the unattended mode.

To install IBM LDAP Client and GSKit on Solaris—unattended mode

1 Perform Step 1 on page 88 through Step 5 on page 88.

2 To add the IBM LDAP Client, enter the following command:

```
pkgadd -d 'pwd' /ldap.client_rted.pkg -r IBMldapc_response -a 'pwd'/adminfile -n
IBMldapc
```

3 To add GSKit, enter the following command:

```
pkgadd -d 'pwd' -r gsk6bas_response -a 'pwd'/adminfile -n gsk6bas
```

The files IBMldapc_response, gsk6bas_response, and adminfile are located in the directory ids510fp2refresh-solaris-client.

Verifying Installation on Solaris

Use the procedure below to verify that IBM LDAP Client and GSKit were successfully installed.

To verify installation on Solaris

1 Use pkginfo to see if software is installed on the machine. Enter the following commands:

```
pkginfo|grep IBMldapc
```

```
pkginfo|grep gsk6bas
```

2 Verify that the directories /opt/IBMldapc and /opt/ibm/gsk6 exist.

3 Verify that the file libibmldap.so exists under /opt/IBMldapc/lib.

4 Verify that the file libgsk6ssl.so exists under /opt/ibm/gsk6/lib.

5 Verify that symbolic links to libibmldap.so and libgsk6ssl.so exist under /usr/lib.

Uninstalling on Solaris

If you have installed IBM LDAP Client and GSKit, use the procedure below to uninstall these components.

To uninstall the IBM LDAP Client and GSKit on Solaris

1 Login as root.

2 Enter the following commands:

```
pkgrm IBMldapc
```

```
pkgrm gsk6bas
```

Installing the IBM LDAP Client and GSKit on AIX

This section describes different methods of installing the IBM LDAP Client and GSKit on AIX platforms.

Installing with Console Mode (Interactive) on AIX

Use the procedures below to install the IBM LDAP Client and GSKit on AIX platforms using the interactive console mode. Separate procedures are provided for installing IBM LDAP Client and IBM GSKit.

To install IBM LDAP Client on AIX—console mode

1. Log in as root.
2. Insert the DVD *Siebel eBusiness Applications, Base Applications for AIX*. Then navigate from the DVD root directory to the folder AIX\Server_Ancillary\ibmldap51.
3. Copy the file ids510fp2refresh-aix-client-us.tar to an empty directory that has at least 50 MB of available space.
4. Enter the following command:

   ```
   tar -xvf ids510fp2refresh-aix-client-us.tar
   ```

   The directory ids510fp2refresh-aix-client is created at the current location.
5. Navigate to the directory ids510fp2refresh-aix-client.
6. Enter the following command:

   ```
   installp -ld 'pwd' | grep ldap
   ```

   A list of installable software is displayed, such as:

   ```
   ldap.client.adt             5.1.0.0                   I  N usr
   ldap.client.rte             5.1.0.0                   I  N usr,root
   ldap.max_crypto_client.adt  5.1.0.0                   I  N usr
   ldap.max_crypto_client.rte  5.1.0.0                   I  N usr
   ```
7. Install the required packages. Enter the following command:

   ```
   installp -acgXd 'pwd' ldap.*
   ```

   where:

   - -a stands for apply
   - -c stands for commit
   - -g installs prerequisites if necessary
   - -X increases the file system space if needed

- -d stands for device

When installation is complete, the system generates an installation summary.

8 Verify that the Result column shows success for all loaded files. You can also verify that IBM Directory Server was installed successfully by typing the following at a command prompt:

```
lslpp -L | grep ldap
```

The output displayed lists all the filesets starting with ldap. This includes the client, html, and message filesets. For example:

```
ldap.client.adt          5.1.0.0  C  F   IBM Directory SDK

ldap.client.rte          5.1.0.0  C  F   IBM Directory Client Runtime

ldap.max_crypto_client.adt

ldap.max_crypto_client.rte
```

To install IBM GSKit on AIX—console mode

1 Perform Step 1 on page 91 through Step 5 on page 91.

2 Enter the following command:

```
installp -ld 'pwd'/gskak.rte
```

A list all of the installable IBM GSK packages is displayed.

```
gskak.rte                   6.0.5.34                   I N usr

#   AIX Certificate and SSL Base Runtime ACME Toolkit
```

3 At the command prompt, install the required packages with the following command:

```
installp -acgXd 'pwd'/gskak.rte gskak.rte
```

where:

-a stands for apply

-c stands for commit

-g installs prerequisites if necessary

-X increases the file system space if needed

-d stands for device

4 When installation is complete, the system generates an installation summary. Verify that the Result column shows success for all loaded files. You can also verify that IBM LDAP Client was installed successfully by typing the following at a command prompt:

```
lslpp -L | grep gsk
```

The output lists all the filesets starting with gsk. For example:

```
gskak.rte                 6.0.5.34    C     F    AIX Certificate and SSL Base
```

Installing with Unattended Mode (Noninteractive) on AIX

Use the procedure below to install the IBM LDAP Client and GSKit on AIX platforms using the unattended mode.

To install IBM LDAP Client and GSKit on AIX—unattended mode

1. Perform Step 1 on page 91 through Step 5 on page 91.
2. Enter the following command:

```
installp -acgXd 'pwd' ldap.*
```

This will install both IBM LDAP Client and GSKit (because LDAP Client is a prerequisite of the GSKit).

Verifying Installation on AIX

Use the procedure below to verify that IBM LDAP Client and GSKit were successfully installed.

To verify installation on AIX

1. Use lslpp to see if software is installed on the machine. Enter the following commands:

```
lslpp -L|grep ldap
```

```
lslpp -L|grep gsk
```

2. Verify that /usr/ldap and /usr/opt/ibm/gskak exist.
3. Verify that libibmldap.a exists under /usr/ldap/lib.
4. Verify that libgsk6ssl.so exists under /usr/opt/ibm/gskak/lib.
5. Verify that symbolic links to libibmldap.a and libgsk6ssl.so exist under /usr/lib.

Uninstalling on AIX

If you have installed IBM LDAP Client and GSKit, use the procedure below to uninstall these components.

To uninstall the IBM LDAP Client and GSKit on AIX

1. Login as root.
2. Enter the following commands:

```
installp -u ldap.*
```

```
installp -u gskak.rte
```

Troubleshooting IBM LDAP Client Installation on AIX

When installing the IBM LDAP Client on AIX, the following error messages may appear:

```
mkdir: 0653-358 Cannot create /home/ldap.

/home/ldap: The file system has read permission only.

chgrp: /home/ldap: A file or directory in the path name does not exist.

chown: /home/ldap: A file or directory in the path name does not exist.

cp: /home/ldap/.profile: A file or directory in the path name does not exist.

chmod: /home/ldap/.profile: A file or directory in the path name does not exist.

chgrp: /home/ldap/.profile: A file or directory in the path name does not exist.

chown: /home/ldap/.profile: A file or directory in the path name does not exist.

3004-721 Could not create user.

3004-703 Check "/usr/lib/security/mkuser.sys" file.

instal: Failed while executing the ldap.client.rte.pre_i script.
```

Solution: A user named ldap is created automatically during installation if this user does not already exist. Sometimes installation may fail because the ldap user cannot be created successfully. In such case, manually create the ldap user before installing the IBM LDAP Client.

Installing the IBM LDAP Client and GSKit on HP-UX

This section describes different methods of installing the IBM LDAP Client and GSKit on HP-UX platforms.

Installing with GUI Mode on HP-UX

Use the procedure below to install the IBM LDAP Client and GSKit on HP-UX platforms using the GUI mode.

To install IBM LDAP Client on HP-UX—GUI mode

1. Login as root.
2. If you have logged into the HP-UX machine remotely, set the DISPLAY environment variable appropriately for your session, so that the SD install GUI displays on your local desktop.
3. Insert the DVD *Siebel eBusiness Applications, Base Applications for HP-UX*. Then navigate from the DVD root directory to the folder HPUX\Server_Ancillary\ibmldap51.
4. Copy ids510fp2refresh-hpux-client-us.tar to an empty directory that has at least 50 MB of available space.

5 Enter the following command:

```
tar -xvf ids510fp2refresh-hpux-client-us.tar
```

6 Navigate to the directory ids510fp2refresh-hpux-client.

7 Enter the following command:

```
swlist -s 'pwd'/hpux11_ibmldap51clients.depot
```

A list of software available in the .depot file is displayed, similar to the following:

```
LDAPClient    5.1.0.0        IBM Directory 5.1 Client (SSL)
```

8 Enter the following command:

```
swinstall -s 'pwd'/ hpux11_ibmldap51clients.depot
```

The SD install GUI is displayed.

9 Select LDAPClient.

10 Select Actions -> Mark For Install.

11 Select Actions -> Install....

Analysis is complete when the status field reads Ready.

12 Click OK.

13 Click Yes to begin installation.

Installation is complete when the status field reads Completed.

14 Click Done.

15 Exit the SD install GUI.

16 Create symbolic links for the LDAP Client libraries.

NOTE: The IBM LDAP Client installer on HP-UX does not set symbolic links for the LDAP Client libraries in the directory /usr/lib. If these symbolic links are not set, then the Siebel LDAP security adapter cannot be loaded.

To set symbolic links for LDAP client libraries in /usr/lib, run the script setlinkforibmldaplib.csh, located in the directory ids510fp2refresh-hpux-client. Because this script is written in the C shell, make sure that /bin/csh exists. First change the script to be executable using the command chmod +x setlinkforibmldaplib.csh, then run it.

To install IBM GSKit on HP-UX—GUI mode

1 Perform Step 1 on page 94 through Step 6 on page 95.

2 Enter the following command:

```
uncompress gsk6bas.tar.Z
```

3 Enter the following command:

```
tar -xvf gsk6bas.tar
```

4 Navigate to the directory gsk6bas.

5 Enter the following command:

```
swlist -s `pwd`
```

A list of available software is displayed, similar to the following:

```
gsk6bas        6.0.4.41      IBM gsk6 RUNTIME KIT
```

6 Enter the following command:

```
swinstall -s 'pwd'
```

The SD install GUI is displayed.

7 Select gsk6bas.

8 Select Actions -> Mark For Install.

9 Select Actions -> Install....

Analysis is complete when the status field reads Ready.

10 Click OK.

11 Click Yes to begin installation.

Installation is complete when the status field reads Completed.

12 Click Done.

13 Exit the SD install GUI.

14 Manually create symbolic links in /usr/lib for every library in /usr/IBMldap/lib.

Installing with Unattended Mode (Noninteractive) on HP-UX

Use the procedures below to install the IBM LDAP Client and GSKit on HP-UX platforms using the unattended mode. Separate procedures are provided for installing IBM LDAP Client and IBM GSKit.

To install IBM LDAP Client on HP-UX—unattended mode

1 Perform Step 1 on page 94 through Step 6 on page 95.

2 Enter the following command:

```
swinstall -s 'pwd'/hpux11_ibmldap51clients.depot LDAPClient
```

3 Create symbolic links for the LDAP Client libraries.

NOTE: The IBM LDAP Client installer on HP-UX does not set symbolic links for the LDAP Client libraries in the directory /usr/lib. If these symbolic links are not set, then the Siebel LDAP security adapter cannot be loaded.

To set symbolic links for LDAP client libraries in /usr/lib, run the script setlinkforibmldaplib.csh, located in the directory ids510fp2refresh-hpux-client. Because this script is written in the C shell, make sure that /bin/csh exists. First change the script to be executable using the command chmod +x setlinkforibmldaplib.csh, then run it.

To install IBM GSKit on HP-UX—unattended mode

1. Perform Step 1 on page 94 through Step 6 on page 95.
2. Enter the following command:

   ```
   swinstall -s 'pwd' gsk6bas
   ```

Verifying Installation on HP-UX

Use the procedure below to verify that IBM LDAP Client and GSKit were successfully installed.

To verify installation on HP-UX

1. Use swlist to see if software is installed on the machine. Enter the following commands:

   ```
   swlist | grep LDAPClient
   ```

   ```
   swlist | grep gsk6bas
   ```

2. Verify that /usr/IBMldap and /opt/ibm/gsk6 exist.
3. Verify that libibmldap.sl exists under /usr/IBMldap.
4. Verify that libgsk6ssl.sl exists under /opt/ibm/gsk6/lib.
5. Verify that symbolic links to libibmldap.sl and libgsk6ssl.sl exist under /usr/lib.

Uninstalling on HP-UX

If you have installed IBM LDAP Client and GSKit, use the procedure below to uninstall these components.

To uninstall on HP-UX

1. Login as root.
2. If you have logged into the HP-UX machine remotely, set the DISPLAY environment variable appropriately for your session, so that the SD Remove window displays on your local desktop.
3. Enter the following command:

   ```
   swremove
   ```

   The SD Remove window is displayed.
4. Select LDAPClient and gsk6bas to be removed.
5. Select Remove....

To uninstall on HP-UX—unattended mode

1. Perform Step 1 on page 97 through Step 2 on page 97.

2 To remove LDAPClient, enter the following command:

```
swremove LDAPClient
```

3 To remove GSKit, enter the following command:

```
swremove gsk6bas
```

Installing and Configuring IBM GSK iKeyMan

This section provides information about installing and configuring IBM GSK iKeyMan. This module needs to be installed only once per deployment.

Prerequisite for Running IBM GSK iKeyMan

- Java 1.3 or 1.3.1 is required for GSK iKeyMan to work properly. (IBM GSK iKeyMan does not work with Java 1.4.)

Installing IBM GSK iKeyMan

Follow the installation instructions for IBM GSKit for your platform:

- "Installing the IBM LDAP Client and GSKit on Windows" on page 84
- "Installing the IBM LDAP Client and GSKit on Solaris" on page 87
- "Installing the IBM LDAP Client and GSKit on AIX" on page 91
- "Installing the IBM LDAP Client and GSKit on HP-UX" on page 94

Enabling CMS Capability for IBM GSK iKeyMan

Perform the following procedure before you start the GSK iKeyMan GUI.

To set up GSK iKeyMan to support CMS key databases

1 Install IBM or an equivalent JDK 1.3 or 1.3.1.

2 Set JAVA_HOME to point to the directory where JDK 1.3 is installed. For example:

- On Windows, set JAVA_HOME=C:\Progam Files\IBM\Java13.
- On UNIX, export JAVA_HOME=/usr/opt/IBMJava13.

NOTE: Java requirements for Siebel high interactivity clients on Microsoft Windows platforms are incompatible with the above setting. If you need to run both Siebel client software and IBM GSK iKeyMan on the same machine, you may need to reset the Java settings after each use of IBM GSK iKeyMan. For more information about Java requirements for Siebel high interactivity clients, see browser configuration information in *Siebel System Administration Guide*.

3 Remove the gskikm.jar and ibmjcaprovider.jar files from your ${JAVA_HOME}/jre/lib/ext directory.

4 Be sure that ${JAVA_HOME}/jre/lib/ext has the following jar files:

```
ibmjceprovider.jar

ibmpkcs.jar

ibmjcefw.jar

local_policy.jar

US_export_policy.jar

ibmjlog.jar
```

NOTE: 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.

5 Register IBM JCE and IBM CMS service providers:

Update the ${JAVA_HOME}/jre/lib/security/java.security file to add the IBMJCE provider and IBMCMS 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 can be found in *GSK_installation_directory*\classes\gsk_java.security.

Generating a CMS File Using IBM GSK iKeyMan

By enabling SSL for the Siebel LDAP security adapter, a secure connection will be established between the Siebel application and its LDAP server.

How to enable SSL for a LDAP server is beyond the scope of this book. Refer to your third-party LDAP server administration documentation for that purpose. This section 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 machine 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 file format. You can generate a CMS file using IBM GSK iKeyMan.

The rest of this section provides detailed instructions for generating a CMS file and enabling SSL for the Siebel LDAP security adapter. Upon completion, you should be able to bring up Siebel applications with LDAP authentication and you can expect that communications between Siebel applications and LDAP server will be secure.

About Generating a CMS File

The CMS file should 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 evlabnet9:392. The server certificate for this LDAP server is issued by the certificate server evlab1. Therefore, the CMS file only needs to contain CA certificate for evlab1. It does not need to contain a server certificate for evlabnet9. If the Siebel Server is configured to authenticate against another LDAP server that gets its server certificate from evlab1, you do not have to update the CMS file.

Generating a CMS File

Use the procedure below to configure IBM GSK iKeyMan to support CMS key databases, and to generate a CMS file.

Before you do this, install the IBM LDAP Client and GSKit software, as described in previous platform-specific sections under this overall topic, "Installing LDAP Client Software" on page 82.

To configure GSK iKeyMan to support CMS key databases

1. Install IBM GSK iKeyMan on your machine. For details, see "Installing and Configuring IBM GSK iKeyMan" on page 98.
2. Determine which CA issued the server certificate for your LDAP server and obtain this CA certificate.
3. Copy the CA certificate to the machine where you have installed GSK iKeyMan.
4. Create a new CMS file using iKeyMan.
   a. Navigate to *GSK_installation_directory*/bin, where *GSK_installation_directory* is the directory where you installed both IBM GSKit and GSK iKeyMan.
   b. Enter the following command:

      ```
      gsk6ikm
      ```

   c. To create a new CMS file, 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 the location where you intend to store your CMS file. Click OK.
   e. In the Password Prompt dialog box, enter and confirm the password, and check the option Stash the password to a file. Click OK.

      The stash password option creates a file with the same name as the CMS file, but with the extension .sth. The file is created at the same location as the CMS file. For example, ldapkey.sth is created if your CMS file is named ldapkey.kdb.
   f. If you are using the stash password option, click OK to confirm the creation of the .sth file.

      The newly created CMS file opens in the iKeyMan main window.
5. Add one or more CA certificates to the CMS file 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 file. 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 file, instead of creating a new CMS file 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 these sections in this chapter:

- "About LDAP/ADSI Security Adapter Authentication" on page 79
- "Implementing LDAP/ADSI Security Adapter Authentication" on page 102 (includes "Using the LDAP/ADSI Configuration Utility" on page 103)

To enable SSL for the Siebel LDAP security adapter

1. Copy the ldapkey.kdb (the CMS file) and ldapkey.sth files you just created in the previous procedure to the Siebel Server machine where you will run AOM components that will 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 file, such as d:\ssldb\ldapkey.kdb.

3. Restart the Siebel Server (if you are configuring LDAP on a Siebel Server).

Implementing LDAP/ADSI Security Adapter Authentication

This section provides instructions for implementing LDAP/ADSI security adapter authentication.

To provide user access to a Siebel application implementing LDAP/ADSI security adapter or Web SSO authentication, the Siebel application must be able to retrieve the following:

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

Task Overview

You must perform the following tasks to set up a typical LDAP/ADSI security adapter authentication architecture:

- Set up a directory from which a database account and a Siebel user ID can be retrieved for each user.
- Configure parameters for the security adapter. You can do this by running the LDAP/ADSI Configuration Utility or by setting Name Server parameters directly using Server Manager.
- Configure parameters to specify which security adapter you are using. You can do this by running the LDAP/ADSI Configuration Utility or by setting Name Server parameters directly using Server Manager.
- *Dedicated Web Clients only*: Configure security-related parameters in application configuration files.
- *Dedicated Web Clients only*: Set a security-related system preference.
- Configure security-related parameters in the eapps.cfg file on the SWSE.
- Restart the Siebel Server and the Web server.

The LDAP/ADSI Configuration Utility can modify parameter values on the Name Server. You can also modify Name Server parameters using Siebel Server Manager.

For Dedicated Web Client deployments, the LDAP/ADSI Configuration Utility can modify parameter values in application configuration files, such as uagent.cfg for Siebel Call Center. You can also modify configuration files by editing them manually.

For more information about using the LDAP/ADSI Configuration Utility, see "Using the LDAP/ADSI Configuration Utility" on page 103.

For more information about security-related configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

Issues for Dedicated and Mobile Web Clients

Special issues apply for authentication for deployments using Siebel Dedicated Web Client or Mobile Web Client:

- For a particular Siebel application, when users connect from the Siebel Dedicated Web Client to the server database, the authentication mechanism must be the same as that used for Siebel Web Client users. This mechanism could be database authentication or a supported external authentication strategy, such as LDAP or ADSI.
- When connecting to the local database from the Mobile Web Client, mobile users must use database authentication. For information about authentication options for local database synchronization, see *Siebel Remote and Replication Manager Administration Guide*.

Using the LDAP/ADSI Configuration Utility

Siebel Systems provides the LDAP/ADSI Configuration Utility to help you configure your Siebel applications to authenticate against an external LDAP or ADS directory.

The utility provides a graphical user interface (GUI) to update configuration parameters, whether those stored in the Siebel Gateway Name Server or those stored in Siebel application configuration files (when configuring Siebel Dedicated Web Clients).

The utility is installed with the Siebel Server. After installation and configuration of the Siebel Enterprise, you can run this utility as a stand-alone program.

- On Windows platforms, the utility runs in console mode.
- On UNIX platforms, the utility runs in command-line mode.

The LDAP/ADSI Configuration Utility comprises the configuration executable program used by multiple Siebel modules (including the main Siebel Software Configuration Utility used for configuring the Siebel Enterprise and the SWSE) and the model file that provides specific LDAP/ADSI configuration functionality.

- The executable program, located in the bin subdirectory of the Siebel Server installation directory, is named ssincfgw.exe on Microsoft Windows platforms, and named icfg on UNIX platforms.
- The model file, located in the admin subdirectory of the Siebel Server installation directory, is named secadpt.scm.

For information about using the main Siebel Software Configuration Utility, see *Siebel Installation Guide* for the operating system you are using.

The full name for the LDAP/ADSI Configuration Utility is Siebel Software Configuration Utility - LDAP/ADSI Security Adapter Configuration. This name appears in the title bar of the utility's title bar (in console mode).

When you are configuring Siebel Gateway Name Server parameters, then the Name Server must be running. Otherwise, there are no special setup requirements to run the utility.

NOTE: The utility works best if run locally rather than over the network. Therefore, it is recommended that you run the utility from the Siebel Server machine.

Figure 6 on page 104 shows an example screen (for Windows platforms).

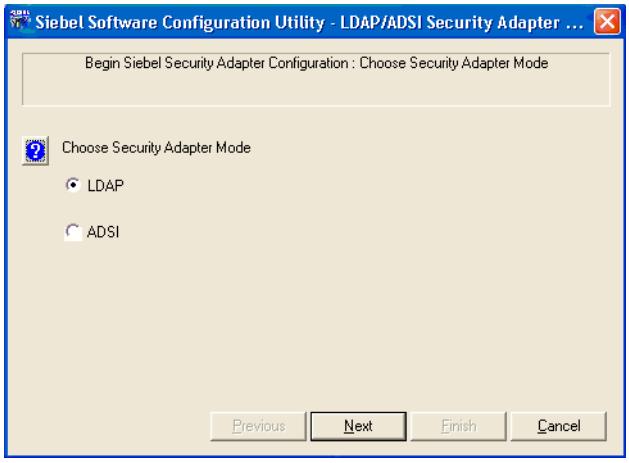


Figure 6. LDAP/ADSI Configuration Utility (Windows version)

When you specify the security adapter mode, either LDAP or ADSI, the setting you make provides the value (either `LDAP` or `ADSI`) for the `Security Adapter Mode` (`SecAdptMode`) parameter.

You also specify the name of the LDAP or ADSI security adapter. This setting provides the value of the `Security Adapter Name` (`SecAdptName`) parameter. You can use the default name or specify a different name. If an enterprise profile (named subsystem) does not already exist with the name you specified, the utility creates a new enterprise profile using that name.

- For LDAP, `Security Adapter Name` defaults to `LDAPSecAdpt`.
- For ADSI, `Security Adapter Name` defaults to `ADSISecAdpt`.

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), then you should create a new LDAP or ADSI security adapter. Otherwise, settings you make will reconfigure the existing security adapter wherever it is used.

Additional configuration parameters will be defined for the particular LDAP or ADSI security adapter—that is, for the `LDAPSecAdpt` or `ADSISecAdpt` enterprise profile or for a similar profile using a nondefault name. As an example of a parameter defined for the security adapter, the `Security Adapter Dll Name` (`SecAdptDllName`) parameter is automatically set when you specify LDAP or ADSI as the security adapter mode.

NOTE: The utility sets authentication-related configuration parameters for Siebel applications, but does not make changes to the LDAP/ADS directory. Make sure the configuration information you enter is compatible with your directory server.

About Configuration for Dedicated Web Clients

When you configure Siebel Dedicated Web Clients (see Step 5 on page 106), parameter values are written to a configuration file you specify, such as uagent.cfg for Siebel Call Center. `SecAdptMode` and `SecAdptName` are defined in the section [InfraSecMgr]. Additional LDAP or ADSI parameters are defined in the [LDAPSecAdpt] or [ADSISecAdpt] section, or in a section using a nondefault name.

CAUTION: The LDAP/ADSI Configuration Utility overwrites, rather than appends, relevant pre-existing sections in the configuration file, such as [LDAPSecAdpt] or [ADSISecAdpt]. To prevent losing important configuration information, back up the file before you begin. The LDAP/ADSI Configuration Utility saves an exact copy of the *modified* configuration file, using the form *filename*.cfg_bak—for example, uagent.cfg_bak. *Do not manually create backup files with this type of name, or they will be overwritten by the utility.*

You can specify a nondefault name for your security adapter by adding a new section using that name. For example, if you specified `LDAPSecAdpt1` as the security adapter name, this will be the value of the `SecAdptName` parameter, and a section named [LDAPSecAdpt1] will be created in the configuration file. In this case, an existing section named [LDAPSecAdpt] will not be modified.

After you have configured one file, you can copy the relevant parameter sections to other configuration files where you want to use the same settings.

For more information, see "Security Adapters and Siebel Dedicated Web Client" on page 139, which also contains a sample section from the configuration file.

Procedure for Configuring LDAP/ADSI Security Adapters

The procedure for configuring LDAP or ADSI security adapters using the LDAP/ADSI Configuration Utility is presented below.

After you start the utility, a series of screens or prompts are displayed. Which items are presented, and how they are presented, depends on how you run the utility and on which selections you have made. As you enter information, choose Next to proceed to the next screen. Choose Previous to return to a previous screen.

To create a detailed log file when running the LDAP/ADSI Configuration Utility, run the utility with the flag -logevents all. The log file is named sw_cfg_util.log. For example, run the following command on Windows:

```
ssincfgw -l enu -f …\admin\secadpt.scm -logevents all
```

NOTE: Except for the `Security Adapter Mode (SecAdptMode)` and `Security Adapter Name (SecAdptName)` parameters, the configuration parameters mentioned in the procedure are defined for the applicable security adapter you are configuring.

To run the LDAP/ADSI Configuration Utility

1. On the Siebel Server machine, change to the *SIEBSRVR_ROOT*\bin directory, where *SIEBSRVR_ROOT* is the installation directory for the Siebel Server.
2. Depending on your Siebel Server platform, do one of the following:
   - In a Microsoft Windows implementation, choose Start > Run, then type:

     ```
     ssincfgw -l enu -f ..\admin\secadpt.scm
     ```

   - In a UNIX implementation, run the utility from the command line. Type:

     ```
     icfg -l enu -f ../admin/secadpt.scm
     ```

3. **Choose Security Adapter Mode.** Select the security adapter mode: LDAP or ADSI. The setting you make will provide a value for the `Security Adapter Mode` parameter.
   - For LDAP, `Security Adapter Mode` is set to `LDAP`.
   - For ADSI, `Security Adapter Mode` is set to `ADSI`.
4. **Security Adapter Name.** Specify the name of the security adapter. You can accept the default name, or specify a nondefault name. The setting you make will provide a value for the `Security Adapter Name` parameter.
   - For LDAP, `Security Adapter Name` defaults to `LDAPSecAdpt`.
   - For ADSI, `Security Adapter Mode` defaults to `ADSISecAdpt`.
5. **Configure Dedicated Web Client?** Specify whether you are configuring for Dedicated Web Clients.
   - If you check Yes, the utility appends relevant sections to the configuration file you specify (such as uagent.cfg for Siebel Call Center), or replaces existing sections. Go to Step 6 on page 107.
   - If you do not check Yes, the utility defines configuration parameters in the Name Server instead (appropriate for Siebel Web Client deployments). You must specify how to apply the configuration settings, and specify server connectivity information. Go to Step 7 on page 107.

   For more information, see "About Configuration for Dedicated Web Clients" on page 105 and "Security Adapters and Siebel Dedicated Web Client" on page 139.

6 **Select Configuration File.** If you are configuring for Dedicated Web Clients, specify the name of the configuration file to modify to include the specified settings. Go to Step 11 on page 107.

CAUTION: Before you specify an existing configuration file, make sure you have backed it up first. For details, see "About Configuration for Dedicated Web Clients" on page 105.

7 **Specify At Which Level to Enable LDAP/ADSI Authentication.** Specify at which level the LDAP/ADSI security adapter configuration should apply:

- **Enterprise.** Configure the LDAP/ADSI security adapter for the Siebel Enterprise Server.
- **Siebel Server.** Configure the LDAP/ADSI security adapter for the Siebel Server.
- **Components on Siebel Server.** Configure the LDAP/ADSI security adapter for an individual AOM component, or for a Synchronization Manager component.

8 Enter server connectivity information:

- **Gateway Name Server Hostname.** The name of the Siebel Gateway Name Server machine. If the Gateway Name Server uses a port other than the default (2320), then also include the port number (following a colon)—in the form *machinename*:*portnumber*.

  NOTE: Do not use port number 2321 as an alternative port for the Gateway Name Server, because it is already used by the SCBroker component.

- **Enterprise Name.** The name of the Siebel Enterprise Server.
- If you specified to configure the Siebel Enterprise, go to Step 11 on page 107.
- If you specified to configure the Siebel Server, or configure components on the Siebel Server, go to Step 9 on page 107.

9 **Siebel Server Name.** Select the Siebel Server you want to apply the security adapter configuration settings to.

- If you specified to configure the Siebel Server, go to Step 11 on page 107.
- If you specified to configure components on the Siebel Server, go to Step 10 on page 107.

10 **Select Components.** Select the individual AOM components or Synchronization Manager to which you want to apply the security adapter configuration settings.

11 Enter configuration information pertaining to directories:

- **Directory Server.** Corresponds to the `ServerName` parameter.
  - For LDAP, this is the name of the directory server (for example, ldap.siebel.com). It is recommended to specify the fully qualified server name, including the domain name.
  - For ADSI, this is either the name of the directory server (for example, adsi.siebel.com) or the domain name only. It is recommended to specify the fully qualified server name, including the domain name. (For domains that contain more than one directory server, specifying a domain name may be useful for maintaining load balance across servers.)
- **Port Number.** The port number used by the LDAP directory server (*LDAP only*). Use port 389 (the default) for standard transmission, or port 636 for secure transmission. (ADS ports are set as part of the directory installation, not as a configuration parameter.) Corresponds to the `Port` parameter.

12 Enter configuration information pertaining to attribute mapping:

- **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.
- **Password Attribute.** The password for the Siebel user ID attribute used by the directory (*LDAP only*). Corresponds to the `PasswordAttributeType` parameter.

13 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, specified in Step 15 on page 108, requires you to have defined the database account attribute.

  The shared database account is handled differently for LDAP and for ADSI environments. For more information, see "Configuring the Shared Database Account" on page 134.

- **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 Directory" on page 138.

14 Configure the application user:

- **Application User Distinguished Name (DN).** The full DN (distinguished name) for the application user stored in the directory. Include quotes when you specify the application user. Corresponds to the `ApplicationUser` parameter.

  In addition to defining the application user here, you must also create the application user in the LDAP/ADS directory. For more information, see "Configuring the Application User" on page 131.

- **Application Password.** The password for the application user stored in the directory. Corresponds to the `ApplicationPassword` parameter. Confirm the password.

15 **Shared Database Account Distinguished Name (DN).** Specify the full DN for the shared database account stored in the directory. Include quotes when you specify the shared database account. Corresponds to the `SharedCredentialsDN` parameter.

Configuring the shared database account also uses the database account attribute you defined in Step 13 on page 108. For more information, see "Configuring the Shared Database Account" on page 134.

16 **Enable Web Single Sign-On.** Specify whether you want to configure Web Single Sign-On (Web SSO). Corresponds to the `SingleSignOn` parameter.

- If you check Yes, then you must specify the shared secret. Go to Step 17 on page 109.
- If you do not check Yes, go to Step 18 on page 109.

For more information about configuring Web SSO, see Chapter 7, "Web Single Sign-On Authentication."

17 **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, which you must add to the file manually.

18 **Propagate Change.** Specify whether you want to configure the ability to propagate changes to the LDAP/ADS directory from a Siebel Dedicated Web Client. Corresponds to the `PropagateChange` parameter.

NOTE: If you specify this option, then you must also set the SecThickClientExtAuthent system preference to `TRUE`.

For more information, see "Security Adapters and Siebel Dedicated Web Client" on page 139.

19 **Checksum.** Specify whether you want to use checksum validation for the security adapter DLL file. Corresponds to the `CRC` parameter.

For more information, see "Configuring Checksum Validation" on page 132.

20 **SSL Database.** Specify the name of the SSL database you are using (*LDAP only*). Corresponds to the `SslDatabase` parameter.

For more information, see "Configuring Secure Communications for Security Adapter" on page 133.

21 **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 "Configuring Password Hashing" on page 125.

22 **Hash User Password.** Specify whether you want to use password hashing for user passwords. Corresponds to the `HashUserPwd` parameter.

- If you checked Yes for *either* Hash User Password or Hash Database Password, then you must specify the hashing algorithm. Go to Step 23 on page 109.
- If you did not check Yes for *either* Hash User Password or Hash Database Password, go to Step 24 on page 109.

23 **Hash Algorithm.** Specify the hashing algorithm to use for database credentials passwords or user passwords. Corresponds to the `HashAlgorithm` parameter.

- Specify either RSASHA1 (RSA SHA-1) or SIEBELHASH. (RSA SHA-1 is required for new customers.)

24 **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 135.

- If you check Yes, then you must specify the Siebel User ID attribute. Go to Step 25 on page 109.
- If you do not check Yes, go to Step 26 on page 109.

25 **Siebel User ID Attribute.** Specify the Siebel User ID attribute for the adapter-defined user name. Corresponds to the `SiebelUsernameAttributeType` parameter.

26 **Base Distinguished Name (DN).** Specify the base distinguished name (DN) in which you are storing your users. Corresponds to the `BaseDN` parameter.

27 Review the settings, and click Finish to apply them.

Setting Up Security Adapter Authentication: A Scenario

This section provides instructions to implement security adapter authentication, in this case for a single Siebel application. The implementation uses either the LDAP security adapter or the ADSI security adapter with one of the supported directories described in *System Requirements and Supported Platforms* on Siebel SupportWeb.

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

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

These instructions implement the following basic configuration:

- The directory is a Siebel-supported LDAP server, or Microsoft ADS.
- The LDAP security adapter or ADSI security adapter is used to communicate between the authentication manager and the directory.
- A user is authenticated by the user's Siebel user ID and a password.

For additional details about configuring security adapter authentication, see also "Security Adapter Deployment Options" on page 130.

For information about special considerations to implementing user authentication, see "User Authentication Issues" on page 289.

If you use a security adapter not provided by Siebel Systems, it must support the Siebel Security Adapter Software Developers Kit, which is described in "Security Adapter SDK" on page 19. You must adapt the applicable parts of the following implementation to your security adapter.

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

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

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

Process of Implementing LDAP/ADSI Authentication

You must perform the following tasks to implement and test your LDAP/ADS directory with a Siebel-provided security adapter.

1. Create a database login. See "Creating a Database Login" on page 111.
2. Set up the attributes for users in the directory. See "Setting Up the LDAP/ADS Directory" on page 111.
3. Create three users in the directory: a regular user, the anonymous user, and the application user. See "Creating Users in the LDAP/ADS Directory" on page 113.
4. Add user records in the Siebel Database corresponding to two users in the directory. See "Adding User Records in the Siebel Database" on page 114.
5. Edit eapps.cfg file parameters. See "Editing Parameters in the eapps.cfg File" on page 115.
6. Edit Name Server parameters using Siebel Server Manager. See "Editing Parameters Using Siebel Server Manager" on page 116.
7. For Siebel Dedicated Web Clients, edit the Siebel application's configuration file parameters. See "Editing Parameters in the Application Configuration File" on page 120.
8. For Siebel Dedicated Web Clients, set a system preference. See "Setting a System Preference for Dedicated Web Clients" on page 121.
9. Restart the Siebel Server and the Web server. See "Restarting Servers" on page 122.
10. Test the implementation. See "Testing the LDAP/ADSI Authentication System" on page 122.

Creating a Database Login

One database login must exist for all users who are authenticated externally. This login must not be assigned to any real person. A seed database login is provided for this purpose when you install your Siebel eBusiness Applications, as described in "Seed Data" on page 311. Its login name is LDAPUSER, and its default password, LDAPUSER, should be changed by an administrator. If this login name is not present, create it.

Setting Up the LDAP/ADS Directory

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

- Authenticates users through the directory.
- Allows self-registration.
- Uses the Siebel user ID as the username.

NOTE: For more information about setting up the directory, review "Requirements for LDAP/ADS Directory" on page 80.

Determine the Base Distinguished Name, a subdirectory in the directory, in which to store users. For details, see the BaseDN parameter description in "Siebel Gateway Name Server Parameters" on page 300.

You cannot distribute the users of a single Siebel application in more than one base DN. However, you can store multiple Siebel 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 in the sample LDAP directories, or in the Users base DN under the domain level in the sample ADS directory.

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

- **Siebel user ID.** Suggested attribute: uid for LDAP, or sAMAccountName for ADS.
- **Database account.** Suggested attribute: dbaccount.
- **Password.** Suggested attribute (*for LDAP only*): userPassword. ADS does not use an attribute to store a user's password.

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

Creating Users in the LDAP/ADS Directory

Create three users in the LDAP/ADS directory, as described in Table 7 on page 113. Specify attribute names, such as uid and userPassword for an LDAP directory, as suggested here. Your entries may vary based on how you assign attributes in "Setting Up the LDAP/ADS Directory" on page 111.

Table 7. Records in the LDAP/ADS Directory

Type of User	Siebel User ID Attribute (uid for LDAP or sAMAccountName for ADS)	Password (userPassword attribute for LDAP or ADS password for ADS)	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. ■ The anonymous user is required even if the application does not allow access by unregistered users. For more information, see "Configuring the Anonymous User" on page 136.	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	Database account is not required for any user record, except the anonymous user.

NOTE: The specific user and password entries are only suggested. You may vary those entries.

This example implements a shared credential. The database account for all users is stored in one object in the directory. In this example, the shared database account is stored in the anonymous user record. The database account must match the database account you reserve for externally authenticated users described in "Creating a Database Login" on page 111. The *P* symbol represents the password in that database account.

NOTE: In a production environment, do not use the anonymous user as the directory object that contains the shared credential. To do so could allow a user with minimum responsibility to log in directly to the directory server and view shared database credentials. Using these database credentials, a user could log in directly to the Siebel Database and see data that he or she does not have the assigned visibility level to see.

For information about formatting requirements for the database account attribute entry, see "Requirements for LDAP/ADS Directory" on page 80.

CAUTION: 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.

Optionally, complete other attribute entries for each user.

Adding User Records in the Siebel Database

You must create a record in the Siebel Database that corresponds to the test user you create in "Creating Users in the LDAP/ADS Directory" on page 113.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in "Seed Users" on page 312. This record must also match the anonymous user you created in "Creating Users in the LDAP/ADS Directory" on page 113.

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 196.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
2. From the application-level menu, choose Navigate > Site Map > Administration - User > Users.
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	Example Entry	Guideline
Last Name		Required. Enter any name.
First Name		Required. Enter any name.
User ID	TESTUSER	Required. This entry must match the uid (LDAP) or sAMAccountName (ADS) attribute value for the test user in the directory. If you used another attribute, it must match that value.
Responsibility		Required. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. If an appropriate seed responsibility does not exist, such as for a Siebel employee application, assign an appropriate responsibility that you create.
New Responsibility		Optional. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. This responsibility is automatically assigned to new users created by this test user.

5 Verify that the seed data user record exists for anonymous users of the Siebel application you implement, as described in "Seed Users" on page 312.

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 312. You can complete other fields, but they are not required.

Editing Parameters in the eapps.cfg File

Provide the parameter values in the eapps.cfg file, as indicated by the guidelines in Table 8 on page 116.

For more information about editing eapps.cfg parameters and about the purposes for the parameters, see "Parameters in the eapps.cfg File" on page 295.

Table 8. 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.
The section particular to your application, such as one of these: [/eservice] [/callcenter]	AnonUserName	Enter the user ID of the seed data user record provided for the application that you implement, or of the user record you create for the anonymous user. This entry also matches the uid (LDAP) or sAMAccountName (ADS) entry for the anonymous user record in the directory. For example, enter GUESTCST for Siebel eService.
	AnonPassword	Enter the password you created in the directory for the anonymous user. **NOTE:** 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 LDAP/ADSI Configuration Utility. See "Managing Encrypted Passwords in the eapps.cfg File" on page 34.
	ProtectedVirtualDirectory	If this parameter is present, comment it out with a semicolon at the beginning of the line.

Editing Parameters Using Siebel Server Manager

Several security-related configuration parameters you use for configuring an LDAP or ADSI security adapter are defined in the Siebel Gateway Name Server. You configure these parameters using Siebel Server Manager.

Set each parameter as described in the subsection where it is listed, following any guidelines provided.

For more information about these parameters, see "Siebel Gateway Name Server Parameters" on page 300.

Parameters for Enterprise, Siebel Servers, or Components

Table 9 on page 117 lists 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).

For this scenario, set the parameters for the applicable AOM component, such as for Siebel Call Center or Siebel eService.

NOTE: You can modify these configuration parameters using Siebel Server Manager, or you can do so using the LDAP/ADSI Configuration Utility. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 103.

Table 9. 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

Table 10 on page 117 lists parameters you would set on the AOM.

Table 10. Siebel Gateway Name Server Parameters (for AOM)

Subsystem	Parameter	Guideline
Object Manager	OM - Proxy Employee	Enter PROXYE.
	OM - Username BC Field	For this scenario, leave this parameter empty.

Parameters for Security Adapter (Profile/Named Subsystem)

Table 11 on page 118 lists parameters you would set for the enterprise profile (named subsystem) for the specific security adapter you are configuring.

For this scenario, you 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`.

NOTE: You can modify these configuration parameters using Siebel Server Manager, or you can do so using the LDAP/ADSI Configuration Utility. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 103.

Table 11. Siebel Gateway Name Server Parameters (for Enterprise Profile/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 machine on which the LDAP or ADS server runs.
`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 ADS directory level, not as a configuration parameter.

Table 11. Siebel Gateway Name Server Parameters (for Enterprise Profile/Named Subsystem)

Parameter	Guideline
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 (including quotes): "ou=People, o=*domainname*" In the example, "o" denotes "organization" and is the domain name system (DNS) name for this server, such as *machine.company.com*. "ou" denotes "organization unit" and is the name of a subdirectory in which users are stored. ADSI example entry (including quotes): "CN=Users, DC=*machinename*, DC=*domainname*, DC=com" Domain Controller (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for user objects in the directory. Therefore, adjust the number of DC and CN 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.
Password Attribute Type (PasswordAttributeType)	The LDAP entry *must* be userPassword. If a different value is specified, the LDAP security adapter will not function properly. ADS does not store the password in an attribute, so this parameter is not used with the ADSI security adapter.
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.

Table 11. Siebel Gateway Name Server Parameters (for Enterprise Profile/Named Subsystem)

Parameter	Guideline
Application User (ApplicationUser)	LDAP example entry (including quotes): "uid=APPUSER, ou=People, o=*domainname*" ADSI example entry (including quotes): "CN=APPUSER, CN=Users, DC=*machinename*, 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.
Application Password (ApplicationPassword)	For LDAP and ADSI, enter APPUSERPW or the password assigned to the application user.
Shared Credentials DN (SharedCredentialsDN)	■ LDAP example entry (including quotes): "uid=anonymous user User ID, ou=People, o=*domainname*" For example: "uid=GUESTCST, ou=People, o=siebel.com" ■ ADSI example entry (including quotes): "CN=anonymous user User ID, CN=Users, DC=*machinename*, DC=*domainname*, DC=com" For example: "CN=GUESTCST, CN=Users, DC=qa1, DC=siebel, DC=com"

Editing Parameters in the Application Configuration File

Provide parameter values, as indicated by the guidelines in Table 12 on page 121, in the configuration file for the Siebel application you are implementing.

For a configuration file on the Siebel Server, some parameters also apply to the AOM and thus to Siebel Web Client: those defined in the [SWE] section.

Parameters in sections that directly pertain to security adapters apply, in this context, only to Siebel Dedicated Web Client. These parameters are counterparts to the Name Server parameters listed in Table 9 on page 117 and Table 11 on page 118.

NOTE: You can use a text editor to make changes to an application configuration file, or you can do so using the LDAP/ADSI Configuration Utility. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 103.

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 306. For a list of Siebel application configuration files, see *Siebel System Administration Guide*.

Table 12. Siebel Application Configuration File Parameters

Section	Parameter	Guidelines for Siebel LDAP and ADSI Security Adapters
[SWE]	AllowAnonUsers	Enter TRUE for LDAP or ADSI.
	SecureLogin	Enter TRUE or FALSE. If TRUE, the login request (HTTP POST) from the login form is transmitted using HTTPS. For information about other requirements for secure login, see the secure login topic in "Login Features" on page 163.
[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 "Editing Parameters Using Siebel Server Manager" on page 116 or Appendix B, "Configuration Parameters Related to Authentication."	
[ADSISecAdpt]	For parameters, see "Editing Parameters Using Siebel Server Manager" on page 116 or Appendix B, "Configuration Parameters Related to Authentication."	

Setting a System Preference for Dedicated Web Clients

If you are configuring LDAP or ADSI authentication for Siebel Dedicated Web Client, also set the system preference shown in Table 13 on page 122.

For more information about setting system preferences, see "System Preference" on page 310.

Table 13. System Preference

System Preference	Example Entry	Guideline
SecThickClientExtAuthent	FALSE	Set this system preference to TRUE to allow Dedicated Web Clients to use a security adapter.

Restarting Servers

You must stop and restart the following Windows services on the Web server machine to activate changes you make to configuration parameters.

- **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*.

Testing the LDAP/ADSI Authentication System

The following tests confirm that the Siebel-provided security adapter, your LDAP or ADS 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.

Figure 7 on page 123 shows the home page for Siebel eService, with the embedded login form.

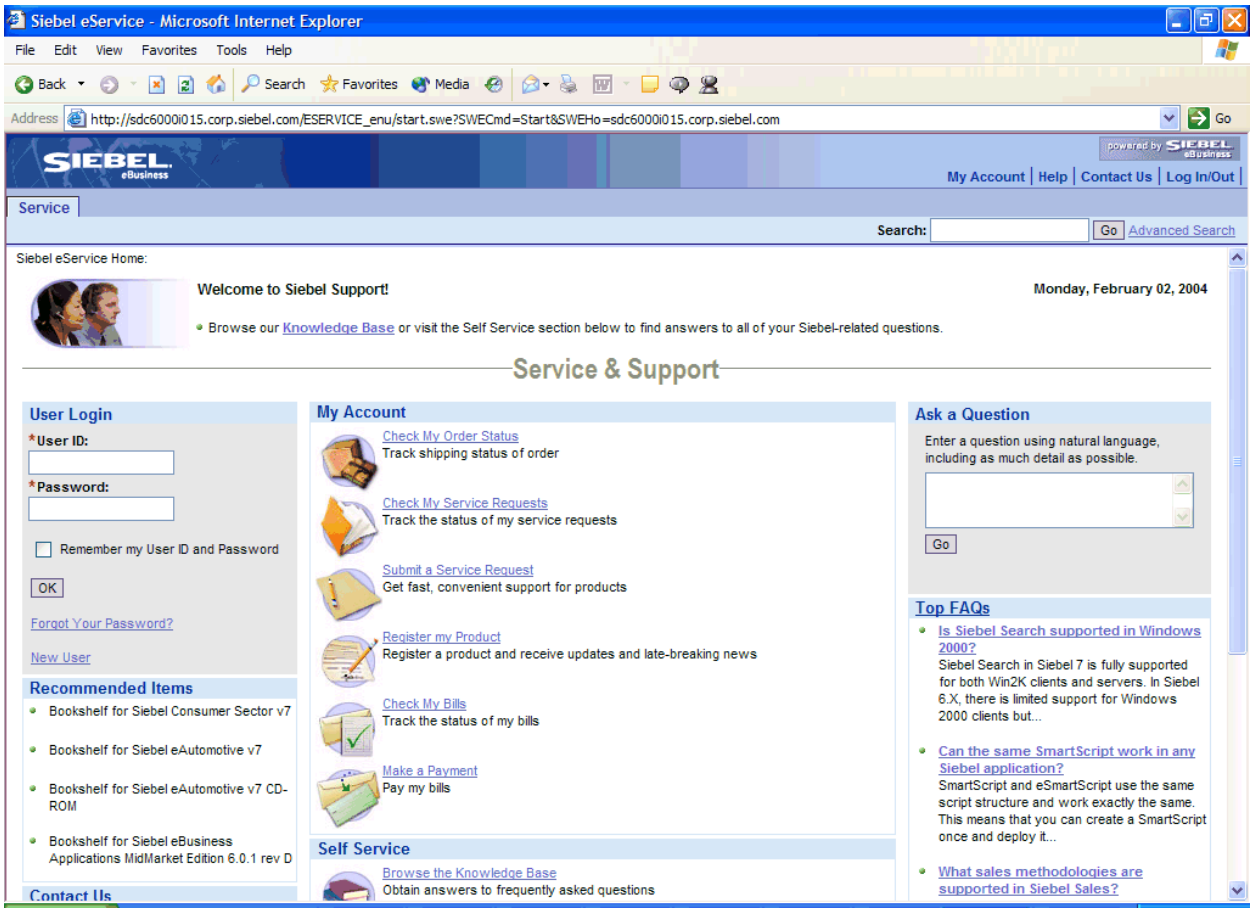


Figure 7. Login Form Embedded in Siebel eService Home Page

To test your LDAP/ADSI authentication system

1 In a Web browser, enter the URL to your Siebel application, such as:

`http://www.mycompany.com/eservice`

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

The Siebel eService login form in Figure 7 on page 123 includes user ID and password fields.

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 may 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 123 to access the login page. If a New User button is present, click it.

   NOTE: If a New User button is not present, your 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 may or may 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/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. 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 124.

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

Configuring Password Hashing

User passwords or database credentials passwords can be hashed for greater security.

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/ADS. 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.

Password hashing is used in the following contexts:

- **User password hashing.** When you are using security adapter authentication (including database, LDAP/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.

- **Database credentials password hashing.** When you are using security adapter authentication other than database authentication (including LDAP/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 external directory, such as LDAP or ADS. This password is hashed during login.

Password hashing is a critical tool for preventing unauthorized users from bypassing Siebel 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.

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.

For more information about configuring each type of password hashing, see "Configuring User and Credentials Password Hashing" on page 128.

Siebel Systems provides a password hashing utility called hashpwd.exe. The default hashing algorithm is RSA SHA-1. For example, using the default option rsasha1 for the hashpwd.exe utility, `siebel` is hashed as `6sxr7MWJDyNiMfW2f0cyo+gOVcs=`. For information about running hashpwd.exe, see "Running the Password Hashing Utility" on page 129.

NOTE: New customers are *required* to use RSA-SHA1, and existing customers are strongly recommended to migrate to RSA-SHA1 promptly.

Configuration parameters for all Siebel-provided security adapters, and for custom security adapters you implement, specify the password hashing settings in effect. For each security adapter, parameters specify whether password hashing should be used for user passwords and/or credentials passwords, and, if so, which hashing algorithm to use.

For database authentication, the relevant parameters are specified for a data source referenced from the database security adapter, rather than specified directory for the security adapter.

For existing customers, the Siebel proprietary hashing algorithm (the mangle algorithm, formerly available through the utility encrypt.exe) is still available as an option for the hashpwd.exe utility. This option, called siebelhash, can also be specified as the value for the applicable configuration parameter. These parameters include `HashAlgorithm` for LDAP/ADSI security adapters and `DSHashAlgorithm` for data sources (used with database authentication).

For more information about parameters for password hashing, see Appendix B, "Configuration Parameters Related to Authentication."

For more information about upgrading your Siebel applications, see *Upgrade Guide* for the operating system you are using.

NOTE: For information about managing encrypted passwords in the eapps.cfg file, see "Managing Encrypted Passwords in the eapps.cfg File" on page 34. The password encryption mechanism described there is unrelated to the password hashing mechanism described in this section.

Login Scenario for Password Hashing

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/ADSI authentication environment:
   a. The authentication manager passes the user credentials, including the hashed password, to the LDAP/ADSI security adapter.
   b. The LDAP/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 application session for the user.

Usage Guidelines for Password Hashing

Guidelines for using password hashing for Siebel applications include the following:

- The password hashing utility, hashpwd.exe, does not automatically store hashed passwords in the Siebel Database or LDAP/ADS 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, it is set as the valid password for the database account.
  - In an LDAP/ADSI authentication environment, it 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 should be stored in unhashed form, because such passwords will be hashed during the authentication process.
- With database authentication, Siebel Server components that log into the database must use the hashed password value stored in the Siebel Database. Otherwise, component login will fail.

  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 will fail.
- 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 77 and "Siebel Application Configuration File Parameters" on page 306.

Configuring User and Credentials Password Hashing

Use the procedures below to implement password hashing for user passwords or for database credentials.

User passwords and database credentials account passwords may be stored in the locations described in "Usage Guidelines for Password Hashing" on page 127, according to the authentication method you are using.

NOTE: Some steps in the procedures below, such as those for setting configuration parameter values using Siebel Server Manager, may alternatively be accomplished by using the LDAP/ADSI Configuration Utility. For details, see "Using the LDAP/ADSI Configuration Utility" on page 103.

Configuring User Password Hashing

Use the procedure below to configure user password hashing.

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 129.
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/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 to each user the username and the clear-text password for logging in.

Configuring Database Credentials Password Hashing

Use the procedure below to configure database credentials password hashing.

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 129.
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/ADS 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 LDAP/ADS Directory" on page 80.
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

To hash passwords, you run the utility hashpwd.exe, which is located in the directory *SIEBSRVR_ROOT*\bin or *SIEBEL_CLIENT_ROOT*/bin, representing Siebel Server or Siebel Mobile/ Dedicated Web Client installation directories.

Hashed passwords can then be stored in the directory or database for use when a password is hashed upon login, and compared to the stored hashed version.

NOTE: For important information about the password hashing options mentioned below, see "Configuring Password Hashing" on page 125.

Hashing Passwords Using the RSA SHA-1 Algorithm

The default password hashing algorithm is RSA SHA-1. For this algorithm, run the utility using one of the following syntaxes:

```
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 may be named passwords.txt), and then specify the filename using the following syntax:

```
hashpwd @password_file_name
```

Hashing Passwords Using the siebelhash Algorithm

The Siebel proprietary password hashing algorithm (formerly available using the utility encrypt.exe) is also available. For this algorithm, run the utility using 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 may be named passwords.txt), and then specify the filename using the following syntax:

```
hashpwd -a siebelhash @password_file_name
```

Security Adapter Deployment Options

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

- **Application user.** A designated entry in the directory is the only user with search and write privileges to the directory. You maintain an unexposed password for the application user in the directory, while an encrypted version of the password is used in other phases of the authentication process. 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.

  For more information, see "Configuring the Application User" on page 131.

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

  For more information, see "Configuring Checksum Validation" on page 132.

- **Secure communications for security adapters.** You can use Secure Sockets Layer (SSL) to transmit data between the Siebel-provided security adapter and the LDAP/ADS directory.

  For more information, see "Configuring Secure Communications for Security Adapter" on page 133.

- **Shared database account.** A designated entry in the directory contains a database account that is shared by other users.

  For more information, see "Configuring the Shared Database Account" on page 134.

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

  For more information, see "Configuring Adapter-Defined User Name" on page 135.

- **Roles defined in directory.** You can choose to store users' Siebel responsibilities as roles in a directory attribute instead of in the Siebel Database.

  For more information, see "Configuring Roles Defined in Directory" on page 138.

Configuring the Application User

The application user *must* be used 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 a user that you define in the directory with the following qualities:

- This user provides the initial binding of the LDAP or Active Directory Server with the AOM when a user requests the login page. Otherwise, binding defaults to the anonymous user.
- 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.
- Permissions for the application user should be defined at the organization level (for example, OU for LDAP).

NOTE: The application user is not an actual user who logs into an application, but rather a special user to handle access to the directory. You must implement an 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. The password should be entered in unencrypted form. If you implement an ADS directory, you specify the password using ADS user management tools, not as an attribute.

  NOTE: 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.

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

  For example, `ApplicationUser` may be set as in the following example:

  ```
  ApplicationUser = "uid=APPUSER, ou=people, o=siebel.com"
  ```

- `ApplicationPassword` = application user password (unencrypted)

For Dedicated Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

For information about setting Siebel configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

Application User and Password Expiration Policies

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

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 Features" on page 163.

Configuring Checksum Validation

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

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

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

Checksum validation supports the following principles:

- A 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.

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, the following command:

   `checksum -f sscfldap.dll`

   would return something similar to:

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

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 133.

NOTE: 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 whenever you upgrade your Siebel applications.

(For previous releases, the CRC checksum value was set using the Security Adapter CRC system preference, rather than a configuration parameter.)

For information about setting Siebel configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

Configuring Secure Communications for Security Adapter

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.

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 GSK iKeyMan, contains a certificate for the certificate authority that is used by the LDAP server.

  For information about generating the SSL database file for an LDAP authentication environment, see "Generating a CMS File Using IBM GSK iKeyMan" on page 99.

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.

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 306.

Configuring 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

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

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

The shared database account option is used differently by LDAP and ADSI:

- For LDAP, if the shared database account is specified, then database credentials are always retrieved from that account.
- 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.

To configure a shared database account

1. Create a database account to be shared by all users who log into a given Siebel application.

2 Create a designated entry in the directory, and enter the username and password parameters for the common database account in one of that entry's attributes, such as the dbaccount attribute. You may need to create this attribute.

   For information about formatting a directory attribute that contains the database account, see "Requirements for LDAP/ADS Directory" on page 80.

3 For each security adapter (such as LDAPSecAdpt) that implements this shared database account, define the following parameter values:

   - `CredentialsAttributeType` = attribute in which the database account is stored in the directory, such as dbaccount
   - `SharedCredentialsDN` = the distinguished name (including quotes) for the designated entry, such as "uid=SHAREDENTRY, ou=People, o=companyname.com"

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 306.

Configuring Adapter-Defined User Name

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

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

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

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

The `UsernameAttributeType` 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 work phone number.

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:
   - `UseAdapterUsername = TRUE`
   - `SiebelUserNameAttributeType` = attribute in which you store the Siebel user ID, such as `uid` (LDAP) or `sAMAccountName` (ADSI).
   - `UsernameAttributeType` = attribute in which you store the adapter-defined user name, such as `telephonenumber`.
2. Determine the field on the User business component that is used to populate the attribute in the directory that contains the adapter-defined user name.

   The AOM parameter to be populated is `OM - Username BC Field`.

   For information about working with Siebel business components, see *Configuring Siebel eBusiness 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: 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/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/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.

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

If you use one anonymous user for most or all of your applications, you may want to define the anonymous user at the defaults level, which requires less administration. To set a default value for a parameter, such as `AnonUserName` and `AnonPassword`, include it in the [defaults] section of the eapps.cfg file.

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

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. 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.

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

For information about working with views in Siebel applications, see *Configuring Siebel eBusiness Applications*.

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

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

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

NOTE: The anonymous user session caches information; therefore, any changes to data such as catalogs, for example, will not be updated until either the user logs in or the anonymous user session is restarted.

In addition to the `AllowAnonUsers` parameter, you can set the `LoginView` parameter. This parameter determines what view appears for login (as opposed to the default Web login page). The `AllowAnonUsers` parameter must be `TRUE` for the `LoginView` parameter to be recognized.

The `LoginView` parameter does not appear in the [SWE] section of an application's configuration file by default. It must be added.

For information about setting Siebel configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

Configuring Roles Defined in Directory

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

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

Responsibilities assigned to each user in Siebel applications provide users with access to particular views. Responsibilities are created in the Siebel application and are stored in the Siebel Database. One or more responsibilities are typically associated with each user in the Administration - Application screen.

Roles in the LDAP/ADS directory are another means of associating Siebel responsibilities with users. Roles are useful for managing large collections of responsibilities. A user has access to all the views associated with all the responsibilities that are directly or indirectly associated with the user.

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

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

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

You can configure Siebel-provided security adapters to retrieve roles for a user from the directory. For each Siebel application that uses roles, set the following parameter value 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 configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

Security Adapters and Siebel Dedicated Web Client

The Siebel Dedicated Web Client relocates business logic from the Siebel Server to the client. The authentication architecture for the Dedicated 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

When you implement security adapter authentication for Siebel Dedicated 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 section.
- Authentication-related configuration parameters stored in application configuration files on client computers, or stored in remote configuration files, should generally contain the same values as the corresponding parameters in the Name Server (for Siebel Web Client users). Distribute the appropriate configuration files to all Siebel Dedicated Web Client users.

  For information about setting parameters in Siebel application configuration files on the Siebel Dedicated Web Client, see "Siebel Application Configuration File Parameters" on page 306.
- 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 132.
- 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 Dedicated Web Client users.
  - Propagation of user administration changes from the Siebel Dedicated Web Client to an external directory such as LDAP or ADS. (For example, if a user changes his or her password in the Dedicated Web Client, the password change will also be populated to the directory.)

  For more information, see "Siebel Application Configuration File Parameters" on page 306 and "System Preference" on page 310.

- In some environments, you may want to rely on the data server itself to determine whether to allow Siebel Dedicated 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).

  This 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 should be allowed to log into the database.

  You can use `IntegratedSecurity = TRUE` with the database security adapter. See also "Configuring Database Authentication" on page 77.

  NOTE: `IntegratedSecurity` is supported for Oracle and Microsoft SQL Server databases only. For additional information, refer to your third-party documentation. For Oracle, refer to the OPS$ and REMOTE_OS_AUTHENT features. For Microsoft SQL Server, refer to Integrated Security.

For more information about the Siebel Dedicated Web Client, see the *Siebel Installation Guide* for the operating system you are using and the *Siebel System Administration Guide*.

Sample LDAP Section in Configuration File

The following is an example of LDAP configuration information generated by the LDAP/ADSI Configuration Utility when you configure an LDAP security adapter for Dedicated Web Clients. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 103.

For information about setting Siebel configuration parameters, see "Siebel Application Configuration File Parameters" on page 306.

```
[LDAPSecAdpt]
SecAdptDllName = sscfldap
ServerName = ldapserver.siebel.com
Port = 636
BaseDN = "ou=people, o=xyz.com"
SharedCredentialsDN = "uid=HKIM, ou=people, o=Siebel.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 Dedicated Web Client

For the Siebel Dedicated 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 Dedicated 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 section, 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 Dedicated 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 Dedicated 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 section 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.

To synchronize the local database

1. The Siebel remote user connects to the local database on their client computer and makes transaction modifications. To do this:
   a. Launch the Siebel icon on the client computer, then enter a user ID and password.
   b. In the Connect To parameter, choose Local.

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

      The Siebel application appears in the Web browser and the user navigates through the application.
   c. Modify data, as appropriate (insert, update, or delete operations).
2. Later, the user decides to synchronize the local database changes and download updates from the Siebel Remote server. To do this:
   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.
3. When the Siebel application appears in the Web browser, the user chooses File > Synchronize Database.

   The user is now accessing the Siebel Remote server for synchronization, and is subject to authentication.
4. 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*.

`Authentication Method` may 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 may be authenticated against the database or against an LDAP/ADS directory. Password hashing is subject to the configuration of this security adapter.

  NOTE: The `Security Adapter Mode` and `Security Adapter Name` parameters may 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 76 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 generally no longer recommended.*)
- **AppServer.** Verifies that the password is the same as the user's operating system password on the Siebel Server machine. (*This option is generally 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 applications support this mode of authentication by providing an interface that allows the third party to pass user information to a Siebel application. Once authenticated by the third party, a user does not have to explicitly log into the Siebel application. Web SSO allows you to deploy Siebel applications into existing Web sites or portals.

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

NOTE: Web SSO authentication does not apply to the Siebel Mobile Web Client.

Web SSO Authentication Process

The steps in the Web SSO authentication process shown are:

1. The user enters credentials at the Web site that are passed to the Web server. A third-party authentication client on the Web server passes the user credentials to the third-party authentication service. The third-party authentication service verifies the user credentials and passes the authenticated user's username to the Siebel Web Server Extension (SWSE).
2. The SWSE passes the authenticated user's username 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.
4. The Application Object Manager (AOM) uses the returned credentials to connect the user to the database and to identify the user.

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 eBusiness 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)

Your Siebel applications may require configuration changes to hide such functionality. For more information, see *Configuring Siebel eBusiness Applications*.

NOTE: Because Siebel application 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 choosing File > Close or by clicking X in the top-right corner of the window. The AOM terminates the task (thread) for the user's session when the session timeout has been reached. 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 295.

Web SSO Implementation Considerations

Following are some implementation considerations for a Web SSO strategy:

- Users are authenticated independently of Siebel applications, such as through a third-party authentication service or through the Web server.
- You must synchronize users in the authentication system and users in the Siebel Database at the Web site level.
- You must configure user administration functionality, such as self-registration, at the Web site level.
- A delegated administrator can add users to the Siebel Database, but not to the authentication system.

For more information about integrating third-party authentication software with Siebel eBusiness Applications, see Siebel SupportWeb or contact the Siebel Alliance Group.

Implementing Web SSO Authentication

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

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

In a Web SSO environment, you must also provide your authentication service and any required components, such as an authentication client component.

NOTE: For a particular Siebel application, when users connect from the Siebel Dedicated Web Client to the server database, the authentication mechanism must be the same as that used for Siebel Web Client users. This mechanism could be database authentication or a supported external authentication strategy, such as LDAP or ADSI. When connecting to the local database using Siebel Mobile Web Client, however, mobile users must use local database authentication.

For information about authentication options for local database synchronization for mobile users, see *Siebel Remote and Replication Manager Administration Guide*.

For an overview of tasks involved in setting up Web SSO, see "Setting Up Web SSO: A Scenario" on page 147.

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 "User Specification Source" on page 160.
- **Digital certificate authentication.** Siebel Systems supports 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 159.
- In addition, many options identified in "Security Adapter Deployment Options" on page 130 can be implemented for Web SSO.

For information about troubleshooting user authentication, see "User Authentication Issues" on page 289.

Setting Up Web SSO: A Scenario

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

Make sure you implement Web SSO in a development environment before deploying it in a production environment. You can repeat the appropriate instructions here to provide Web SSO access to additional Siebel applications.

These instructions implement the following basic (example) configuration:

- IIS Web server is deployed on Windows 2000. The IIS Web server functions as the authentication service.
- An Active Directory Server (ADS) and the Web server are installed on different machines. ADS serves 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 ADS.

- The Siebel Server, which includes the AOMs representing the deployment of your Siebel Web-based applications.

  NOTE: The instructions in this section describe a minimal, baseline configuration. In a production environment, it is not recommended to install the Siebel Server on the same machine as the Web server.

If you use a non-Siebel security adapter, it must support the Siebel Security Adapter Software Developers Kit, described in "Security Adapter SDK" on page 19. You must adapt the applicable parts of the implementation to your security adapter.

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

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

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

Process of Implementing Web SSO

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

1. Create protected virtual directories for Siebel applications on the Web server machine. See "Creating Protected Virtual Directories" on page 149.
2. Set up third-party Web SSO authentication.
3. Set up a directory from which database accounts and the user's Siebel user ID can be retrieved.
4. Create a database login for users who are authenticated externally. See "Creating a Database Login" on page 150.
5. Set up the ADS. See "Setting Up the Active Directory Server" on page 151.
6. Create three users in the ADS directory: a regular user, the anonymous user, and the application user. See "Creating Users in the Directory" on page 152.
7. Add user records in the Siebel Database corresponding to the regular user and the anonymous user in the directory. See "Adding User Records in the Siebel Database" on page 153.
8. Edit eapps.cfg file parameters. See "Editing Parameters in the eapps.cfg File" on page 154.
9. For Dedicated Web Clients, edit the Siebel application's configuration file parameters. See "Editing Parameters in the Application Configuration File" on page 158.
10. Edit Siebel Gateway Name Server parameters. See "Editing Name Server Parameters" on page 156.
11. Restart the Siebel Server and the Web server. See "Restarting Servers" on page 158.
12. Test the implementation. See "Testing Web SSO Authentication" on page 158.

Creating Protected Virtual Directories

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

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

- Create the virtual directory.
- Specify to the Web server a particular DLL file that allows the SWSE to communicate with the Web server.

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

NOTE: Optionally, instead of creating a new virtual directory, you can modify an existing virtual directory.

To create a virtual directory on Microsoft Internet Information Server

1. Start the Internet Service Manager. Choose Programs > Administrative Tools > Internet Service Manager.
2. In the Internet Service Manager explorer, right-click the default Web site, and then choose New > Virtual directory.

   The New Virtual Directory wizard appears.
3. Enter a virtual directory name for a Siebel application, and then click Next. For example, enter `p_eservice` as a virtual directory for Siebel eService.
4. Enter the full path to the *SWEAPP_ROOT*\public directory, and 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.

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.

   The Add/Edit Application Extension Mapping dialog box appears.

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 Basic Authentication check box, and uncheck all others.

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

    The Directory Security tab in the Properties dialog box appears.

11. Click Apply, and then click OK.

Creating a Database Login

One database login must exist for all users who are authenticated externally. This login must not be assigned to any real person. A seed database login is provided for this purpose when you install your Siebel eBusiness Applications, as described in "Seed Data" on page 311. Its login name is LDAPUSER, and its default password, LDAPUSER, should be changed by an administrator. If this login name is not present, create it.

Setting Up the Active Directory Server

In this scenario, Active Directory Server (ADS) performs two functions that might be handled by two separate entities in other Web SSO implementations.

- Users are authenticated through the ADS performing its function as the IIS Web server directory.
- ADS 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 ADS as the directory which provides the user IDs and the Siebel Database account for authenticated users.
- Configure the IIS Web server to authenticate against the ADS.

Configuring the Active Directory Server

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

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

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

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

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

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

Configuring the IIS Web Server

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

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

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

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

Creating Users in the Directory

Create three users in the directory as described in Table 14 on page 152. The attribute names, sAMAccountName and Password, are those suggested in this example. Your entries may vary, depending on how you make attribute assignments in "Setting Up the Active Directory Server" on page 151.

Table 14. 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 311, 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 "Creating a Database Login" on page 150. *P* represents the password in that database account. For information about formatting the database account attribute entry, see "Requirements for LDAP/ADS Directory" on page 80.

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 needed.

Adding User Records in the Siebel Database

You must create a record in the Siebel Database that corresponds to the test user you create in "Creating Users in the Directory" on page 152.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in Table 27 on page 312. This record must also match the anonymous user you create in "Creating Users in the Directory" on page 152.

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

For purposes of confirming connectivity to the database, you can use the following procedure to add the test user for any Siebel application. However, if you are configuring a Siebel employee or partner application, and you want the user to be an employee or partner user, complete with position, division, and organization, see the instructions for adding such users in "Internal Administration of Users" on page 196.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
2. From the application-level menu, choose Navigate > Site Map > Administration - User > Users.
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	Example Entry	Guideline
Last Name		Required. Enter any name.
First Name		Required. Enter any name.
User ID	TESTUSER	Required. This entry must match the sAMAccountName attribute value for the test user in the directory. If you used another attribute instead of sAMAccountName, it must match that value.
Responsibility		Required. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for Siebel eService. If an appropriate seed responsibility does not exist, such as for a Siebel employee application, assign an appropriate responsibility that you create.
New Responsibility		Optional. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for Siebel eService. This responsibility is automatically assigned to new users created by this test user.

5 Verify that the seed data user record exists for anonymous users of the Siebel application you implement, as described in Table 27 on page 312.

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 27 on page 312. You can complete other fields, but they are not required.

Editing Parameters in the eapps.cfg File

Provide parameter values in the eapps.cfg file, as indicated by the guidelines in Table 15 on page 154.

For information about editing eapps.cfg parameters and about the purposes for the parameters, see "Parameters in the eapps.cfg File" on page 295.

Table 15. Parameter Values in eapps.cfg File

Section	Parameter	Example Entry	Guideline
[defaults]			The values of the parameters in this section are overridden by the parameter values you set in the sections for individual applications. For this scenario, you set Web SSO and related parameters in application-specific sections.

Table 15. Parameter Values in eapps.cfg File

Section	Parameter	Example Entry	Guideline
The section particular to your application, such as one of these: [/eservice] [/callcenter]	AnonUserName		Enter the user ID of the seed data User record provided for the application that you implement or of the User record you create for the anonymous user. This entry also matches the sAMAccountName entry for the anonymous user record in the directory. For example, enter GUESTCST for Siebel eService.
	AnonPassword		Enter the password you created in the directory for the anonymous user. **NOTE:** 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 34.
	SingleSignOn	TRUE	
	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.

Table 15. Parameter Values in eapps.cfg File

Section	Parameter	Example Entry	Guideline
	UserSpec	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	Server	REMOTE_USER is a Web server variable.
	ProtectedVirtualDirectory		Generally, you would enter the name of the protected virtual directory that you created in "Creating Protected Virtual Directories" on page 149. **NOTE:** It is recommended that this parameter should always be used in a Web SSO implementation.
[swe]	IntegratedDomainAuth	TRUE	Set to TRUE for Windows Integrated Authentication. Parameter is FALSE by default.

Editing Name Server Parameters

Set each Name Server parameter listed in Table 16 on page 156 for the component that corresponds to the Object Manager for the application you are implementing, such as Call Center Object Manager or eService Object Manager. Set the parameters at the component level and follow the guidelines provided in the table.

For information about setting Name Server parameters and the purposes for the parameters, see "Siebel Gateway Name Server Parameters" on page 300.

Table 16. Name Server Parameters

Subsystem	Parameter	Guideline
Object Manager	OM - Proxy Employee	Enter PROXYE.
	OM - Username BC Field	Leave empty.

Table 16. 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 may 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 may 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.	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

Provide the parameter values as indicated by the guidelines in Table 17 on page 158 in the configuration file for the Siebel application you are implementing. For a list of Siebel application configuration files, see *Siebel System Administration Guide*.

For information about editing an application's configuration file and about the purposes for the parameters, see "Siebel Application Configuration File Parameters" on page 306.

Table 17. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for ADSI Security Adapter
[SWE]	AllowAnonUsers	Enter TRUE. **NOTE:** If you do not set this parameter to TRUE, browser looping behavior may occur.
	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 the secure login topic in "Login Features" on page 163.

Restarting Servers

You must stop and restart the following Windows services on the Web server machine to activate changes you make to AOM configuration.

- **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*.

Testing Web SSO Authentication

The following tests 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 the Siebel application without requiring an additional login.

To test your Web SSO authentication

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

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

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

   You should gain access to the Web site.

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

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

Digital Certificate Authentication

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

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

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

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

To implement X.509 digital certificate authentication, you must perform the tasks for implementing Web SSO authentication, as described in "Implementing Web SSO Authentication" on page 146, with the following specific guidelines:

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

Parameter	Comment
SingleSignOn = TRUE	
TrustToken = HELLO	
ClientCertificate = TRUE	
UserSpec = CERT_SUBJECT or REMOTE_USER	For client authentication on Windows and AIX, use CERT_SUBJECT. For other UNIX platforms, use REMOTE_USER.

Parameter	Comment
SubUserSpec = CN	This parameter value tells the application to extract the username from the certificate name. For the Sun ONE Web Server, this setting is ignored.
UserSpecSource = Server	

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

```
[SWE]
SecureBrowse = FALSE
```

- For each security adapter (such as LDAPSecAdpt) that is to support certificate-based authentication, define the following parameter values:

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

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

User Specification Source

This option can be implemented in the following authentication strategy:

- Web SSO authentication

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.

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

To specify the source of the username

- In the eapps.cfg file, provide the following parameter values in either the [defaults] section or the section for each individual application, such as, for example, [/eservice].
  - UserSpec = name of the variable. For example: REMOTE_USER, if UserSpecSource is set to Server. If UserSpecSource is set to Header, the value of UserSpec will be the variable that will be passed into the HTTP header; the name of the variable should 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 IIS Web server, first configure the IIS Web server to allow anonymous access. You make this security setting for the default Web site in the IIS Service Manager.

For information about setting parameters in the eapps.cfg file, see "Parameters in the eapps.cfg File" on page 295.

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 Secure Views

You can require URLs to use the HTTPS protocol for specific views in your Siebel application.

NOTE: The ability to selectively specify secure views applies to standard interactivity applications only, not high interactivity applications.

The following factors determine whether the Siebel Web Engine verifies that requests for a view use the HTTPS protocol:

- The value (TRUE or FALSE) of the view's Secure attribute. For information about the Secure attribute for a view, see *Configuring Siebel eBusiness Applications*.
- The value (TRUE or FALSE) of the SecureBrowse parameter, located in the [SWE] section of the application's configuration file, such as siebel.cfg.
  - If SecureBrowse is set to TRUE, then HTTPS is required for all views in the entire application, regardless of how the Secure attribute is set for individual views.
  - If SecureBrowse is set to FALSE, then HTTP is used for all views in the entire application, except for those views for which the Secure attribute is set to TRUE. Secure views require HTTPS.

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

- 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. Set the value of SecureBrowse to TRUE.
- Your Web server must be configured to support HTTPS.
- The Sun ONE Web Server does not support switching between secure and nonsecure views in Siebel applications. If you are using the Sun ONE Web Server, set the value of SecureBrowse to TRUE.

Login Features

This section describes features and considerations associated with user login to Siebel applications.

A login page or a login form embedded in a Siebel application page is the means by which user credentials are collected. Figure 8 on page 164 shows the Siebel eService home page with the login form embedded in it.

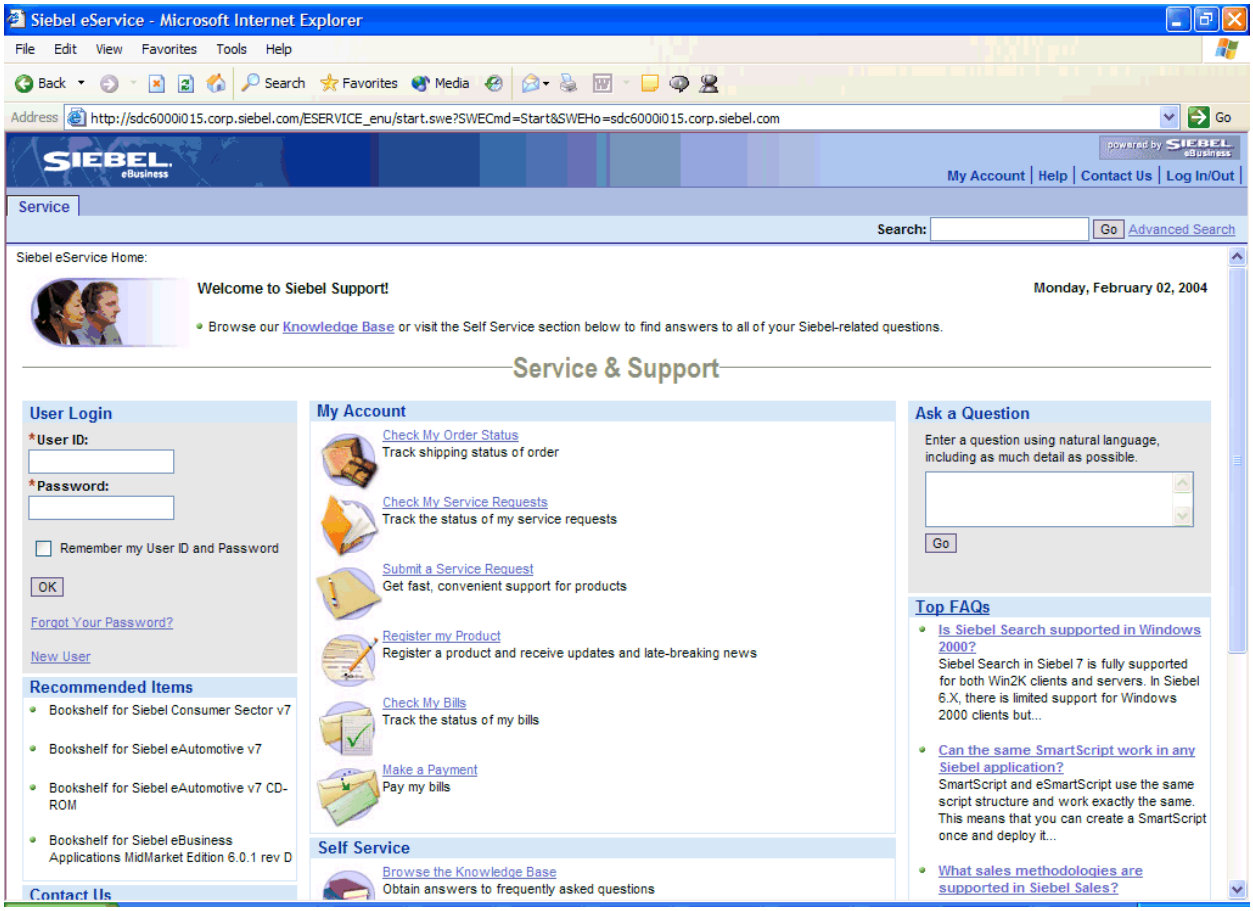


Figure 8. Login Form Embedded in Siebel eService Home Page

A user is required to login, thereby identifying himself or herself as a registered user, to be allowed access to protected views in Siebel applications. Protected views are designated for explicit login. Views that are not designated for explicit login are available for anonymous browsing, if the Siebel application allows anonymous browsing.

For information about setting view properties, see *Configuring Siebel eBusiness Applications*.

For information about anonymous browsing, see "Configuring the Anonymous User" on page 136.

Siebel 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.

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

To implement secure login

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

  ```
  SecureLogin = TRUE
  ```

- To implement secure login, you must also have a certificate from a certificate authority on the Web server where you installed SWSE.

For information about setting Siebel configuration parameters, see Appendix B, "Configuration Parameters Related to Authentication."

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—as long as the user did not log out of the Siebel application using the File > Log Out command.

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 "Cookies and Siebel Applications" on page 168.

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 191.

Account Policies

For enhanced security, you may want to implement the following account policies. Account policies are functions of your authentication service. If you want to implement account policies, you are responsible for setting them up through administration features provided by the authentication service vendor.

- Password syntax rules, such as minimum password length. When creating or changing passwords, minimum length requirements and other syntax rules defined in the external directory will be enforced by the Siebel application.
- An account lockout after a specified number of failed attempts to log in. Account lockout protects against password guessing attacks. Siebel applications support lockout conditions for accounts that have been disabled by the external directory.
- Password expiration after a specified period of time. The external directory can be configured to expire passwords and warn users that passwords are about to expire. Password expiration warnings issued by the external directory will be recognized by Siebel applications and users will be notified to change their passwords.

Password Expiration

Password expiration is handled by the external LDAP directory or Active 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 may provide warning messages to the Siebel application to display when the user logs in. Such a warning would indicate the user's password is about to expire and should be changed. If the user ignores such warnings and allows the password to expire, then the user may be required to change the password before logging into the application. Or, the user may 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 in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, or applicable custom security adapter; database authentication where supported by the RDBMS

Password Expiration on ADS

On ADS, 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, a user will not get a password expired error. No password will expire in the domain.
  - Else, 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`, this user will get a password expired error.
  - Else, if the difference between current time and the last time a user has set the password is smaller than `Password Expire Warn Days` (set for the ADSI security adapter), this user will get a password expiring warning message.
  - Else, if the difference between current time and the last time a user has set the password is smaller than `Maximum Password Age`, and larger than `Password Expire Warn Days`, this user will log in successfully and will not get any error or warning message.

NOTE: Confirm all third-party directory product behavior and configuration with your third-party documentation.

URL Login

Users can log into a Siebel application by presenting user credentials as parameters in a URL. The user does not have to manually type credentials into a login form.

CAUTION: When URL login is used, user passwords may be transmitted in clear text over the network. However,

The easiest, but least secure, option for a form of Web SSO to Siebel applications is to make explicit login requests to a Siebel customer or partner application from navigational entry points to the application. This option works best if the number of navigational entry points to the Siebel application is small, if you are not concerned about users knowing their Siebel username and password, and if you are not deploying a full Web SSO infrastructure.

Following is a sample showing the URL syntax:

```
http://yourhost/eservice/
start.swe?SWECmd=ExecuteLogin&SWEUserName=HKIM&SWEPassword=HKIM
```

NOTE: The parameter names in the URL are case-sensitive.

You can create a single URL that contains a path to a predefined view in addition to a 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/
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"
```

NOTE: You must use commas instead of ampersands (&) as delimiters between arguments in an SWEAC expression.

Cookies and Siebel Applications

Siebel applications running in the Web browser can optionally use cookies for a variety of purposes. Some optional Siebel application functionality requires the ability to use cookies. More details are provided in the sections about each particular type of cookie.

Unless otherwise noted, all of the cookies described in this section apply to both high interactivity and standard interactivity applications. All cookies used by Siebel applications are encrypted using standard encryption algorithms provided by RSA.

For information about enabling cookies in the Microsoft Internet Explorer Web browser, see "Enabling Cookies for Siebel Applications" on page 171.

Siebel applications use the following kinds of cookies:

- **Session cookie.** Manages user sessions for Siebel Web Client users. For details, see "Session Cookie" on page 168.
- **Auto-login credential cookie.** Stores user credentials for Siebel Web Client users. For details, see "Auto-Login Credential Cookie" on page 170.
- **Siebel QuickStart cookie.** Used by the Mobile Web Client when Siebel QuickStart is used. For details, see "Siebel QuickStart Cookie" on page 171.

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 will function in cookieless mode and use URLs instead.
- To force the SWSE to always use cookie-based mode, set `SessionTracking` to `Cookie`.
- To force the SWSE to always use cookieless mode, 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 application 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 *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 eBusiness Application Integration Volume III* 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*.

Cookie-Based Mode

This section 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 may 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. Encrypting the session ID prevents unauthorized attackers from capturing the cookie and determining its format.

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 may 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 should log out and log in again in order to be able to run reports.

Cookieless Mode

This section describes the behavior or cookieless mode. Cookieless mode applies when `SessionTracking` is set to `URL`, or when `SessionTracking` is set to `Automatic` and the user's browser does not accept cookies.

In cookieless mode, 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 it will be rejected by the Web server.

The session ID in the URL is encrypted if the `EncryptSessionId` parameter is set to `TRUE` in the eapps.cfg file.

A cookieless session is invoked when the browser does not send back a session cookie to the Siebel Web Engine. This event can be caused by cookies being disabled in the user's browser, or by a browser that does not support cookies.

You may want a Siebel application to function in cookieless mode for all sessions for reasons such as security requirements that do not permit cookies.

Auto-Login Credential Cookie

The auto-login credential cookie underlies the Remember My User ID and Password feature. 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). 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 in cookieless mode.

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 Applications

This section describes how to enable the Microsoft Internet Explorer Web browser to handle cookies used by Siebel applications.

Review instructions for your supported browser version.

To enable cookies using Internet Explorer 6.0

1. Choose Tools > Internet Options.
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.

To enable cookies using Internet Explorer 5.5

1. Choose Tools > Internet Options.
2. Click the Security tab.
3. In Security settings, under Allow cookies that are stored on your computer, select Enable or Prompt.

   This setting enables persistently storing the auto-login credential cookie and, for the Mobile Web Client, the Siebel QuickStart cookie.
4. In Security settings, under Allow per-session cookies (not stored), select Enable or Prompt.

   This setting enables storing the session cookie during the length of the session.
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 application user has no authenticated access to the Siebel Database. Depending on the Siebel application, unregistered users have various levels of access. Minimally, the user can access a login page. By default, or by your configuration, unregistered users may have access to some or all of the views of a particular Siebel application.

You typically grant registered users more access to data and features than you grant unregistered users. A user can be registered for some or for all of your Siebel applications. You can grant different registered users different levels of access to the database and features.

Typically, a user is registered when the following tasks are performed:

- Create a user record in the Siebel Database.
- Provide the means for the user to be authenticated at login.

Depending on the Siebel application, a user can be registered in one or more of the following ways:

- **Self-registration.** The user can self-register at the Web site.
- **Internal registration.** An administrator at your company can register users.
- **External registration.** A delegated administrator (a user at a customer or partner company) can register users.

If you implement an external authentication system, then adding a user to the Siebel Database, whether by self-registration or by an administrator, may or may not propagate the user's login data to the external authentication system. If the login credentials do not propagate to the authentication system, then you must create the login credentials separately in the authentication system.

If you implement database authentication, then adding the user to the database, with the user 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 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 eBusiness Applications, you are provided seed data that is related to user registration, user authentication, and user access to Siebel applications. The seed data includes users, responsibilities, positions, an organization, and a database login. References to the seed data appear throughout this 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 section provides information about anonymous browsing and how to configure it for Siebel applications.

About Anonymous Browsing and Unregistered Users

Several Siebel applications allow anonymous browsing of views intended for public access as default functionality. Anonymous browsing typically applies to Siebel customer and partner applications, not employee applications. However, you can configure any Siebel application to either allow or disallow anonymous browsing.

Unregistered users gain access to application views and the database through the anonymous user. The anonymous user is a record in the Siebel Database that also performs functions during user authentication and user self-registration. If you implement an external authentication system, the anonymous user has a corresponding record in the user directory.

The anonymous user is required even if your applications do not allow access by unregistered users. When the 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 applications for which anonymous browsing is implemented by default, you should confirm that these tasks are done.

Modifying the Anonymous User Record

The anonymous user is a record in the Siebel Database and, if you implement external user authentication, a corresponding record in the external directory of users. The anonymous user is a component in user authentication, anonymous browsing, and self-registration. For applications that allow anonymous browsing, the anonymous user provides visibility of the pages for which you allow anonymous browsing.

You should set up your user authentication architecture before configuring an application for user access. Therefore, the anonymous user should already exist in your Siebel Database and in your directory.

The responsibility that is assigned to a user record in the database contains a list of views to which the user has access. You must confirm that the anonymous user that you use for your Siebel application includes an appropriate responsibility so that unregistered users can see the views you intend them to see.

If you choose to use a seed anonymous user in your authentication setup, then you should verify that its seed responsibility includes the views you want to provide for anonymous browsing. For example, if you use the GUESTCST seed user for a Siebel customer application, then you should verify that its responsibility, Web Anonymous User, includes the required views. If the responsibility does not include your required views, then you can do one of the following:

- Create one or more additional responsibilities that include missing views, and then add 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 196.

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 306.

- **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 295.

- **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 eBusiness Applications*.

To set or remove the explicit login requirement for a view

1. Open Siebel Tools.
2. Choose Tools > Lock Project.
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 applications allow users to self-register as default functionality. This section observes the following principles about self-registration functionality that is provided by default with your Siebel applications:

- Self-registration applies to Siebel customer and partner applications.
- Self-registration can be implemented only in Siebel 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/ADSI security adapter authentication with Siebel applications for which you allow self-registration.

To implement self-registration for applications that use Web SSO user authentication, you are responsible for configuring the self-registration functionality at the Web site level and for synchronizing the user data with the Siebel Database. Configuration guidelines are not provided in Siebel applications documentation. Self-registration is not feasible when you implement database authentication.

NOTE: If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel applications, including user self-registration. For information about user authentication, see Chapter 6, "Security Adapter Authentication."

Self-registration functionality for Siebel customer and partner applications is included in your Siebel eBusiness 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 eSales.** 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*.

To self-register

1 The user clicks New User on a Siebel application 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 may or may 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/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 eSales, 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 eSales 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.

Modifying the Anonymous User Record

The anonymous user is a record in the Siebel Database and a corresponding record in the user directory. The anonymous user is a component in user authentication, anonymous browsing, and self-registration.

Your user authentication architecture should be set up before configuring an application for user access. Therefore, the anonymous user should already exist in your Siebel Database and in your user directory.

For information about user authentication, see Chapter 6, "Security Adapter Authentication."

Different Siebel applications in the same implementation may 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 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 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.

  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 seed data, see Appendix C, "Seed Data."

Setting Configuration Parameters for Self-Registration

The user directory can be administered through Siebel applications if you implement security adapter authentication. Changes such as adding a user or changing a password by an internal administrator, a delegated administrator, or when a user self-registers are propagated to the user directory.

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 300.

NOTE: If you do not configure your security adapter authentication architecture to allow administration through the Siebel Web Client as described here, then you must manually create a record in the user directory whenever a new user of this application is created in the Siebel Database.

Activating Workflow Processes for Self-Registration

When you install your Siebel eBusiness Applications, you are provided several workflow processes that control self-registration for several Siebel applications.

NOTE: For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Designer Administration Guide*.

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 eSales. This process is also invoked by clicking Forgot Your Password? on the login form. The process branches to one of the following subprocesses:
  - User Registration Process
  - User Registration Forgot Password Process
- **User Registration Process.** This is the main self-registration process. It updates the database, including:
  - Creating a new User record
  - Checking for a duplicate User record
  - Updating the existing User record with new information if a duplicate record is found
- **User Registration SubProcess.** This process is a subprocess to User Registration Process. It performs all of the information gathering and validation. The validated information includes:
  - A duplicate user ID does not exist in the database
  - The Password and Verify Password entries are identical
  - All required fields are completed

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 eSales, Siebel eService, Siebel eCustomer, Siebel Training, Siebel Events, and Siebel eMarketing.

Table 18 on page 182 lists the views specified in the workflow processes that provide interactive forms during self-registration.

Table 18. 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.

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 should 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, there is no need to perform the time-consuming process of undoing a new, partially written record in the database. This process requires searching several tables.
- User record duplication can be prevented before a record is written.

Replacing the License Agreement Text

You can replace the default license agreement that appears to the self-registering user in the User Registration Legal Confirmation View.

The DotCom Applet License Base 1 Column Web template includes the Web template file with the name DotCom Applet Form Base 1 Column which is the file of name dCCAppletLicenseBase1Col.swt. The license agreement is contained in the dCCAppletLicenseBase1Col.swt file, following the phrasing <!--This is where we include the html license agreement-->. You can replace the license agreement text.

For information about working with Web templates, see *Configuring Siebel eBusiness Applications*.

Revising a Workflow Process

The self-registration workflow processes for your business scenario may require that you do revisions to the seed self-registration workflow processes, such as:

- Replace or insert a view
- Insert or delete a step
- Modify a step

You cannot directly modify a seed workflow process, such as any of the self-registration processes. Instead, you must create a copy of the process, and then revise the copy.

By convention, to avoid renaming processes, you can use the Revise button to make a copy of the same name, but with an incremented version number. All other processes of the same name are assigned Outdated status, so that the new version can be the only active version. This convention is recommended for revising any workflow process, not just seed processes.

NOTE: For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Designer Administration Guide*.

Creating Custom Business Services

Siebel applications provides predefined business services that you can use in a step of a workflow process. You can also script your own custom business services and then run them in workflow process steps.

For information about predefined business services and creating business services, see *Configuring Siebel eBusiness Applications*.

For information about running business services in workflow processes, see *Siebel Business Process Designer Administration Guide*.

Redefining Required Fields

As default functionality, a user who is self-registering is required to provide entries in certain fields. These fields may differ depending on the application. 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.

NOTE: For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Designer Administration Guide*.

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 in a Siebel Tools task. For detailed information about working with applets and views in Siebel Tools, see *Configuring Siebel eBusiness 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, choose Edit > New Record.

    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 185, 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 185, 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 eBusiness 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 eBusiness 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 eBusiness 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 eBusiness 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.
   e. 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 188.

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 eBusiness 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 Designer Administration 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 182.

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 applications, choose the Check User Key step.

6 Delete the bypassed process step, which should 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

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.

NOTE: 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 or database 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.

User Experience for a Forgotten Password

A user who has previously self-registered can retrieve a new password, if they have 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.

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 191, 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 19 on page 193 describes the arguments for the FindContact method.

Table 19. 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 is not determined that matches the criteria, RegError receives an error value. ■ Siebel Operation Object Id is used to identify the user record for subsequent operations in the workflow process, and it receives its value from the temporary table's Id column, that is, the ID of the user record. The Login Name process property receives its value from the temporary table's Login Name column, that is, the Login Name of the user record.

Modifying 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 following fields and values:

Table 20. 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 Designer Administration 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 eBusiness 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 182.

   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 need 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 194, 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 eBusiness 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 following fields and values:

Table 21. 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 194 of "Modifying the User Interface for User Registration" on page 194, 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 194 of "Modifying the User Interface for User Registration" on page 194, 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 applications by performing the following tasks:

- Provide the user with a method to be authenticated and thus to connect to a database account.
- An internal administrator uses a Siebel employee application, such as Siebel Call Center, to add the user to the Siebel Database.

User Authentication Requirements

Your authentication architecture should be implemented before adding new users. As an ongoing task, you must arrange that each new user can be authenticated at login. The setup and administration that you must perform for each new user depends on the authentication architecture you implement.

For information about user authentication concepts mentioned in the following descriptions, see Chapter 6, "Security Adapter Authentication."

- **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/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.

  NOTE: For a Siebel security adapter to propagate new or modified user data from the Siebel Database to the user directory, the administrator who modifies the database records must log in through the same security adapter.

  If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel applications. This includes internal administration of users that provides propagation of a user's Siebel user ID to the directory.

  For information about user authentication, see Chapter 6, "Security Adapter Authentication."

  CAUTION: 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 applications documentation. You must provide authentication credentials to the new user.

Adding a User to the Siebel Database

A user of a Siebel application is a record in the User business component. The S_PARTY, S_CONTACT, and S_USER tables in the Siebel Database underlie the User business component. Each user is assigned a responsibility, a user ID, and, depending on the authentication architecture being used, a password.

An employee or a partner user is a user who has a position within a division, either internal or external, in the Siebel Database. Other users, such as those who use customer applications such as Siebel eSales, do not have a position or a division. The S_EMP_PER table underlies the Employee business component, to which employees and partner users belong, in addition to the tables that underlie the User business component.

For more information about the functions of responsibilities, positions, divisions, and organizations, see 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.

CAUTION: 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 may 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 and Siebel Professional Services Automation.

The following procedure creates a User record for the employee only as a stage in allowing the employee to access the database.

To add a new employee

1. Log in as an administrator to a employee application, such as Siebel Call Center, and then choose Navigate > Site Map > Administration - User > Employees.

   The Employees list appears.

2. Add a new record.

3. 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 may or may not log in with this identifier. If you implement database authentication, this field must be the login name for a database account.
Password	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/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 creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "New Responsibility Field for User Record" on page 203.

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 "New Responsibility Field for User Record" on page 203.
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 section of *Applications Administration Guide*.

Also see *Siebel Assignment Manager Administration Guide* and *Siebel Professional Services Automation User Guide*.

Deactivating an Employee

You can deactivate an employee by dissociating the employee record from its responsibilities, altering the user ID, and removing the employee's access to the database.

To deactivate an employee

1. From the application-level menu, choose Navigate > Site Map > Administration - User > Employees.

   The Employees view appears.

2. In the Employees list, select the employee you want to deactivate.
3. In the More Info view tab, delete all records from the Responsibility field.

4 Change the user ID slightly, to indicate that the employee is no longer current.

   You may want to establish a convention for renaming user IDs when you deactivate employees. One possible convention is to append some text such as "expired" to the user ID. For example, you might change CARD to CARD-expired. That way you can continue to see the person's name associated with previous activity in history records.

5 Remove the employee's access to the database.

   If you implemented database user authentication, you should remove the user's database account. If you implemented external authentication, then delete the user from the directory from which the user's database credentials are retrieved.

   NOTE: In the case of external authentication, if the external user 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 eSales 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 section 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 may 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, and then choose Navigate > Site Map > Administration - User > Users.

   The Users list appears.

2. Add a new record.

3 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 may or may 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/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. For information about the function of the account in delegated administration, see "Delegated Administration of Users" on page 204.
Responsibility	Pick one or more responsibilities which include appropriate views in the customer application, such as Siebel eService, for this user. If the administrator who creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default.
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 "New Responsibility Field for User Record" on page 203.
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. From the application-level menu, choose Navigate > Site Map > Administration - User > Persons.

   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 200.

New Responsibility Field for User Record

A user record may or may not 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 any type of user (employee, partner user, contact user) creating any type of user that their application allows them to create.

A user's own New Responsibility field is populated in one of the following ways:

- The New Responsibility field value is inherited from the New Responsibility field of the user who creates this new user.
- The New Responsibility field value is manually assigned to the user.

A user's New Responsibility field can only be modified by an internal administrator.

Delegated administrators of Siebel customer and partner applications can upgrade a user's Responsibility, but they cannot edit the New Responsibility field. Therefore, your internal administrators control the default responsibility that any customer or partner user inherits from a delegated administrator. It is important to make sure delegated administrators have New Responsibility values that you intend your new customer and partner users to have, such as the seed responsibilities provided for such users.

You may or may not want to use the New Responsibility field functionality when administrators create new employee records. If there are a variety of responsibilities assigned new employees, then it may make sense to leave employee's New Responsibility field empty. If most of your new employees are assigned the same responsibility or you want to create a batch of new employee records that all have the same responsibility, then it is probably more efficient to assign a New Responsibility value to the administrator who adds the employees.

An internal administrator can modify New Responsibility values for employees, partner users, and contact users in the same administration screen.

To modify a user's New Responsibility field value

1. Log in as an administrator to a Siebel employee application, and then choose Navigate > Site Map > Administration - User > Users.

   The Users list appears, containing all the employees, partner users, and contact users in the database.

2. In the Users list, select the user record to modify.

3. 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 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 applications, including delegated administration of users. For information about user authentication, see Chapter 6, "Security Adapter Authentication."

CAUTION: 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 has restricted access to user data.

- **Customer applications.** A delegated administrator can only see users that are associated with accounts with which the delegated administrator is associated. The My Account User Administration View is based on the Account (Delegated Admin) business component. This business component essentially restricts a delegated administrator's access to data that is associated with the accounts with which the delegated administrator is also associated.
- **Partner applications.** A delegated administrator can only see partner users whose positions are in the same partner organization to which the delegated administrator's position belongs.

A delegated administrator can add regular registered users or other delegated administrators. However, an administrator at your host company must add the first delegated administrator in:

- Each account for a Siebel customer application
- Each partner organization for a Siebel partner application

Creating a delegated administrator internally requires that you provide a user with a responsibility that includes the views needed for delegated administration. Your Siebel application provides seed responsibilities for delegated administrators of customer and partner applications.

For information about seed responsibilities, see Appendix C, "Seed Data."

NOTE: Delegated user administration screens, navigation, and procedures vary somewhat among Siebel applications. The remaining sections 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. A delegated administrator only has responsibilities, including seed responsibilities, available for assigning to users that your host company associates with the organization with which the delegated administrator is associated. The delegated administrator is associated with the organization to which the proxy employee for the application belongs. A responsibility is associated with an organization by an administrator at your company using an employee application such as Siebel Call Center.

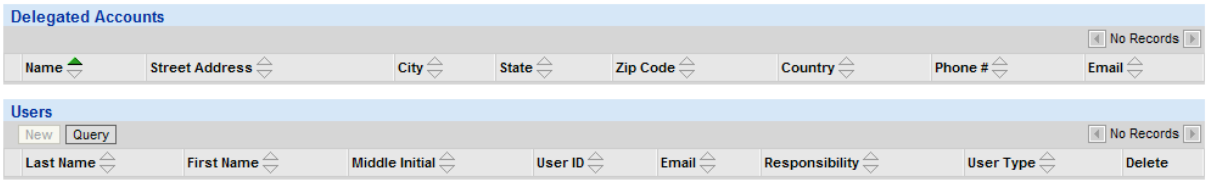
To register a new customer user (by a delegated administrator)

1. Log into a Siebel customer application that implements delegated administration, such as Siebel eSales 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 may vary somewhat by application.



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 may or may 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/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 "New Responsibility Field for User Record" on page 203.
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 only has responsibilities available for assigning to partner users that your host company associates with the delegated administrator's partner organization. An administrator at your company associates partner organizations with responsibilities using an employee application such as Siebel 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. Choose Site Map > 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 may or may 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/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 "New Responsibility Field for User Record" on page 203.
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 applications. The procedures in this section are representative of those in Siebel employee, partner, and customer applications. Procedures in individual applications may differ.

Editing Personal Information

Users can change a variety of personal information in their profile form. In this context, authentication and access control data, such as passwords and positions, are not included.

To edit personal information

1. Depending on the application, the user does one of the following:
   - In a Siebel customer application, the user clicks My Account, and then clicks User Profile under My Settings. The User Profile form appears.
   - In a Siebel partner application, the user clicks Profile. The Personal Profile form appears.
   - In a Siebel employee application, the user chooses Navigate > Site Map > User Preferences > Profile. 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.

NOTE: 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 the Siebel application views. Configuration guidelines are not provided in Siebel applications documentation.

To change a password, a user accesses the profile form as described in "Editing Personal Information" on page 210, 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. A user who is associated with more than one position has 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. From the application-level menu, choose Navigate > Site Map > User Preferences > Change Position.

   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 application functionality. It includes the following topics:

About Access Control

Access control is the term used to describe the set of Siebel application mechanisms that control user access to data and application functionality.

NOTE: As you work with this chapter, you should determine how the terminology and concepts presented here correspond to your company's internal terminology and structure. This chapter explains the mechanism 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 needs.

In Siebel application terms, 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 may 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 9 on page 214 shows the Account List View, which corresponds to the applet title My Accounts (the current visibility filter selection). Multiple visibility 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.

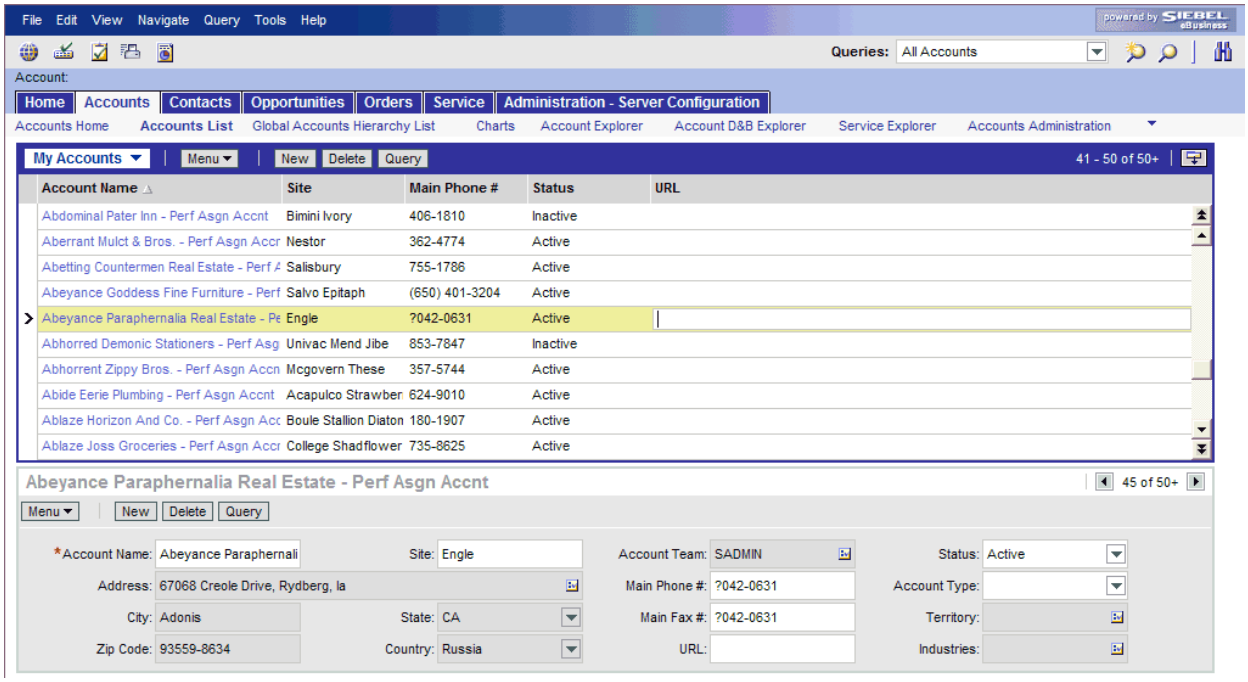


Figure 9. My Accounts View

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 needed 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 215.

- **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 218.
- **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 220
- "Planning for Access Control" on page 230
- "Implementing Access Control" on page 237
- "Implementing Access-Group Access Control" on page 256

Access Control for Parties

Individual people, groupings of people, and entities that represent people or groups are unified in the common notion of *parties*.

NOTE: For technical information about how parties function at the data model level, see "Party Data Model" on page 276.

Parties are categorized into the following party types: Person, Position, Organization, Household, User List, and Access Group. Table 22 on page 215 describes the qualitative differences among different parties and identifies the applicable party type for each party.

Table 22. 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.

Table 22. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Employee	Person	■ An employee at your company.	■ An Employee is a User who is associated with a position in a division within your company.
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 may have a parent position. It may also have child positions. ■ One or more employees can be associated with an internal position, and one or more partner users can be associated with an external position. ■ An employee or partner user can be associated with more than one position, but only one position is active at any time.

Table 22. 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 may have a parent account. It may 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 may have a parent division. It may 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 22. 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 may 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 may have any combination of contacts, users, employees, and partner users as members. ■ A user list cannot have a parent or children.
Access Group	Access Group	■ 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 may have a parent access group. It may 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 > 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 10 on page 220.

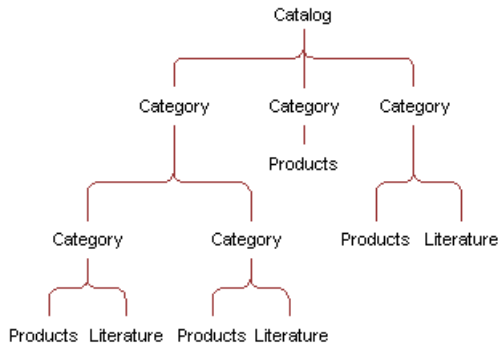


Figure 10. Example Catalog/Category Hierarchy

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 subsections that follow:

- **Personal access control.** For details, see "About Personal Access Control" on page 221.
- **Position access control.** This includes single-position, team, and manager access control. For details, see:
  - "About Position Access Control" on page 221
  - "About Single-Position Access Control" on page 222
  - "About Team (Multiple-Position) Access Control" on page 223
  - "About Manager Access Control" on page 223

- **Organization access control.** This includes single-organization, multiple-organization, and suborganization access control. For details, see:
  - "About Organization Access Control" on page 225
  - "About Single- and Multiple-Organization Access Control" on page 225
  - "About Suborganization Access Control" on page 227
- **All access control.** For details, see "About All Access Control" on page 228.
- **Access-group access control.** For details, see "About Access-Group Access Control" on page 229.

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 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

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 222.
- **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 223.
- **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 223.

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 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

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 may include internal and partner positions.

The display names for fields representing position teams vary with the view in which they appear. Some common views that apply 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, may 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 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

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 your Siebel application.

You can specify one parent position for a position, which represents that the position is a direct report to the parent. The parent of an internal position may be in the same division or a different division. For example, a sales manager in the Sales division may report to a sales vice president in the Corporate division.

In a view using manager access control, 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*.

  CAUTION: Configuring nonprimary manager visibility to support mobile users requires changes to docking visibility rules. Customers who require this functionality must engage Siebel 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.

NOTE: 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 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

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 225.
- **Multiple-organization access control.** You can associate multiple organizations with individual data. For details, see "About Single- and Multiple-Organization Access Control" on page 225.
- **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 227.

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 221.

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 311.

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 23 on page 226 lists data on which you can apply organization access control and whether a single organization or multiple organizations can be associated with the data.

Table 23. Organization-Enabled Data

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	N/A (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 *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 228.

For information about business component view modes, see "Business Component View Modes" on page 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

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 choosing Navigate > Site Map > Administration - Group > Organizations.

The organizational hierarchy is included as seed data when you install your Siebel application. Within the organizational hierarchy, you can create branches for both internal and partner organizational structures.

You can specify one parent organization for an organization.

In a view using 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 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

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 may 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 need not 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 244.

For information about implementing access control in a view, see "View Access Control Properties" on page 250.

For information about Admin mode, see "View Access Control Properties" on page 250.

About Access-Group Access Control

Access groups are used to control access to master data by diverse groups of party types.

For information about administering access-group access control, see "Implementing Access-Group Access Control" on page 256.

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 218.

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 218.

For more information about parties, see "Access Control for Parties" on page 215.

Planning for Access Control

Two main strategies are available for controlling access to data in Siebel applications:

- **Multiple-organization access control.** This strategy limits data access to only those organizations that have a need to see the information. Organizational access control can be implemented across internal or external organizations. This strategy can be applied to transaction data, master data, and other referential data.

  For more information, see "About Organization Access Control" on page 225, the sections following this one, and "Implementing Access Control" on page 237.

- **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 229 and "Implementing Access-Group Access Control" on page 256.

For analysis and recommendations for choosing and implementing access control strategies, see *Access Control Upgrade and Migration Guide for Siebel 7*, available on Siebel SupportWeb.

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 will need 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 section 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 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 24 on page 231.

Table 24. Elements of Business Environment Structure

Element	Parent-Child	Description
Divisions	Y	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	Y	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 225.
Positions	Y	Control the data set (records) to which a user has access. See "About Position Access Control" on page 221.
Responsibilities	N	Control the views to which a user has access.
Employees	N	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.

NOTE: Because organizations are based on divisions, it may be best to create your hierarchy of divisions first, and then to determine which of these divisions will be designated as organizations.

CAUTION: 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 your Siebel application is already deployed and you do not need to change your users' visibility (access), your company may not need more organizations. Some circumstances where your company could benefit from multiple organizations are as follows:

- **Internal business units.** If you have a small number of distinct internal business units, you may want to use organizations to support specific versions of a limited number of data entities such as products and price lists.
- **Complex 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 should 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 may make fewer views available to these external organizations than to your internal organizations. You may also configure the employee drop-down list so that it shows only employees who belong to the user's organization.
- **Different rules for business units.** If you would like to make different 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 section and those that follow explain the common tasks for defining a company structure in your Siebel application. 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 eBusiness 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 division records, because business components throughout your Siebel application refer to organization records. Deleting a division would cause invalid references on transaction records. This would lead to unexpected negative results, such as valid data not appearing in the user interface.

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 your Siebel application, all the data is automatically assigned to one default organization. With one organization, there is no impact on visibility and data access. However, if you want to divide your company into multiple structural units, you can create multiple organizations.

You may want to delegate administration of users to organizations that access only their users. To do this, you must configure the appropriate views using Siebel Tools. For more information on configuring views, see *Configuring Siebel eBusiness 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 may 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 may need 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 eBusiness Applications*.

NOTE: You cannot delete organization records. Business components throughout your Siebel application refer to organization records. Deleting an organization could cause invalid references on transaction records. This could lead to unexpected negative results, such as valid data not appearing in the user interface.

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.

NOTE: An employee should have a position in order to create and use accounts, opportunities, contacts, and other customer data objects in your Siebel application.

Each position typically has only one associated employee. In some circumstances such as job-sharing situations, a position may have multiple associated employees. One employee can be associated with multiple positions. There can be only one primary employee for a position, but an employee can be primary for more than one position.

There is a drawback to having multiple employees associated with a position. Because a position can have only one primary employee, only the primary employee is visible in the Employee field. If you search for an employee in a positions list, you may not find relevant position records in which the employee is not primary for the position.

Only the primary employee for a position appears in the Account Team, Opportunity Sales Team, and Contact Access lists. However, all the employees in that position can access the My Accounts, My Opportunities, and My Contacts views.

A position can be associated with only one organization. If you want an employee to have visibility to multiple organizations, you must create a position for each organization and assign that employee to each position. The employee can then see one organization’s data at a time by changing positions.

Positions can be set up in a multilevel hierarchy, 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.)

Your Siebel application allows 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 choosing Tools > User Preferences > Change Position, selecting a different position in the list, and clicking 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.

NOTE: You cannot make a position obsolete by setting the End Date. This field records only the end date for the current employee associated with the position. It does not make the position obsolete after that date has passed.

CAUTION: Do not delete a position. This can cause unexpected and negative results. For example, if you delete a position that is primary for an account, and you do not select a new primary position for that account, Assignment Manager may not be able to assign resources to activities for that account.

If you rename a position, check these areas in your Siebel application to make sure the name change is reflected correctly:

- 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 Designer Administration 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 will be distributed to all users. See also "Position Data Model" on page 281.

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 your Siebel application's information and functions. You must assign responsibilities to all users. Without a responsibility, a user cannot use the Siebel application, because that user cannot access any views.

You can also assign tab layouts and tasks to responsibilities. For more information, see "Managing Tab Layouts Through Responsibilities" on page 268 and "Managing Tasks Through Responsibilities" on page 271.

NOTE: 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 your Siebel application. These can be copied and then customized.

NOTE: You cannot modify or delete the seed responsibilities. For instance, you cannot change the Siebel administrator responsibility. You can copy the seed responsibilities and modify the copies.

When you are defining responsibilities, consider the following issues:

- You should grant access to the System Preferences view to only a selected group of administrators. End users should not be given access to the System Preferences view. System preferences control many things throughout the system, including some server logic and processing for Siebel Remote and Siebel Assignment Manager.
- You should not add Administration views to responsibilities associated with end users. Likewise, you should 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 should not be able to create or modify data, specify that the view will be 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 may 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 *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 in the Administration - Application > Responsibilities view.

  However, if you log into the application through the Siebel Mobile or Dedicated Web Client, the New button in the View applet of the Responsibilities view is unavailable. To activate the button, so you can add views to responsibilities using these client types, you can start the Siebel client with the command-line option `/editseeddata`.

  CAUTION: Before using the `/editseeddata` command-line option, you must fully understand the impact this feature may have upon your data. It is generally recommended not to use this option.

  For more information about startup options for the Siebel Mobile or Dedicated Web Client, see *Siebel Installation Guide* for the operating system you are using.

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 section specifies where to find these settings within Siebel Tools, but in most cases does not provide procedures to implement them. Changing any settings in Siebel Tools requires recompiling the Siebel repository file.

For more information about required practices when using Siebel Tools, see *Configuring Siebel eBusiness 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 may 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

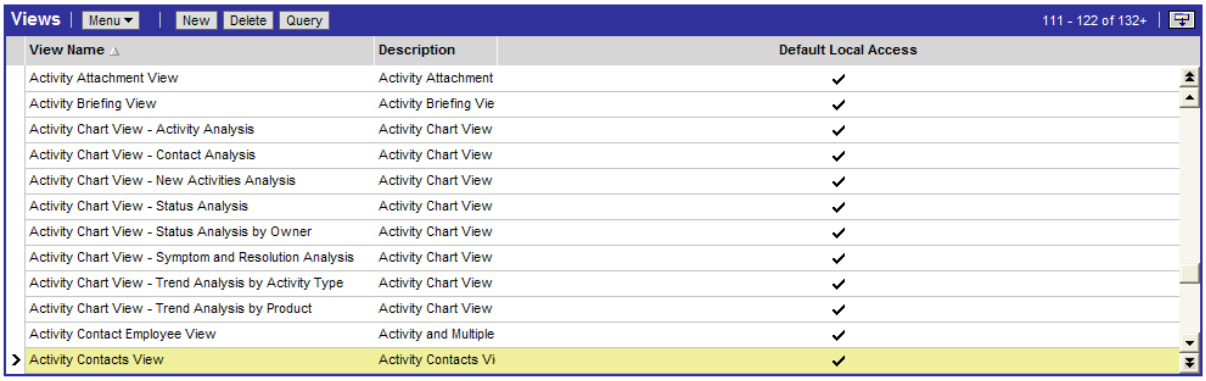
Each Siebel application is associated with a set of screens. Each screen is in turn made up of a set of views.

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 eBusiness Applications.

To see which views an application includes

1. Log in as an administrator.
2. From the application-level menu, choose Navigate > Site Map > Administration - Application > Views.

   The figure below shows a sample list of some of the views defined for an application.



View Name	Description	Default Local Access
Activity Attachment View	Activity Attachment	✓
Activity Briefing View	Activity Briefing Vie	✓
Activity Chart View - Activity Analysis	Activity Chart View	✓
Activity Chart View - Contact Analysis	Activity Chart View	✓
Activity Chart View - New Activities Analysis	Activity Chart View	✓
Activity Chart View - Status Analysis	Activity Chart View	✓
Activity Chart View - Status Analysis by Owner	Activity Chart View	✓
Activity Chart View - Symptom and Resolution Analysis	Activity Chart View	✓
Activity Chart View - Trend Analysis by Activity Type	Activity Chart View	✓
Activity Chart View - Trend Analysis by Product	Activity Chart View	✓
Activity Contact Employee View	Activity and Multiple	✓
Activity Contacts View	Activity Contacts Vi	✓

For information about configuring screens and views, see *Configuring Siebel eBusiness Applications*.

Setting Up Divisions, Organizations, and Positions

This topic describes how to set up divisions, organizations, and positions.

Setting Up Divisions

This section describes how to set up divisions.

To set up a division

1. From the application-level menu, choose Navigate > Site Map > Administration - Group > Internal Divisions.

   The Internal Divisions view appears.

2 In the 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 section describes how to set up organizations.

To set up an organization

1 From the application-level menu, choose Navigate > Site Map > Administration - Group > Organizations.

The Organizations view appears.

2 In the 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. **NOTE:** Partners are registered and promoted to organizations using the Approved Partners view in the Administration - Partner screen, as described in *Developing and Deploying Siebel eBusiness Applications*.

Setting Up Positions

This section describes how to set up positions.

To set up a position

1 From the application-level menu, choose Navigate > Site Map > Administration - Group > Positions.

The Positions view appears.

2 In the form, add a new record and complete the necessary fields.

Some fields are described in the following table.

NOTE: 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
Billing Product	Used by Siebel Professional Services Automation.
Compensable	Used by Incentive Compensation.
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	Allows a position to be associated with a territory. For use by Siebel Assignment Manager.

Setting Up Responsibilities and Adding Views and Users

This section describes how to set up responsibilities and add views and users.

To define a responsibility and add views and users

1 From the application-level menu, choose Navigate > Site Map > Administration - Application > Responsibilities.

The Responsibilities view appears.

NOTE: By default, the Responsibilities view shows all responsibilities, regardless of organization. However, you may want to configure new views in Siebel Tools that restrict the visibility to responsibilities. For more information on configuring views, see *Configuring Siebel eBusiness 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 should be read-only for users with this responsibility.

   NOTE: You can also delete views from the Views list.

5 To add users, do the following:

   a In the Users list, add a new record.

   b Select the appropriate users in the Add Users dialog box and click OK.

   NOTE: You can also delete employees from the Users list.

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 268.

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 may in some cases require that the associated 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 272.

Associating a Responsibility with Organizations

You can associate a responsibility with one or more organizations.

NOTE: Responsibilities should 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 should only be assigned to users by internal administrators, and not by other delegated administrators. A user can then have a delegated administrator responsibility, but would not be able to see it in a list of responsibilities. Therefore, the delegated administrator could not assign it to other users. You can accomplish this scenario by associating the delegated administrator responsibility with an organization other than that with which the delegated administrator is associated.

NOTE: You should associate each responsibility with at least one organization if you include 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 Dedicated 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 in Views list under Navigate > Site Map > Administration - Application > Views. This setting defines a default setting to be inherited for the view, unless the setting is overridden in another context.
- Local Access flag in Views list under Navigate > Site Map > Administration - Application > Responsibilities. This 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 in Responsibilities list under Navigate > Site Map > Administration - Application > Views. This setting is 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.

Figure 11 on page 243 shows the Local Access field specified for views associated with a responsibility (seen here in the Responsibilities view).

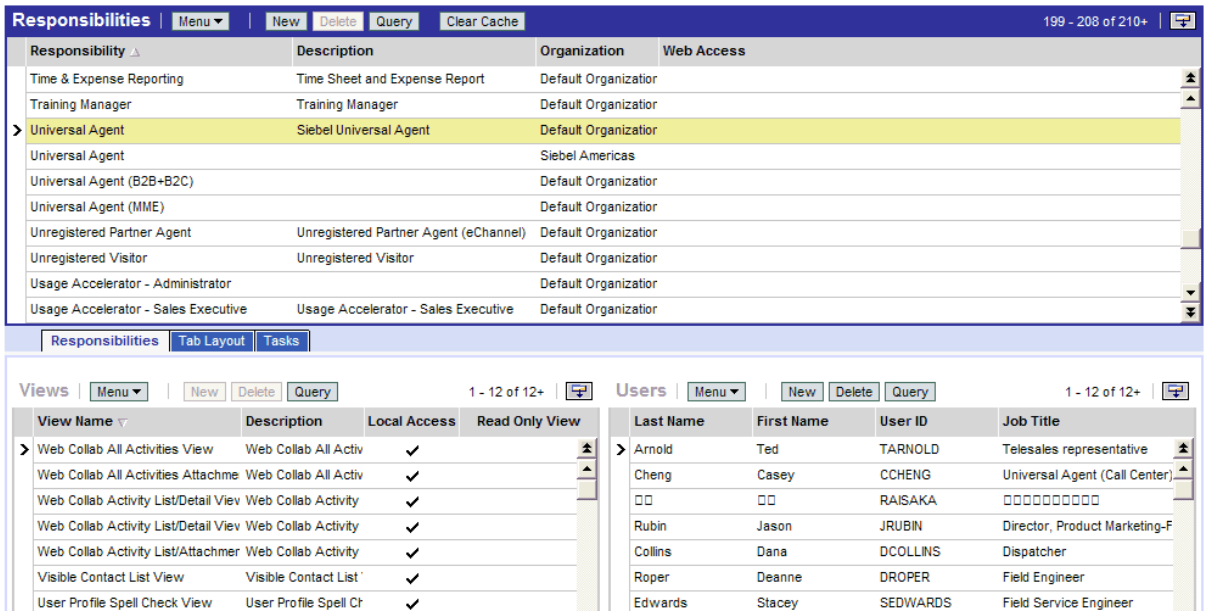


Figure 11. Responsibilities View

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: You should disable access to views applying All access control by setting the Local Access field to FALSE. A view with All access control will have unpredictable and possibly undesirable results for a mobile user. For information about All access control, see "About All Access Control" on page 228.

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 From the application-level menu, choose Navigate > Site Map > Administration - User > Persons.

The Persons list appears.

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 may connect the data to the person by comparing the data's Owner Id field to the person's user ID. Another business component may apply personal access control through the data's Created by field.

You use Siebel Tools to work with properties of business components.

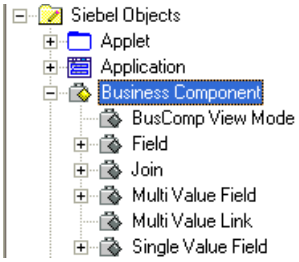
NOTE: If a business component has no listed view modes, then there is no access control based on the business component in views that are based on that business component.

To view a business component's view mode and visibility fields

1 Launch Siebel Tools.

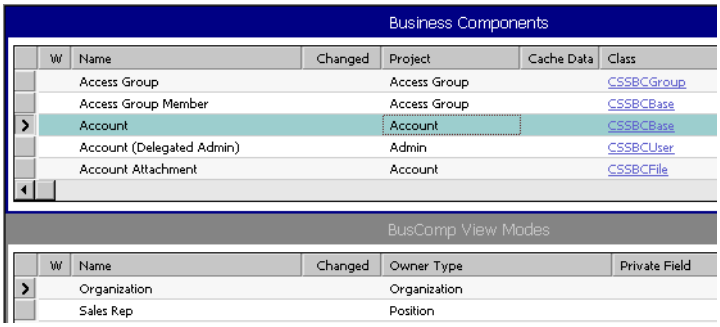
2 In the Object Explorer, click + (the plus sign) to expand the Business Component object type.

The Business Component subtree appears, as shown below.



3 Click the BusComp View Mode icon.

The Business Components list and its BusComp View Modes detail list appear, as shown below.



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 they are associated, the user gets access to the record.

  A value in this field indicates that there is only one party associated with this business component when using this view mode.

  For example, the Service Request business component's Personal view mode determines whether the user is associated with the record by comparing the user's Login ID with the value in the Contact Id field.

  When this view mode is used, only one user qualifies as being associated with this record. Typically, this user would be the creator of the service request.
- **Visibility MVField (or 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 should be used to determine the value in the MVField for this record.

  Links establish a parent/child relationship between business components, often by specifying an intersection table (in the case of a many-to-many relationship). This 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 needed because the creator and the customer care agent both need access to the data based on a person.

For information about working with business components, see *Configuring Siebel eBusiness Applications*.

Applet Access Control Properties

A view presents a collection of lists, forms, and trees at once, as shown in Figure 12 on page 248 (Organization Chart view). These lists and forms are referred to as applets in a configuration context.

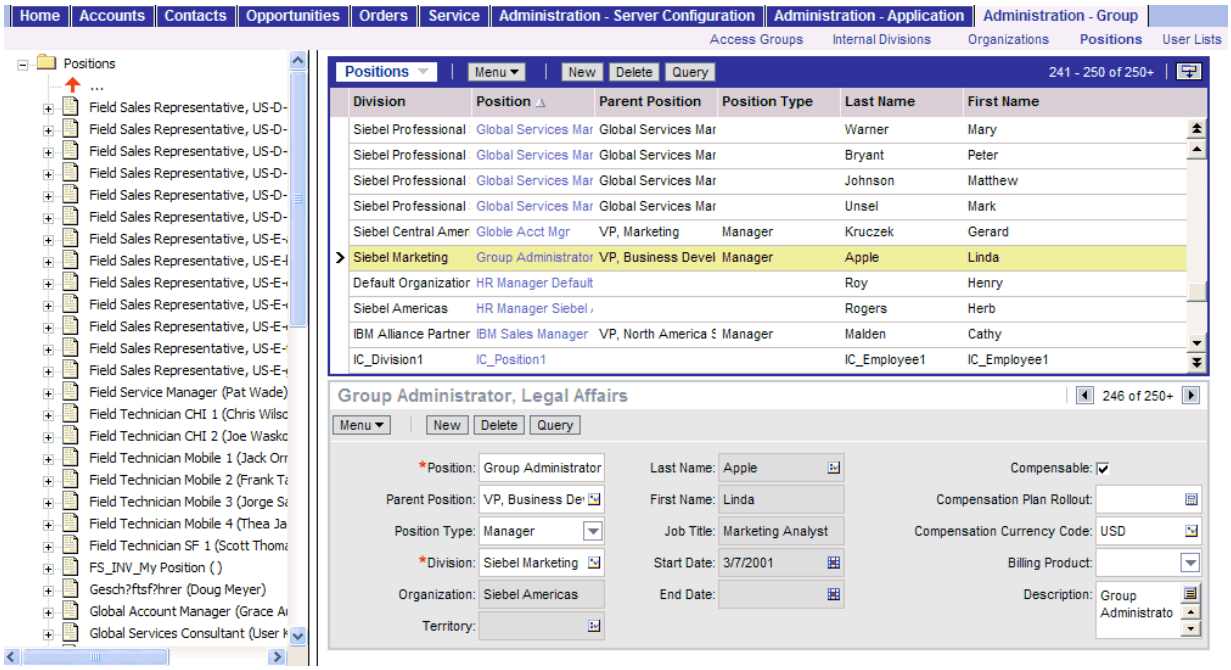


Figure 12. Examples of Applets in a Siebel Application

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.

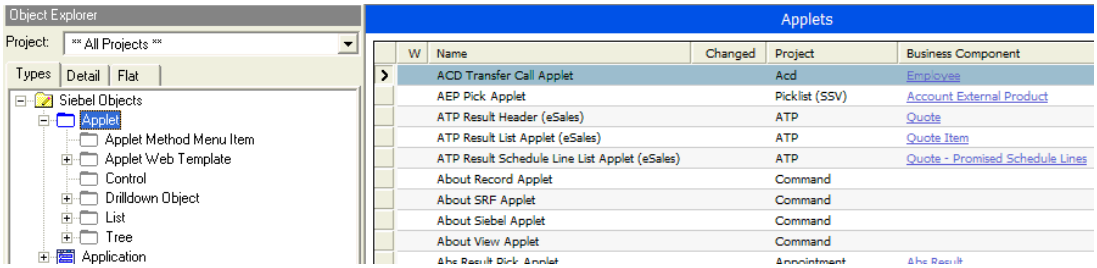
You use Siebel Tools to work with applets and their properties. For more information, see *Configuring Siebel eBusiness Applications*.

To view an applet's properties

1 Launch Siebel Tools.

2 In the Object Explorer, click + to expand the Applet object type.

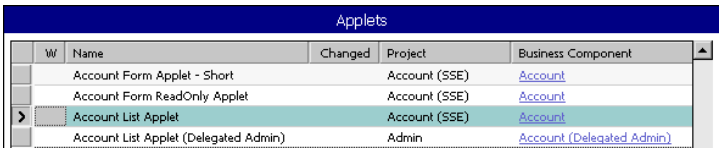
The Applet subtree appears. The Applets list also appears, as shown below.



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.

As shown below, the Business Component field specifies the business component on which the applet is based. For example, Account List Applet uses the Account business component.



4 In the Object Explorer, choose Applets > List > List Columns.

As shown in Figure 13 on page 250, 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.

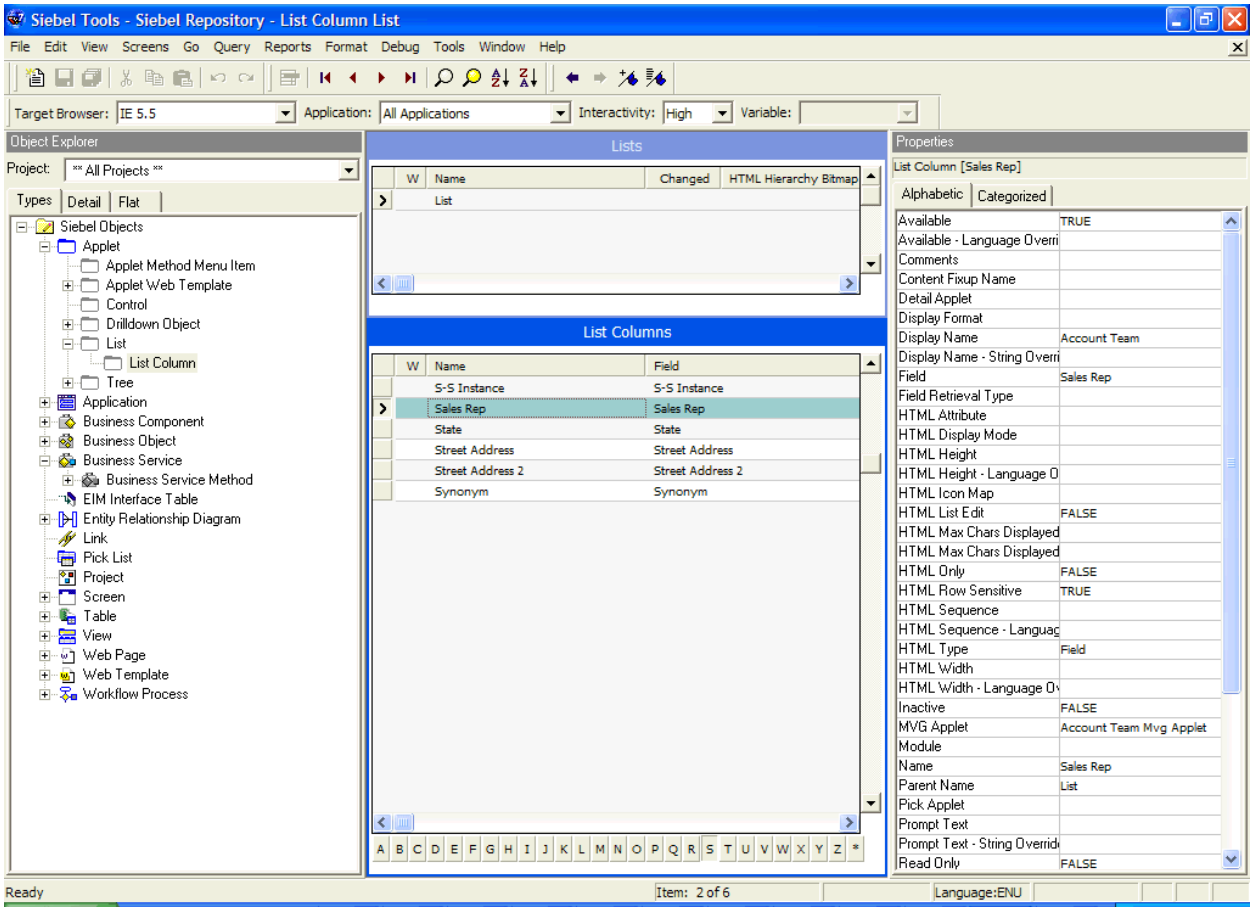


Figure 13. Lists and List Columns for an Applet

View Access Control Properties

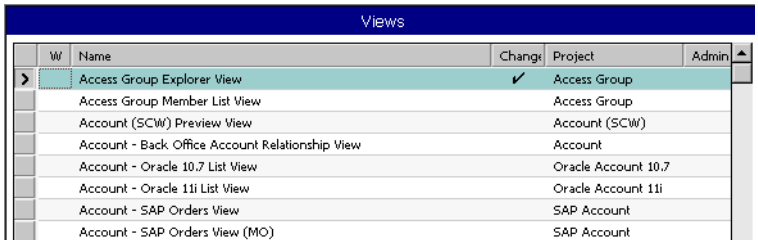
A view's access control properties determine what applet is used to drive visibility and what access control mechanism is applied to the business component on which the view is based.

You use Siebel Tools to work with properties of views.

To see a view's access control properties

1. Launch Siebel Tools.
2. In the Object Explorer, click the Views object type.

   The Views list appears as shown in the figure below. Its fields include those that influence visibility.



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. It should suggest the level of access control on the view's data. For example, My Accounts suggests more restricted visibility than My Team's Accounts.
- **Visibility applet.** Typically, this is the master in a master-detail applet relationship. This applet defines the business component on which the view is based and how fields of the business component are displayed.

  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 will re-query 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 should 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.

- **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.

  NOTE: Despite setting the visibility type to Catalog, you may 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 eBusiness Applications*.

Figure 14 on page 254 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 14. Account Business Component View Modes

Figure 15 on page 254 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 15. 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 25 on page 255.

Table 25. 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 That Applies Access-Group Access Control

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 16 on page 257 illustrates one access control structure that solves this business problem.

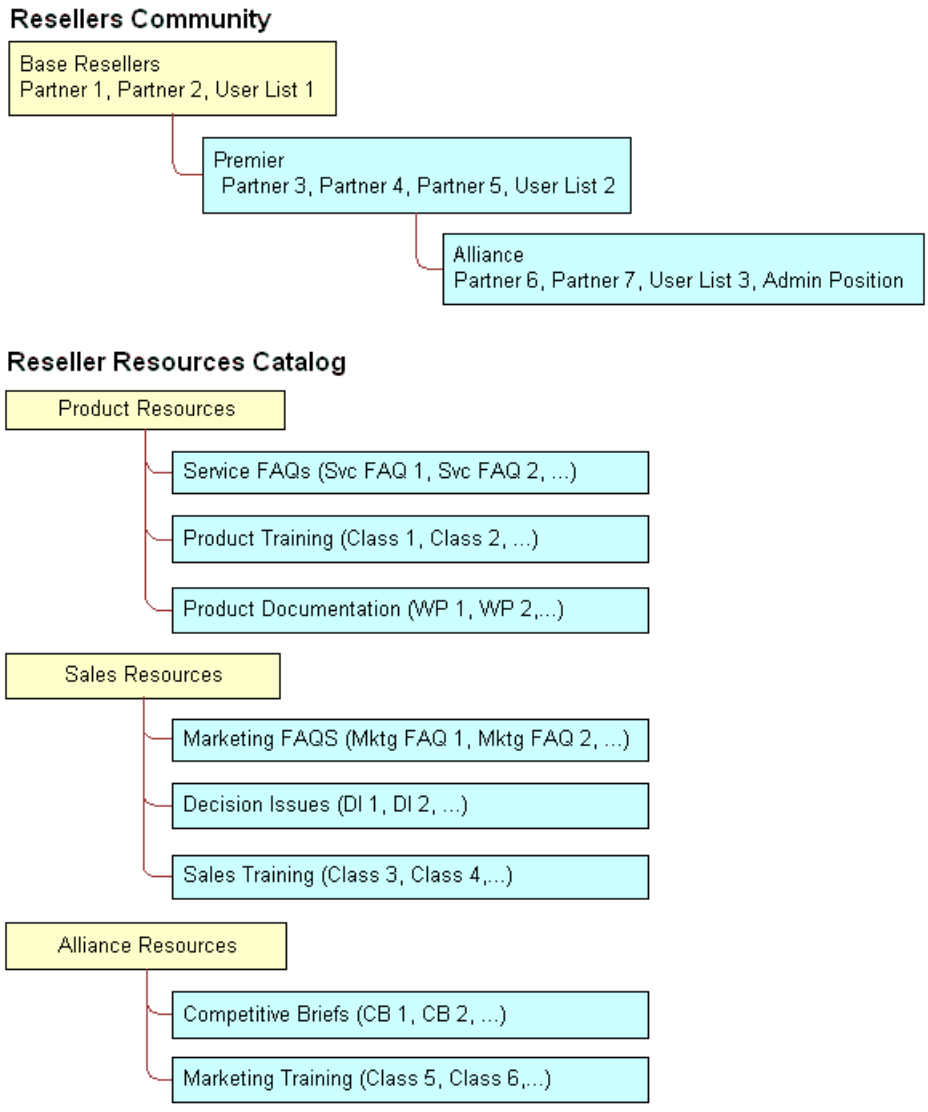


Figure 16. Reseller Resources Access Control Example

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 256.

The User's Experience

You can configure a catalog to display in Siebel employee applications and in selected customer and partner applications, such as Siebel eSales and Siebel 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.

As shown in Figure 17 on page 260, Info Center Explorer provides a tree interface for navigating all the catalogs to which the user has access, down to the data item level.

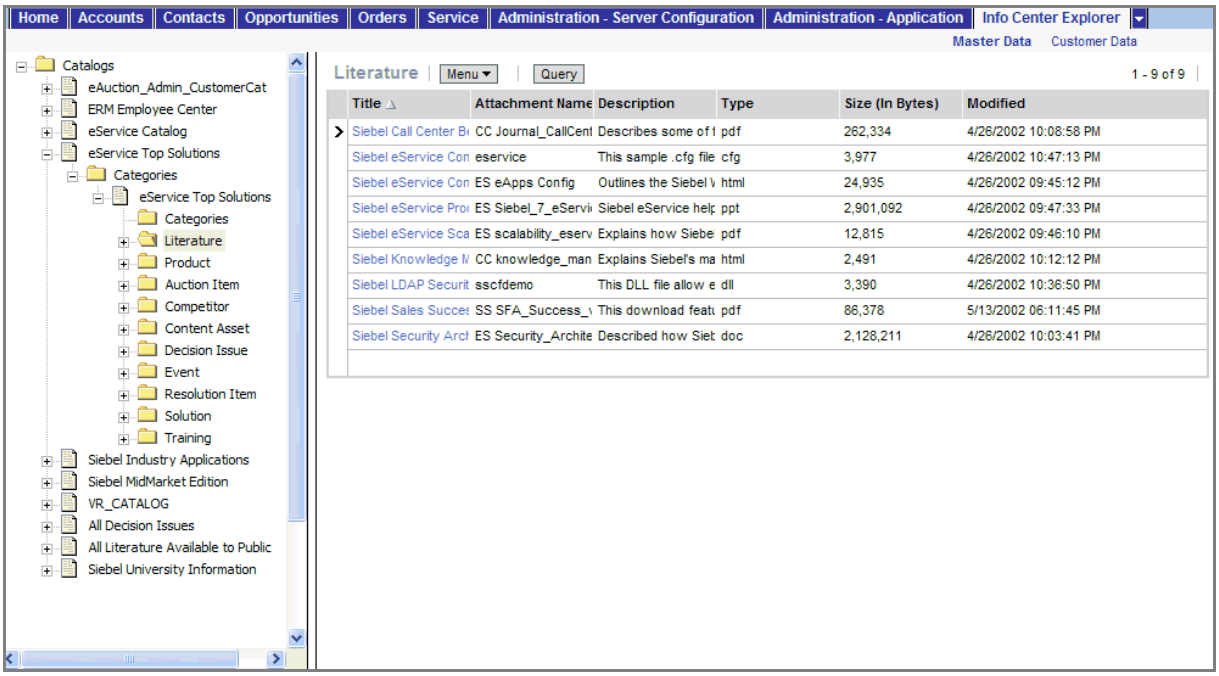


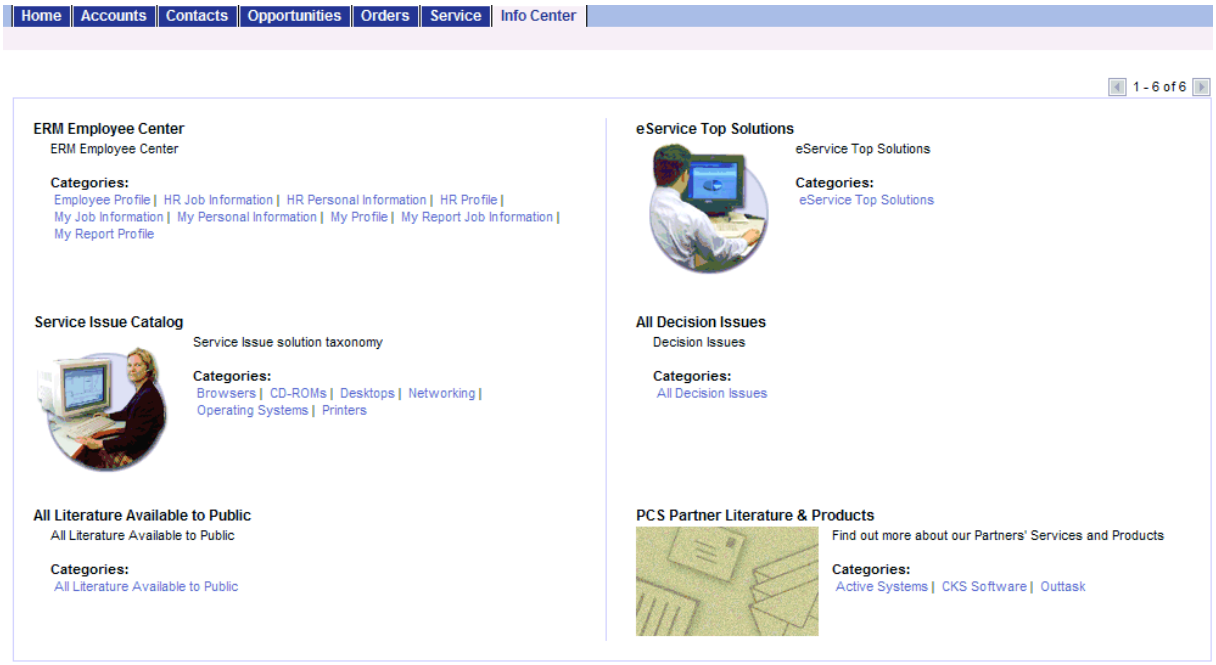
Figure 17. Info Center Explorer

Info Center, as compared to Info Center Explorer, shows how categorized data can be presented in Siebel applications using a rich and more open user interface.

To see categorized data in Info Center

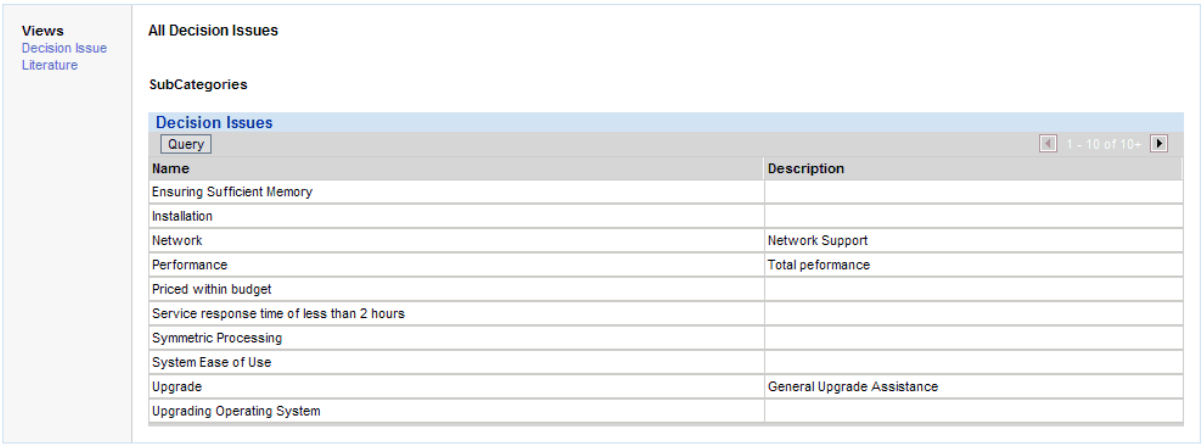
1 From the application-level menu, choose Navigate > Site Map > Info Center.

The Info Center screen appears, as shown in the following figure. It shows accessible catalogs and their first-level categories.



2 Click a category link. For example, you might choose Decision Issues.

As shown below, 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 needed.
- 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 needed.
- Associate access groups with catalogs and categories of data.

Administering Catalogs of Data

You can do the following catalog and category administration tasks in the 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.

Administering Positions

You must do the following administrative tasks with positions:

- Create positions.
- Associate positions with employees and partner users.
- Maintain position hierarchies.

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.

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 *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 215.

Creating a User List

You can create a user list in the Administration - Group screen.

To create a user list

1. From the application-level menu, choose Navigate > Site Map > Administration - Group > User Lists.

   The User Lists list appears.

2. In the User Lists list, add a new record.

   A new user list record appears.

3. Enter a name for the user list. Optionally, change the default entry for Group Type.
4. Save the record.

Modifying a User List

You can modify a user list by adding or deleting users.

To add users to a user list

1. From the application-level menu, choose Navigate > Site Map > Administration - Group > User Lists.

   The User Lists list appears.

2. In the User Lists list, select a user list.
3. In the Users list at the bottom of the view, add a new record.
4. Select one or more users, and then click OK.

   The selected users appear in the Users list. If a user, such as a customer user, belongs to an account, the Account field populates automatically.

You can delete users from a user list similarly.

Administering Access Groups

You can group parties of types Position, Organization, Household, and User List into access groups for the purpose of controlling their individual members' access to data.

You administer access groups in the Administration - Group screen by choosing Navigate > Site Map > Administration - Group > Access Groups. This screen contains the Access Groups tree and the Access Groups list.

The Access Groups tree lists all access groups on the second level of the tree. Each access group can be expanded to show its descendants. Therefore, an access group may appear at different levels in multiple branches of the tree.

An access group that has no parent access group is the top node of an access group hierarchy.

For information about access groups, see "Access Control for Parties" on page 215 and "About Access-Group Access Control" on page 229.

Creating an Access Group

You can create an access group in the Administration - Group screen.

To create an access group

1. From the application-level menu, choose Navigate > Site Map > Administration - Group > Access Groups.

   The Access Groups tree and the Access Groups list appear.

2. In the Access Groups list, add a new record.

   A new access group record.

3 Complete the following fields, 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 From the application-level menu, choose Navigate > Site Map > Administration - Group > Access Groups.

The Access Groups list appears.

2 In the Access Groups list, select an access group.

3 In the Members list, add a new record.

A pop-up list appears that contains positions, organizations, accounts, 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 From the application-level menu, choose Navigate > Site Map > Administration - Group > Access Groups.

The Access Groups list appears.

2 In the Access Groups list, select an access group.

3 Click on the Parent Access Group field.

The text box becomes editable and its entry is highlighted.

4 Do one of the following to modify the hierarchy:

- To make the access group the top node of its own hierarchy, delete the entry in the Parent Access Group field. 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 From the application-level menu, choose Navigate > Site Map > Administration - Catalog > Access Groups.

The Catalogs list appears.

2 Select a catalog.

3 In the Access Groups list, add a new record.

A pop-up list appears that contains access groups.

4 Select an access group, and then click Add.

The access group appears in the Access Groups list.

5 In the Access Groups list, 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 From the application-level menu, choose Navigate > Site Map > Administration - Catalog > Access Groups.

The Catalogs list appears.

2 Drill down on a catalog name.

The Categories list for the catalog appears.

3 Click the Access Groups view 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 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 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 (Tools > User Preferences). 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 *Fundamentals*.

If a user selects a screen from the Site Map that is not part of their tab layout, a screen tab is created for that screen which will only be available for that session.

Administering Tab Layout

To manage tab layouts, navigate to Administration - Application > Responsibilities and click the Tab Layout view tab.

The Tab Layout view (Responsibility Detail - 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 270.

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 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 may 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. From the application-level menu, choose Navigate > Site Map > Administration - Application > Responsibilities.
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.

The administrator sets the primary responsibility for a user by checking the Primary flag in the Responsibilities dialog box, in the Administration - User screen.

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 should 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.

NOTE: 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 section provides the procedure for exporting tab layouts to an XML file.

To export tab layouts

1. From the application level-menu, choose Navigate > Site Map > Administration - Application > Responsibilities.
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.

   NOTE: 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 section provides the procedure for importing tab layouts from an XML file you previously exported to.

To import tab layout to a target responsibility

1 From the application level-menu, choose Navigate > Site Map > Administration - Application > Responsibilities.

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

After creating a responsibility, you can enter the tasks commonly performed by employees who have that responsibility. These tasks will appear in the task list on the home page for these employees.

For each task, enter a caption and select an image file. Each task will be displayed as a hyperlink in the task list. Enter a description, which will also be displayed in the task list.

In addition, for each task, specify the view where the task is performed. When the user clicks on the hyperlink for this task on the home page, this view will appear.

Personalization of this type is already specified for various seed responsibilities.

To associate tasks with a responsibility

1 Log in as an administrator.

2 From the application-level menu, choose Navigate > Site Map > Administration - Application > Responsibilities.

3 In the Responsibilities list, select the responsibility you want to associate tasks with.

4 Click the Tasks view tab.

5 In the Tasks list, add a new record for each task associated with this responsibility, and enter information about each task in the new records.

Field	Guideline
Name	Enter the name of the task.
Caption	Enter a caption for the task that will be displayed as a hyperlink in the task list.
Description	Enter a description of the task that will be displayed under the caption in the task list.
Destination View	Click the select button and choose the view that will appear when the user clicks the hyperlink for this task.
Sequence	Optionally, specify the order in which this task will be displayed in the task list for this responsibility on the home page. If this field is left blank, tasks will be displayed in the order that you list them here.
Image	Select the graphic image that will be displayed as a hyperlink to the left of this task in the task list.
Group	This field is be used if search specifications are applied to filter the tasks that will be displayed in the task applet, if multiple task applets are associated with the responsibility.

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 may 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 need to be restarted.

To clear cached responsibilities

1 From the application-level menu, choose Navigate > Site Map > Administration - Application > Responsibilities.

2 In the Responsibilities list, click Clear Cache.

Additional Access Control Mechanisms

This section contains access control information that is supplemental to the basic access control mechanisms. It describes how to configure visibility for pop-up applets, pick applets, and drilldowns.

Configuring Visibility of Pop-Up and Pick Applets

Pop-up visibility determines what data will be shown when a pop-up pick applet is displayed, for example, when a user associates a contact with an account, or adds a sales representative to the sales team.

Pop-up visibility is usually set using the Popup Visibility Type property of the business component object in Siebel Tools. When pop-up visibility is set in this way, any pop-up based on that business component will show the same data for all users.

NOTE: This section provides configuration background information. It does not provide detailed instructions for working in Siebel Tools. For information about using Siebel Tools, see *Configuring Siebel eBusiness Applications*.

There are often circumstances where you need greater flexibility when determining what data should be shown in pop-up pick applets. For example:

- Most employees of your company only need to see positions for your organizations when they are assigning a sales representative to the sales team.
- Partner Managers need to see positions for your organization, as well as the partner organizations that they manage.

There are also many scenarios where your partners should have more restrictive visibility than your employees.

In order to meet this business requirement, Siebel eBusiness Applications have three capabilities that allow the developer to override the visibility set in the Business Component Popup Visibility Type property at the business component level in favor of another setting. The developer can:

- Set visibility of the Pick List object definition
- Use the visibility Auto All property
- Use the Special Frame Class and User Property

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 may 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 your Siebel application.

Using the Special Frame Class and User Property

The developer can use a special frame class and user property to set visibility for a pick applet on the applet object depending on which application is being used.

For example, if users are running Siebel Sales, the Pick Positions applet for the sales team will show positions only for the user’s organization. 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.
- 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

Configuring Drilldown Visibility

Drilldown visibility can occur in two different scenarios:

- **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 and not to the drilldown record.

- **Between different business objects.** If the original view and drilldown view are based on different business objects, moving from one to the other might require resetting the visibility in the destination to something other than its standard setting.

  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, for example, Sales Rep visibility on the drilldown view when drilling down.

  The Visibility Type property in a drilldown object only overrides the target 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 target view, the original visibility of the target 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 target 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.

Drilldown Visibility and Visibility Rules

After using a drilldown that directs you to another screen, the thread bar is updated. The current view displays its records using a kind of master-detail relationship, based on the link defined between the business components of the applets in the old view (before the drilldown) and those in the current view (after the drilldown).

In addition to the master-detail relationship described, the retrieved records within the view can be restricted by visibility rules determined by the link property Visibility Rule Applied.

If Visibility Rule Applied is set to Never, no additional visibility rule will be applied. The thread context's master-detail relationship determines the records visible in the view, regardless of current view's visibility settings. If you change the view using the viewbar, the thread context is retained. Records may be displayed that normally (without the thread context) are not visible in this new view.

On the other hand, if Visibility Rule Applied is set to Always, additional visibility rules are applied. The Siebel application may display an error message when performing the drilldown, to let the user know that he or she does not have the appropriate privileges to see the detail records.

Party Data Model

The S_PARTY table is the base table for all of the parties listed in Table 22 on page 215: 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 eBusiness Applications*.

In Figure 18 on page 276, 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. Sections that follow illustrate how the party data model applies to various particular parties.

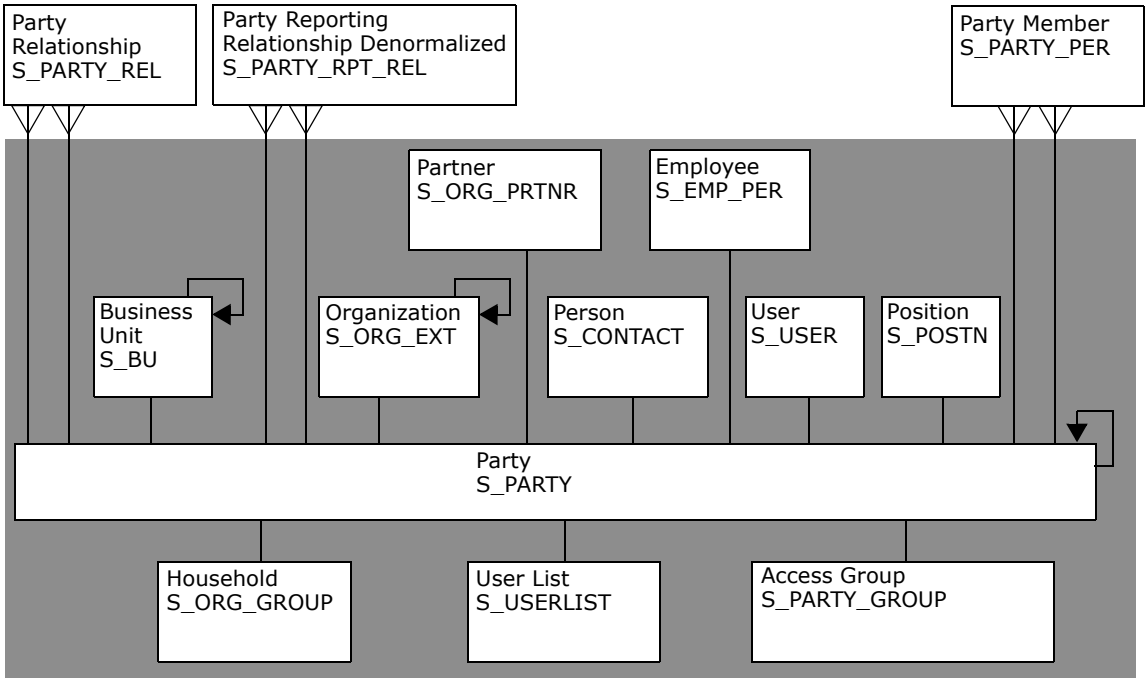


Figure 18. Party Data Model

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 may 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 may 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 may 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 19 on page 278, 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.

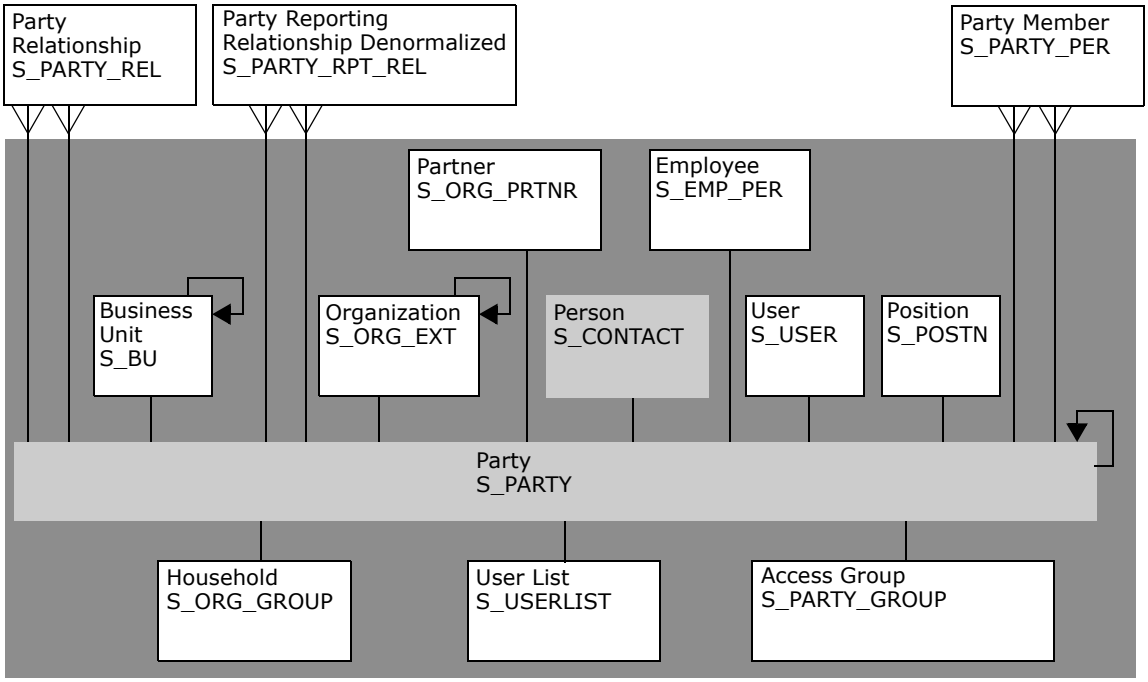


Figure 19. Person (Contact) Data Model

User Data Model

In Figure 20 on page 279, 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.

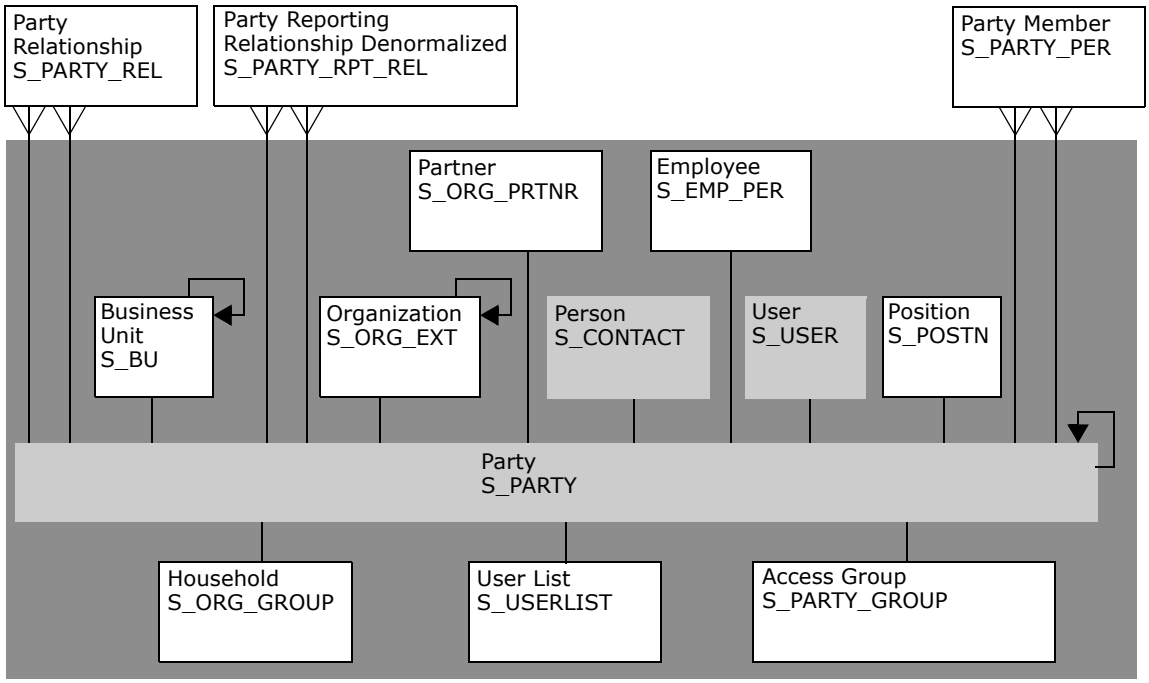


Figure 20. User Data Model

Employee Data Model

In Figure 21 on page 280, 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.

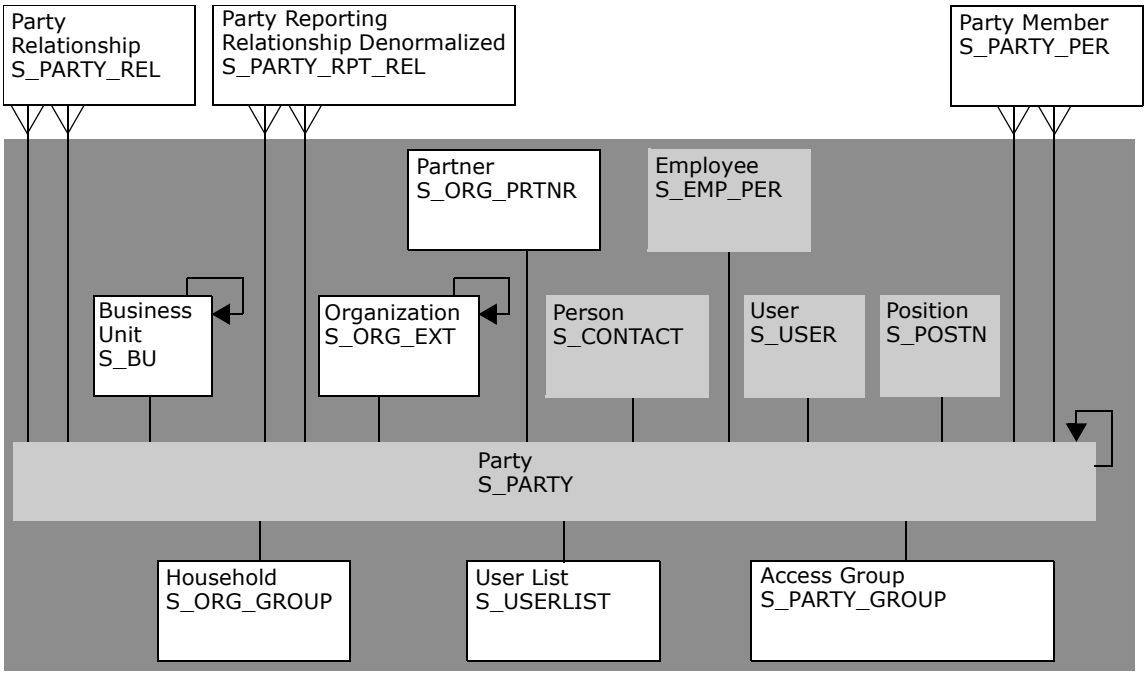


Figure 21. Employee Data Model

Position Data Model

In Figure 22 on page 281, the base table and extension table (S_POSTN) that define a Position are shaded.

NOTE: In positions, as in other areas of your Siebel application, 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).

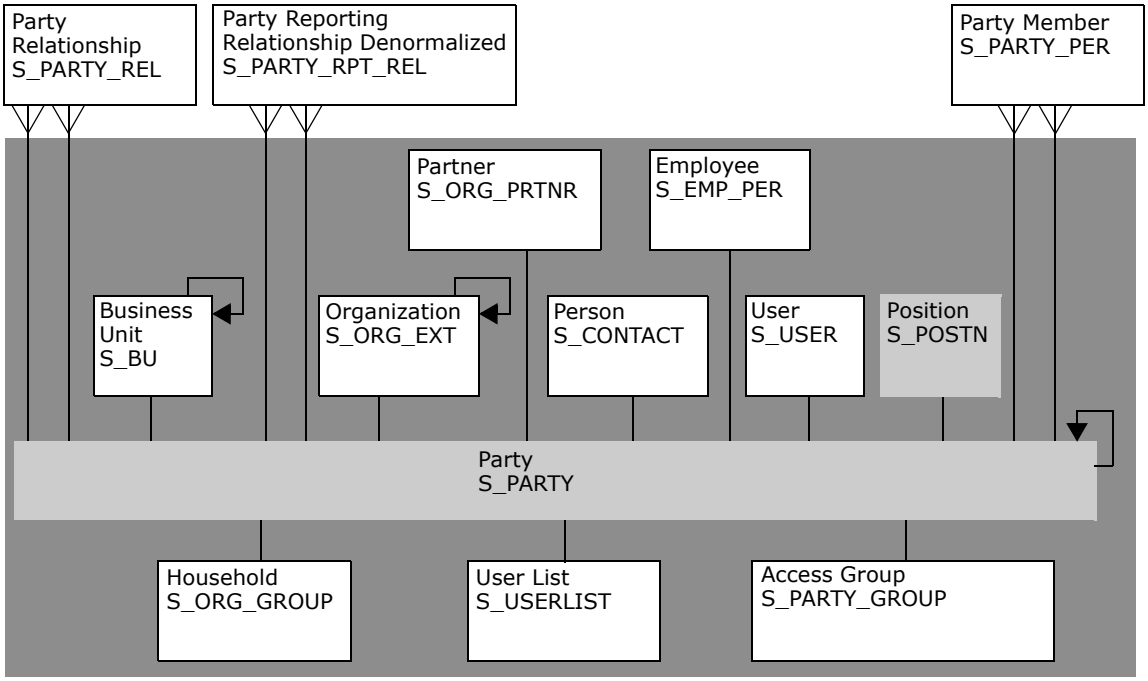


Figure 22. Position Data Model

Account Data Model

In Figure 23 on page 282, 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.)

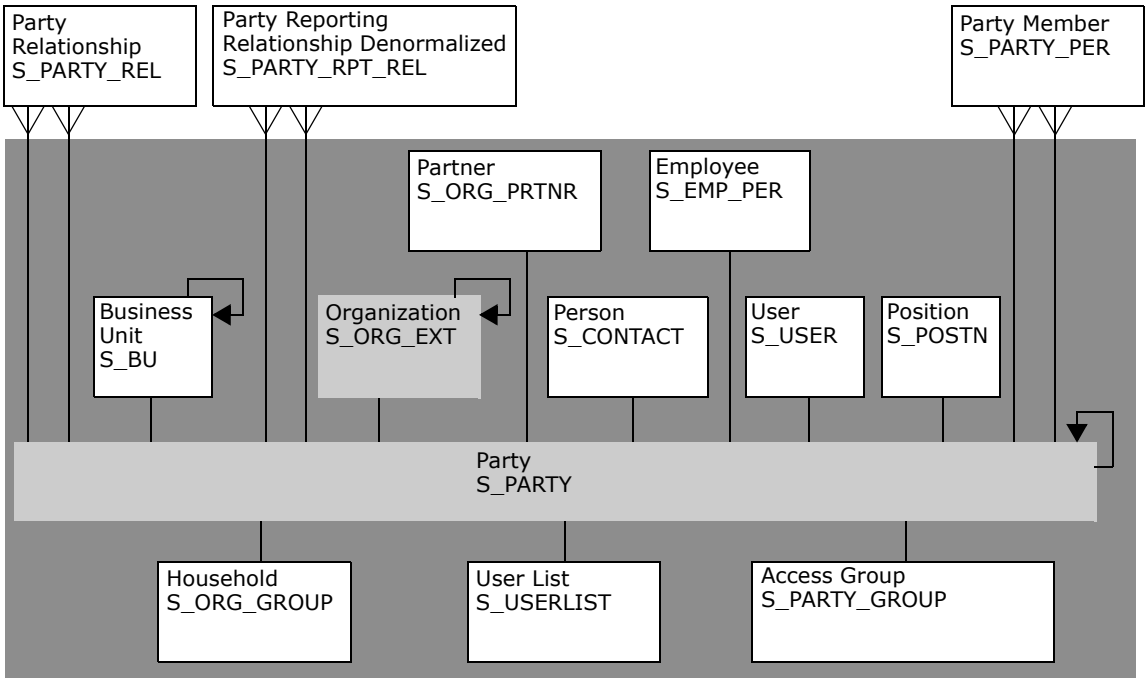


Figure 23. Account Data Model

Division Data Model

In Figure 24 on page 283, 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.)

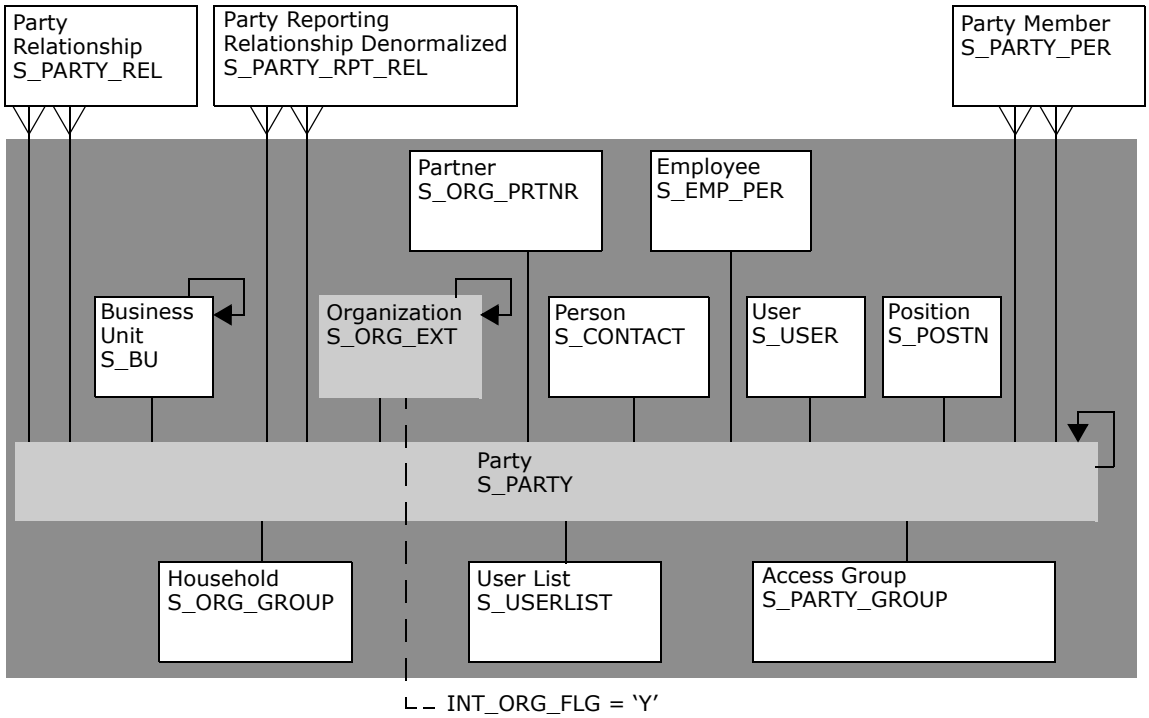


Figure 24. Division Data Model

Organization Data Model

In Figure 25 on page 284, 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.)

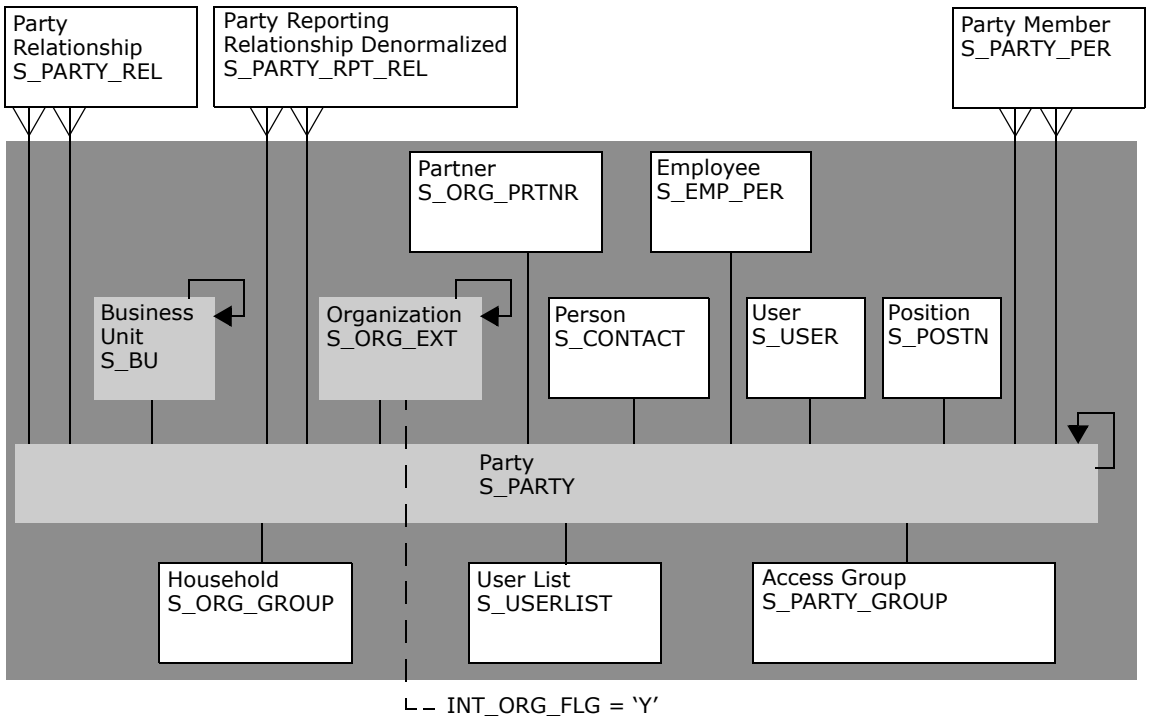


Figure 25. Organization Data Model

Partner Organization Data Model

In Figure 26 on page 285, 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.)

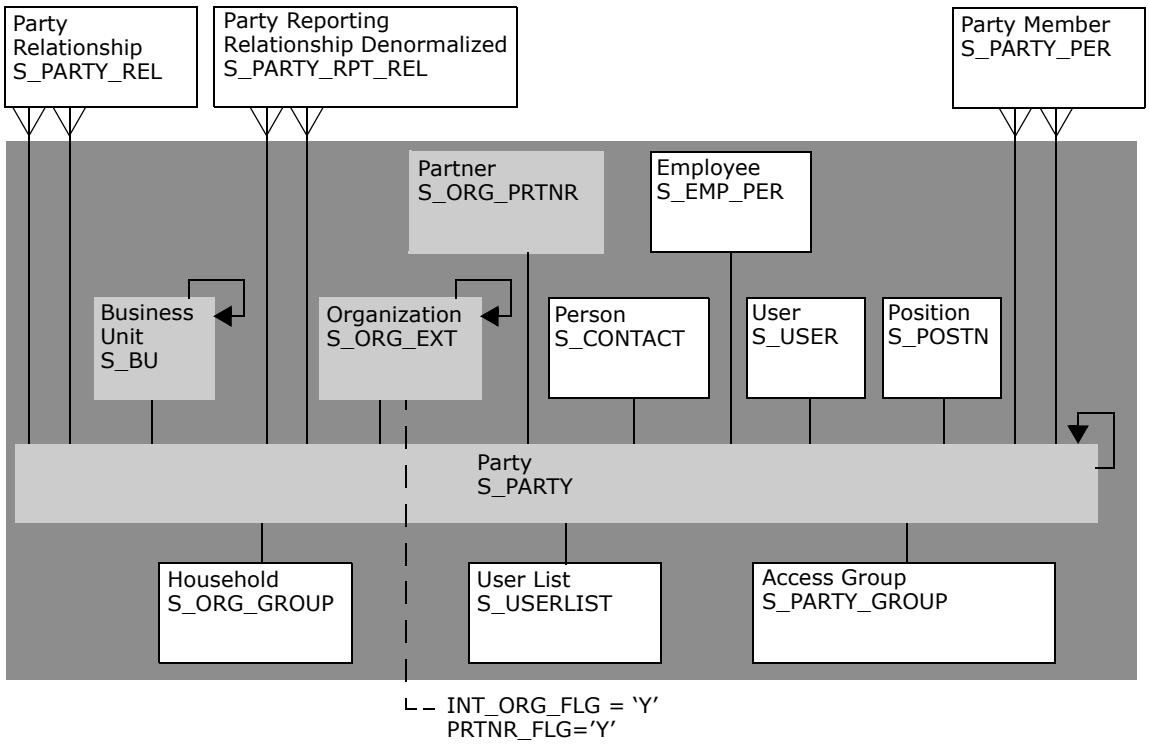


Figure 26. Partner Organization Data Model

Household Data Model

In Figure 27 on page 286, the base table and extension table (S_ORG_GROUP) that define a Household are shaded.

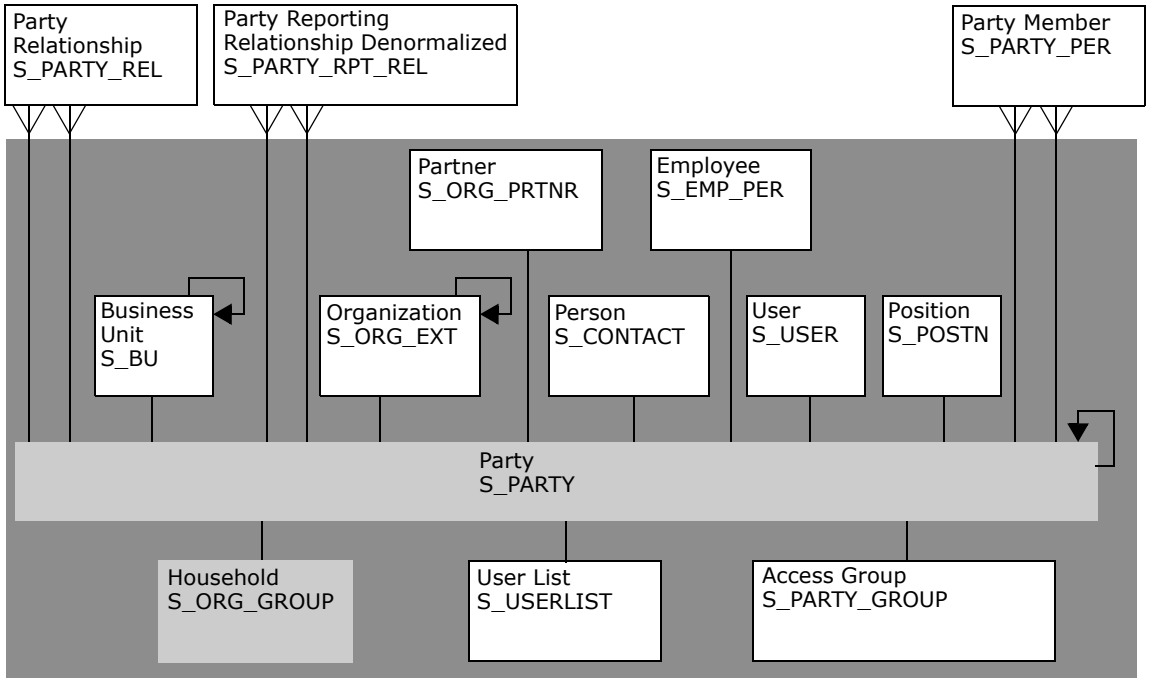


Figure 27. Household Data Model

User List Data Model

In Figure 28 on page 287, the base table and extension table (S_USERLIST) that define a User List are shaded.

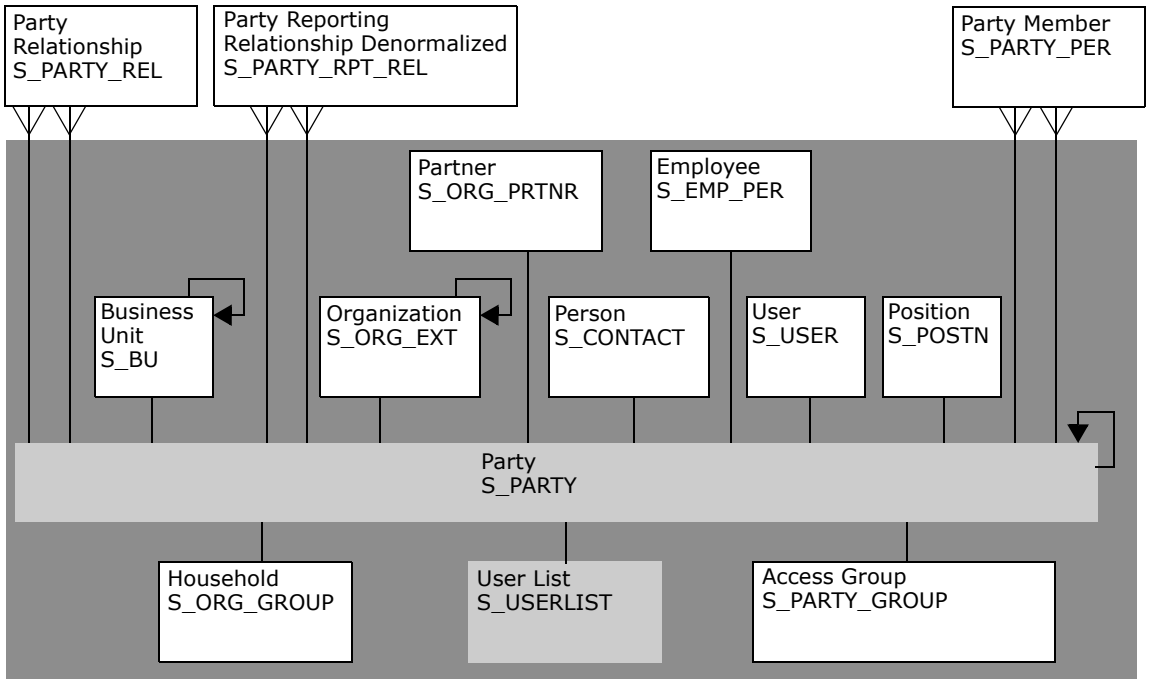


Figure 28. User List Data Model

Access Group Data Model

In Figure 29 on page 288, the base table and extension table (S_PARTY_GROUP) that define an Access Group are shaded.

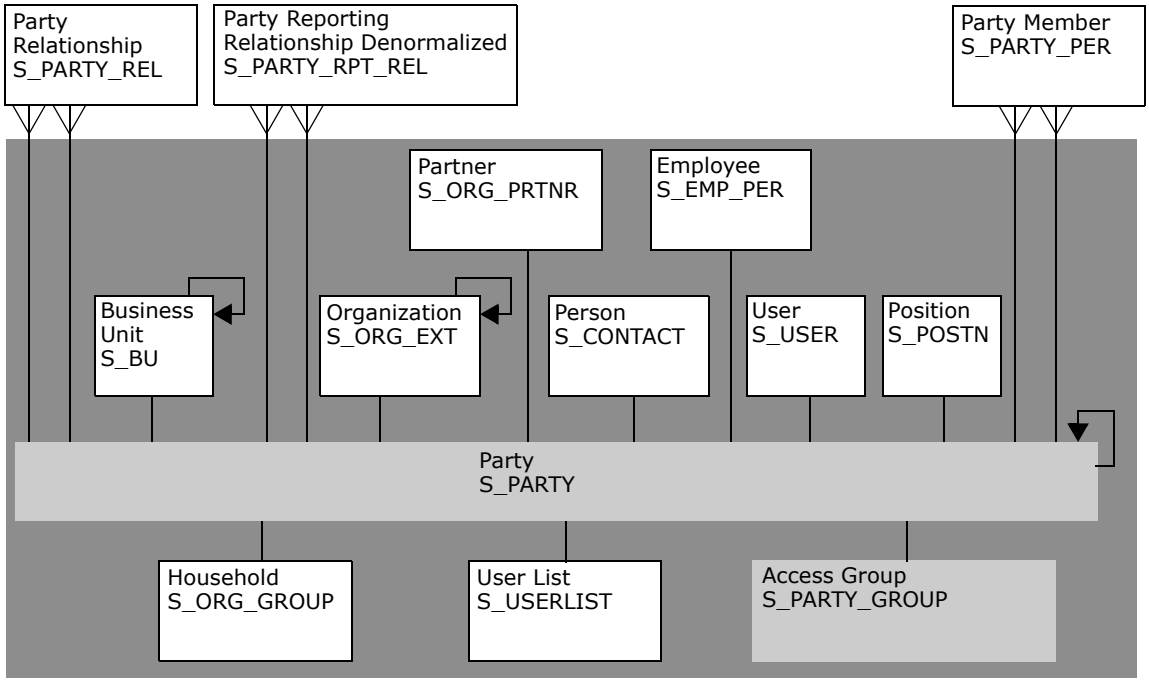


Figure 29. Access Group Data Model

A Troubleshooting Security Issues

This appendix provides troubleshooting tips and information about security-related issues that may occur in Siebel eBusiness Applications. It includes the following topics:

User Authentication Issues

This section describes problems that may 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 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 may 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 may 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 should log into the application using either a different AOM or a Siebel Dedicated 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 77 and related sections.

Adding Users or Changing Passwords Is Not Reflected in the Directory

If you add users or change passwords in a Siebel application and the changes are not reflected in the directory, make sure the `PropagateChange` parameter is set to `TRUE` for the security adapter. For more information, see "Siebel Gateway Name Server Parameters" on page 300.

Having Trouble Running the LDAP/ADSI Configuration Utility

Try running the utility from the machine that hosts the Siebel application you want to configure. The utility works best if run locally, rather than over the network.

Responsibilities in the Directory Conflict with Responsibilities in Siebel Applications

It is recommended that you assign user responsibilities in the directory or by using a Siebel application, but not both. For more information, see "Configuring Roles Defined in Directory" on page 138.

Upgrading Siebel Application Appears to Disable Checksum Validation

You must recalculate the security adapter's CRC checksum value whenever you upgrade your Siebel applications. For more information, see "Configuring Checksum Validation" on page 132.

"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 may 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 section describes problems that may 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 181.
- 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 may be new to the database but may already exist in the LDAP directory. This problem commonly occurs if the directory is not refreshed after deployment testing.

Try to create another user or use the LDAP console to check whether the user exists in the directory. Connect to the LDAP server, but instead of creating a new user, right-click on People and select Search.

After I Click Finish, the "View not accessible" Message Appears

The user was successfully created and was able to log in. However, the user that was created did not receive the appropriate responsibility and cannot access the view.

Change the New Responsibility field for the Anonymous User of the application to one that contains the necessary views.

When I Click the New User Link, Nothing Happens

Most likely, some or all of the User Registration workflow processes have not been activated; or if they are, the server needs to be restarted.

In the 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 may be another workflow that is being triggered and is disrupting the User Registration workflow. It is also possible that not all necessary workflows have been activated. You must activate all the necessary workflows.

To deactivate a disruptive workflow:

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 "System Preference" on page 310.

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 section 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 eSales). 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 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 242.

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:

NOTE: In general, parameters values related to security adapter configuration should be verified by your LDAP or ADSI administrator, or database administrator. Many values shown are examples only and may 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 applications deploying the Siebel Web Client.

The eapps.cfg file is located in the *SWEAPP_ROOT*\bin directory, where *SWEAPP_ROOT* is the directory in which you installed the SWSE.

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

CAUTION: Typically, password encryption is in effect for the eapps.cfg file, as determined by the setting `EncryptedPassword = TRUE`. In this case, values for `WebUpdatePassword` and `AnonPassword` would be encrypted. For details, see "Managing Encrypted Passwords in the eapps.cfg File" on page 34.

```
[swe]
Language = enu
Log = all
LogDirectory = D:\sea77\SWEApp\log
ClientRootDir = D:\sea77\SWEApp
WebPublicRootDir = D:\sea77\SWEApp\public\enu
WebUpdatePassword = test
IntegratedDomainAuth = FALSE

[defaults]
EncryptedPassword = TRUE
AnonUserName = GUESTCST
AnonPassword = GUESTCST
StatsPage = _stats.swe
SingleSignOn = TRUE
TrustToken = HELLO
UserSpec = REMOTE_USER
UserSpecSource = Server
```

```
DoCompression = TRUE
SessionTimeout = 300
GuestSessionTimeout = 900

[/prmportal_enu]
AnonUserName = guestcp
AnonPassword = ldap
ProtectedVirtualDirectory = /p_prmportal_enu
ConnectString = siebel.TCPIP.None.None://172.20.167.200:2320/siebel/eChannelObjMgr_enu

[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
```

The eapps.cfg file includes sections such as [swe], [defaults], and [connmgmt] and sections for individual Siebel applications, such as [/prmportal_enu] and [/callcenter]. 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.

In the eapps.cfg sample above, 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.

NOTE: You can use any plain text editor to add parameters and their values or to change values for existing parameters. When you edit configuration files, do not use a text editor that adds additional, nontext characters to the file.

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

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 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. The home page that is displayed likely provides an interface for the user to log in.

- **AnonPassword.** This parameter is the authenticated password that is paired with `AnonUserName`.

- **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 159.

- **DoCompression.** Specifies whether the SWSE will compress HTTP traffic.

  Compressing HTTP traffic, where it is feasible to do so, substantially reduces bandwidth consumption. This feature is supported on HTTP 1.1, and is not supported on HTTP 1.0.

  - When this parameter is set to FALSE, HTTP traffic will not be compressed. Use this setting if HTTP traffic should never be compressed. For example, you might use this setting if your proxy servers only support HTTP 1.0, or if the overhead of compression/decompression is of more concern to you than bandwidth constraints.
  - When this parameter is set to TRUE, HTTP traffic will be compressed if no proxy server is detected. However, if any proxy server is detected, it will be assumed not to support HTTP 1.1, and HTTP traffic will not be compressed. Use this setting if you want to compress HTTP traffic where feasible, but cannot be certain that proxy servers that do not support HTTP 1.1 may be used.
  - When this parameter is set to `CompressProxyTraffic`, HTTP traffic will always be compressed. Use this setting for Siebel applications only if you are certain that any proxy server that resides in front of your Siebel application users supports HTTP 1.1.

  You can set this parameter for individual Siebel applications, or set it for multiple applications by defining it in the [defaults] section. For example, you might set this parameter to `CompressProxyTraffic` for employee applications accessed on an intranet—if you know that any proxy servers that are deployed support HTTP 1.1. Otherwise, set this parameter to either FALSE or TRUE (such as in the [defaults] section).

  NOTE: Because it is impossible to know what type of proxy server an external user (that is, a partner or customer) may be using, the setting `CompressProxyTraffic` should be used for employee applications only, not for customer or partner applications.

- **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 use the SWSE configuration utility. 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 34.

- **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 (in cookieless mode).

  For more information about cookies, see "Cookies and Siebel Applications" on page 168.

- **GuestSessionTimeout.** The session timeout for guest users. The default is 300 seconds (five minutes). For more information about session timeouts, see the description for the `SessionTimeout` parameter.

- **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). Standard sessions are those where users log in using their registered user name and password.

  NOTE: All the session timeouts mentioned above deal with the session inactivity. In other words, if they are set to 3600 seconds, then it requires one hour of session inactivity for that session to time out. The session inactivity means there should be no request made to the server on that session. Any act that pings the server, including message bar updates and calendar alarm functionality, resets the session timeout period. If the update interval is less than the `SessionTimeout` value, the session will never timeout.

- **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 should be extracted from the certificate's CN (Common Name) attribute.

  For more information, see "User Specification Source" on page 160.

- **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` would be "`CERT_SUBJECT`"/"`CN`". For other UNIX platforms, use "`REMOTE_USER`" for `UserSpec`. The `SubUserSpec` setting is disregarded.

  For more information, see "User Specification Source" on page 160.

- **UserSpecSource.** In a Web SSO implementation, this parameter specifies the source from which the SWSE derives the user credentials: Server, if from the usual Web server user name field; Header, if the variable is within the HTTP request header.

  For more information, see "User Specification Source" on page 160.

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 the protected virtual directory for a Siebel application. This parameter specifies a Web server virtual directory that represents the protected location of the Siebel application. This parameter must have a value in a Web SSO implementation, and is optional in other implementations.

  The protected directory allows you to configure your Web server or third-party authentication software to require user authentication to access specific Siebel application views. Requests for any views that require explicit login are redirected to this virtual directory.

  For more information, see "Creating Protected Virtual Directories" on page 149.

  For example, if you used the suggested name for the protected virtual directory for Siebel eService, enter:

  ```
  [/eservice]
  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]
  ProtectedVirtualDirectory = /eservice
  ```

  Otherwise, a Web Authentication Failed message may 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. The Siebel application redirects 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 55.

- **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.
- **PeerCertValidation.** Independently verifies that the hostname of the SWSE machine 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 Object Manager or the eService 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 = LDAP` at the Enterprise level, and `Security Adapter Mode = ADSI` at the component level for the eService 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: For detailed information about how to set parameters on the Siebel Gateway Name Server, using Siebel Server Manager, 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 may 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 132.

- **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 credentials in the database through Siebel applications. When an administrator then adds a user or changes a password from within a Siebel application or a user changes a password or self-registers, the change is propagated to the database.
- **Security Adapter Dll Name (alias DBSecAdpt_SecAdptDllName).** Specifies the DLL that implements the security adapter API required for integration with Siebel eBusiness Applications. The file extension need not be explicitly specified. For example, sscfsadb.dll implements the Siebel database security adapter in a Windows implementation, and sscfsadb.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 may 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 DSHashAlgorith parameter. For details, see "Configuring Password Hashing" on page 125.
- **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 Systems (supported for existing customers only). For details, see "Configuring Password Hashing" on page 125.

Parameters for LDAP/ADSI Authentication

The following parameters are for LDAP/ADSI authentication, and are defined for named subsystems of type InfraSecAdpt_LDAP (that is, they may 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 ADS, the password is stored using ADS 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 ADS with the AOM when a user requests the login page, or else anonymous browsing of the directory is required.

  You enter this parameter as a full distinguished name (DN), for example "uid=APPUSER, ou=People, o=*companyname.com*"—including quotes—for LDAP. The security adapter uses this name to bind.

  NOTE: You *must* implement an application user.

- **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`*`"`. "o" denotes "organization" and is typically your Web site's domain name. "ou" denotes "organization unit" and is the subdirectory in which users are stored.

  A typical entry for an ADS server might be `BaseDN = "CN=Users, DC=qatest, DC=siebel, DC=com"`. Domain Component (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for the user objects in the directory. Therefore, adjust the number of CN and DC entries to represent your architecture.

- **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 132.

- **Credentials Attribute Type (alias CredentialsAttributeType).** Specifies the attribute type that stores a database account. For example, if `CredentialsAttributeType = 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`*` password=`*`P`*, where *U* and *P* are credentials for a database account. There may 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. For information on shared database accounts, see "Configuring the Shared Database Account" on page 134.

- **Hash DB Cred (alias HashDBPwd).** Specifies password hashing for database credentials passwords. For details, see "Configuring Password Hashing" on page 125.

- **Hash User Password (alias HashUserPwd).** Specifies password hashing for user passwords. Uses the hashing algorithm specified using the `HashAlgorith` parameter. For details, see "Configuring Password Hashing" on page 125.

- **Password Attribute Type (alias PasswordAttributeType).** Specifies the attribute type under which the user's login password is stored in the directory.

  `PasswordAttributeType = userPassword` is the only supported value for LDAP. When a user with user name HKIM attempts to log in, the security adapter compares the value in the userPassword attribute for HKIM with the password the user enters.

  This parameter is used by the LDAP security adapter only. (ADS does not store the password in an attribute, so this parameter is not used with the ADSI security adapter.)

- **Password Expire Warn Days (ADSI only) (alias PasswordExpireWarnDays).** Specifies the number of days to display a warning message before a password expires.

  This parameter is used by the ADSI security adapter only.

- **Port (alias Port).** Specifies the port on the server machine that is used to access the LDAP server. Typically, use 389, the default value, for standard transmission or use 636 for secure transmission.

  This parameter is used by the LDAP security adapter only. (For ADS, you set the port at the directory level, so this parameter is not used with the ADSI security adapter.)

- **Propagate Change (alias PropagateChange).** Set this parameter to TRUE to allow administration of the directory through Siebel applications. When an administrator then adds a user or changes a password from within a Siebel application or a user 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 = 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 Directory" on page 138.

- **Security Adapter Dll Name (alias SecAdptDllName).** Specifies the DLL that implements the security adapter API required for integration with Siebel eBusiness Applications. The file extension need not be explicitly specified. For example, sscfldap.dll implements the LDAP security adapter in a Windows implementation. On supported UNIX platforms, the file name may 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 machine on which the LDAP or ADS server runs, for example ldapserver.siebel.com.

  NOTE: For ADSI, this parameter must be populated with the ADS server's complete machine name, not its IP address—otherwise, users will be unable to change their passwords through the Siebel application. This restriction is due to a limitation of the ADSI client library used by the ADSI security adapter.

- **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 CredentialsAttributeType.

  For example, if SharedCredentialsDN = "uid=HKIM, ou=People, o=siebel.com", then when any user is authenticated, the security adapter retrieves the database account from the appropriate attribute in the HKIM record. This parameter's default value is an empty string.

- **Siebel Username Attribute Type (alias SiebelUsernameAttributeType).** If UseAdapterUsername = TRUE, this parameter is the attribute from which the security adapter retrieves an authenticated user's Siebel user ID. If this parameter is left empty, the 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 Systems (supported for existing customers only). For details, see "Configuring Password Hashing" on page 125.

- **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 = 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 = 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 135.

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/ADSI security adapters, in "Siebel Gateway Name Server Parameters" on page 300.

- **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:

- **OM - Proxy Employee (alias ProxyEmployee).** User ID of the proxy employee.

  For information about the proxy employee, see "Seed Data" on page 311.

- **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 135.

Siebel Application Configuration File Parameters

A configuration file exists for each Siebel eBusiness Application for each language. The parameters in the file determine how the user interacts with the 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.

  NOTE: Most of the security-related parameters applicable to Siebel Servers (and, consequently, Siebel Web Clients) are stored in the Name Server. Parameters in the [SWE] section of the configuration file do apply to Siebel Servers. However, most other parameters described in this section do *not* apply to the Siebel Server.

- **Configuration file on the Siebel Mobile Web Client or Dedicated Web Client.** For users connecting through the Siebel Mobile Web Client or Dedicated 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 Dedicated Web Client connects directly to the server database; it bypasses the Siebel Server.

  NOTE: LDAP/ADSI security adapter configuration does not apply to Siebel Mobile Web Client.

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

In a given configuration file, some parameters may not appear by default. Others may appear with a preceding semicolon (;), indicating that the parameter is a comment and is not being interpreted. The semicolon must be deleted to make the parameter active. Changes to an application configuration file are not active until you restart the Siebel Server or Siebel client.

CAUTION: 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 [SWE] Section

The following parameters are located in the [SWE] section of the application configuration file. These parameters apply to all Siebel client types.

- **AllowAnonUsers.** (TRUE or FALSE) Unregistered users are not allowed access to this Siebel application if this parameter value is FALSE.
- **SecureLogin.** (TRUE or FALSE) If TRUE, the login form completed by the user is transmitted over Secure 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.

  CAUTION: 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 Secure Views" on page 163.

  For information about the Secure attribute for a view, see *Configuring Siebel eBusiness Applications*.

Parameters in [InfraSecMgr] Section

The following parameters are located in the [InfraSecMgr] section of the application configuration file.

NOTE: These parameters apply to Siebel Mobile Web Client and Dedicated Web Client only. For SecAdptMode and SecAdptName, see the descriptions for the equivalent parameters in "Siebel Gateway Name Server Parameters" on page 300.

- **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 Dedicated 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 Dedicated Web Client configuration, the section [LDAPSecAdpt] is created by default in the configuration file if you configure LDAP using the LDAP/ADSI Configuration Utility.
  - For ADSI authentication, specify ADSISecAdpt (or another name of your choice). For Dedicated Web Client configuration, the section [ADSISecAdpt] is created by default in the configuration file if you configure ADSI using the LDAP/ADSI Configuration Utility.
  - For a custom security adapter, specify a name such as SecAdpt_Custom. (You must add the applicable section to the file.)

NOTE: 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.

The following parameter applies *only* to the Siebel Dedicated Web Client:

- **UseRemoteConfig.** 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 Siebel Dedicated Web Client" on page 139.

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.

NOTE: These parameters apply to Siebel Mobile Web Client and Dedicated 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 300.

- **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 132.

- **DBSecAdpt_PropagateChange.** Set this parameter to TRUE to allow administration of credentials in the database through Siebel applications. When an administrator then adds a user or changes a password from within a Siebel application or a user changes a password or self-registers, the change is propagated to the database.

  For Siebel Dedicated Web Client, the system preference SecThickClientExtAuthent must also be set to TRUE. For details, see "System Preference" on page 310.

- **DBSecAdpt_SecAdptDllName.** Specifies the DLL that implements the security adapter API required for integration with Siebel eBusiness Applications. The file extension need not 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 Data Source Section

The following parameters are located in the data source section of the application configuration file, such as [ServerDataSrc] (for Siebel Dedicated 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 Systems (supported for existing customers only). For details, see "Configuring Password Hashing" on page 125.
- **DSHashUserPwd.** Specifies password hashing for user passwords. Uses the hashing algorithm specified using the `DSHashAlgorith` parameter. For details, see "Configuring Password Hashing" on page 125.
- **IntegratedSecurity.** Applicable only to Siebel Dedicated Web Client, with Oracle or Microsoft SQL Server database. For details, see "Security Adapters and Siebel Dedicated Web Client" on page 139.

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.

LDAP and ADSI authentication do not apply to the Siebel Mobile Web Client.

The following parameters also apply to the Siebel Dedicated Web Client. 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 300.

- **ApplicationPassword**
- **ApplicationUser**
- **BaseDN**
- **CRC**
- **CredentialsAttributeType**
- **HashAlgorithm**
- **HashDBPwd**
- **HashUserPwd**
- **PasswordAttributeType**
- **PasswordExpireWarnDays**
- **Port**
- **PropagateChange**
- **RolesAttributeType**
- **SecAdptDllName**
- **ServerName**

- **SharedCredentialsDN**
- **SiebelUsernameAttributeType**
- **SingleSignOn**
- **SslDatabase**
- **TrustToken**
- **UseAdapterUsername**
- **UsernameAttributeType**

System Preference

You can set an authentication-related system preference for Siebel applications in the Administration - Application screen. System preferences are enterprise-wide settings.

Following is the authentication-related system preference:

- **SecThickClientExtAuthent.** (TRUE or FALSE) To allow security adapter authentication for users who log in through the Siebel Dedicated Web Client, you must set the SecThickClientExtAuthent system preference to TRUE. This system preference has no effect on security adapter authentication for users who log in through the Siebel Web Client.

To edit a system preference

1. Log in as an administrator to a Siebel employee application.
2. From the application-level menu, choose Navigate > Site Map > Administration - Application > System Preferences.
3. In the System Preferences list, select a system preference to edit.
4. Edit the entry in the System Preference Value column, then commit the record.
5. Restart the Siebel Server.

C Seed Data

This appendix describes seed data provided for your Siebel eBusiness 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 eSales, Siebel eService, Siebel eCustomer, Siebel Training, Siebel Events, and Siebel eMarketing.

Seed Employee

One Employee record is provided as seed data at installation, as described in Table 26 on page 311. This record does not have a database login or a responsibility, but, like other employees, it does have a position and an organization.

Customer users, such as Siebel eService users, are not assigned their own position or organization. When a customer user logs in, the application programmatically associates the proxy employee with the user. The proxy employee provides the following functions:

- Data subsequently created by the user is associated with the organization of the proxy employee, which allows the data to display in views that implement organization access control.
- The user can see data created by the user and by others in views that implement organization access control.

The proxy employee is specified at the application level as a Name Server parameter.

For information about associating the proxy employee with an application, see "Siebel Gateway Name Server Parameters" on page 300.

For information about organization access control, see "Access Control Mechanisms" on page 220.

Table 26. Proxy Employee Seed Data Field Values

Last Name	First Name	User ID	Responsibility	Position	Organization
Proxy	Employee	PROXYE	None	Proxy Employee	Default Organization

Seed Users

Table 27 on page 312 describes nonemployee User records provided as seed data.

Table 27. 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 28 on page 312. 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.

NOTE: For all responsibilities provided in seed data, refer to those listed in the Siebel application.

Table 28. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
Web Anonymous User	Default Organization	Views provided for anonymous browsing	Customer applications
Web Registered User	Default Organization	Views provided for a typical registered user	Customer applications
Web Delegated Customer Administrator	Default Organization	Includes views in the Web Registered User responsibility plus views for administering users	Customer applications
Web Corporate User	Default Organization	Views for eSales corporate user	eSales
Web Purchasing Manager	Default Organization	Views for eSales purchasing manager	eSales
Unregistered Partner Agent	Default Organization	Views provided for anonymous browsing	Siebel Partner Portal
Self-Registered Partner Agent	Default Organization	Limited set of views provided for a user who self-registers	Siebel Partner Portal

Table 28. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
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
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

To see the views included in a responsibility

1. From the application-level menu, choose Navigate > Site Map > Administration - Application > Responsibilities.
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 should not be assigned to any individual user. The login credentials are login = LDAPUSER and password = LDAPUSER.

CAUTION: It is strongly recommended that an administrator change the password.

D Addendum for Siebel Financial Services

This appendix provides 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

The applications listed in Table 29 on page 316 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 may 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 29. Siebel Financial Services Applications

Tools Application Object Name	Users	Options	Products
Siebel Financial Services	Employees	Siebel Sales Siebel Service Siebel Call Center Siebel Partner Manager	Siebel Finance Siebel Insurance Siebel Healthcare
Siebel Financial Services ERM	Employees		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		Siebel PRM for Finance Siebel Agent Portal Siebel Healthcare Group Portal Siebel Healthcare Provider Portal
Siebel eBanking	Customers		Siebel eBanking
Siebel Financial eBrokerage	Customers		Siebel eBrokerage
Siebel Financial eService	Customers		Siebel Insurance/ Healthcare eService Siebel Healthcare Member Portal
Siebel Financial eEnrollment	Customers		Siebel Healthcare Enrollment Portal
Siebel FINS eSales	Customers		Siebel eSales
Siebel Financial eCustomer	Customers		Siebel eCustomer
Siebel eEvents Management	Customers		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 section 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 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 "Registering and Administering Users for Siebel Financial Services" on page 319.

Implementing LDAP and ADSI Security Adapter Authentication

Implementation of LDAP/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. References throughout this section to the eapps.cfg file should be replaced by references to the eapps.cfg file *and* the eapps_fins.cfg file.

Setting Up Security Adapter Authentication: A Scenario

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 as they are documented for GUESTCST in "Seed Data" on page 311.

When you add TESTUSER to the database, you should 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 325 and "Seed Data" on page 311.

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. References throughout this section to the eapps.cfg file should be replaced by references to the eapps.cfg file and the eapps_fins.cfg file.

Setting Up Web SSO: A Scenario

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 as they are documented for GUESTCST in "Seed Data" on page 311.

When you add TESTUSER to the database, you should 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 325 and "Seed Data" on page 311.

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 section 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 30 on page 319 lists the sections in the eapps.cfg file and in the eapps_fins.cfg file, which are provided for Siebel Financial Services applications.

Table 30. 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		[/fins]
Siebel Financial Services ERM		[/finserm]
Siebel Marketing	[/marketing]	
Siebel Financial PRM		[/finsechannel]
Siebel eBanking		[/finsebanking]
Siebel Financial eBrokerage		[/finsebrokerage]
Siebel Financial eService		[/finseservice]
Siebel Financial eEnrollment		[/finseenrollment]
Siebel FINS eSales		[/finsesales]
Siebel Financial eCustomer		[/finsecustomer]
Siebel eEvents for Finance	[/eevents]	

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 324.

Registering and Administering Users for Siebel Financial Services

This section contains information for Siebel Financial Services applications that differs from the information in the section 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 as they are documented for GUESTCST in "Seed Data" on page 311.

For information about seed data specific to Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 325.

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 325.

Self-Registration

User self-registration is default functionality for the Siebel Financial Services applications listed below.

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.

Adding a New Partner User

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.

NOTE: 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 311. 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 sections 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 following exceptions.

Editing Personal Information

Depending on the Siebel customer application, the user may 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 note affects access control to Opportunities in any view that uses personal, position, or organization access control.

NOTE: 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 should be included in lists of the party types that can be members of access groups.

Administering Access-Group Access Control

Access-group access control is administered as documented in other sections of this guide with the following exceptions. The following sections augment the sections on administering various party types.

Associating Access Groups with Data

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

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. From the application-level menu, choose Navigate > Site Map > Administration - Catalog > Catalogs.

   The Catalogs list appears.

2. Select a catalog.
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

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. From the application-level menu, choose Navigate > Site Map > Administration - Catalog > Catalogs.

   The Catalogs list appears.

2. 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. 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 section contains information for Siebel Financial Services applications that differs from the information in the appendix that contains Siebel application configuration file names in other sections of this guide, or that otherwise warrants mention.

Table 31 on page 325 contains the names of application configuration files that are used by Siebel Financial Services applications.

Table 31. 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
Siebel Financial eCustomer	finsecustomer.cfg
Siebel eEvents Management	eevents.cfg

Seed Data for Siebel Financial Services

This section contains information for Siebel Financial Services applications that differs from the information in "Seed Data" on page 311 or that otherwise warrants mention.

The seed data related to user access is also provided with Siebel Financial Services applications.

In this section, the term "Siebel Financial Services customer applications" represents the group denoted as customer applications in Table 29 on page 316.

Seed Users

Table 32 on page 326 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 311, functions as the anonymous user for Siebel Financial PRM, the partner application in Siebel Financial Services. Its responsibility provides views for anonymous browsing, and the responsibility in its New Responsibility field provides views for users who self-register.

Table 32. 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		Siebel Financial Services ERM

Seed Responsibilities

Table 33 on page 326 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 33. 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.

Table 33. Seed Responsibilities

Name	Organization	Description and Comments	Used by These Applications
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. A manager should be assigned this responsibility in addition to a responsibility that contains views for a regular user.	Siebel Financial Services ERM.

For information about creating and modifying responsibilities, see Chapter 10, "Configuring Access Control."

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X