SIEBEL eBusiness 7

SECURITY GUIDE FOR SIEBEL *e*BUSINESS APPLICATIONS

VERSION 7.5.3

JULY 2003

12-FNVC73

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

Contents

Introduction

Chapter 1. About Security Resources for Siebel Applications

Chapter 2. Configuring for Security: Overview

Chapter 3. Physical Deployment and Auditing

Chapter 4. Communications and Data Encryption

Chapter 5. User Authentication Overview

Chapter 6. Security Adapter Authentication

Chapter 7. Web Single Sign-On and Remote Authentication

Chapter 8. Authentication Details

Chapter 9. User Administration

Chapter 10. Access Control

Appendix A. Troubleshooting Security Issues

Appendix B. Seed Data

Appendix C. Addendum for Siebel Financial Services

Index

Introduction

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

NOTE: This book replaces *Authentication and Access Control Administration Guide*. It also replaces *Authentication and Access Control Administration Guide Addendum for Siebel Financial Services*.

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

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

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

Product Modules and Options

This *Siebel Bookshelf* contains descriptions of modules that are optional and for which you may not have purchased a license. Siebel's Sample Database also includes data related to these optional modules. As a result, your software implementation may differ from descriptions in this Bookshelf. To find out more about the modules your organization has purchased, see your corporate purchasing agent or your Siebel sales representative.

How This Guide Is Organized

Major topics covered in this guide include:

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

Additional Resources

For additional information on topics related to those covered in this book, see the following books:

- *Siebel Server Installation Guide* for the operating system you are using, for information about server installation procedures.
- *Siebel Server Administration Guide*, for information about managing Siebel Server components such as Application Object Manager.
- *Siebel Web Client Administration Guide*, for information about deploying Siebel clients and about installing Siebel Mobile and Dedicated Web Client.
- *Upgrade Guide* for the operating system and database you are using, for information about upgrading Siebel eBusiness Applications.

Revision History

Security Guide for Siebel eBusiness Applications

Version 7.5.3

Table 1. Changes Made in Version 7.5.3

Topic	Revision
"Using Industry Standards" on page 24	Added note about using Microsoft Crypto on different machines.
"Changing Default Passwords" on page 39	Added paragraph about limitations in the availability of the Password and Confirm Password fields when using external authentication. Added paragraph about the implications of changing passwords at both the Enterprise and Component level.
"Configuring Siebel Enterprise for Microsoft Crypto or RSA Encryption" on page 64	Moved content about keyfile exchange here from a previously separate section.
"Configuring Siebel Enterprise or Siebel Server for SSL Encryption" on page 66 "Configuring Siebel Web Server Extension for SSL Encryption" on page 70	New for 7.5.3: Added sections about configuring Secure Sockets Layer (SSL) encryption and authentication for Siebel Server and Siebel Web Server Extension.
"Configuring Web Clients for Encryption" on page 73	Moved content about session cookies here from a previously separate section.
"Business Component Encryption" on page 77	Removed content about the Standard Encryptor, which is no longer supported. Added information about restrictions and requirements for encrypted field data and business component fields used for this purpose.
"ADSI Adapter Requirements" on page 105	Updated section on requirements for using the security adapter for ADSI.
"Implementing LDAP and ADSI Security Adapter Authentication" on page 111	Updated note about authentication issues for multiple Siebel client types.

Table 1. Changes Made in Version 7.5.3

Topic	Revision
"Editing Parameter Values in the Application Configuration File" on page 124	Updated description of `PasswordAttributeType` parameter.
"Implementing Web SSO Authentication" on page 136	Updated note about authentication issues for multiple Siebel client types.
"Setting Up Web SSO: A Scenario" on page 138	Updated description of Siebel Server and Application Object Manager in a Web SSO environment.
"Editing Parameter Values in the Application Configuration File" on page 149	Updated description of `AllowAnonUsers` parameter in application configuration file.
"User Password Encryption" on page 170	Updated note about password encryption utility. Added optional procedure step for modifying the `AnonPassword` parameter in the eapps.cfg file. Added information about how password encryption affects running Siebel Server components.
"Credentials Password Encryption" on page 173	Updated note about password encryption utility.
"Adapter-Defined User Name" on page 184	Deleted obsolete note about duplicating Siebel user ID data in a directory.
"Secure Views" on page 190	Updated description of effect of `SecureBrowse` parameter.
"Password Expiration" on page 213	Enhanced section to specify some requirements specific to ADSI, and to document using the parameter `PasswordExpireWarnDays`.
"Changing the Active Position" on page 284	Added note about relationship of data visibility and active position.
"Access Control for Data" on page 289	Added note about divisions and access groups.

Table 1. Changes Made in Version 7.5.3

Topic	Revision
"Party Data Model" on page 295	Added illustrations pertaining to data models for User List and Access Group parties. Added statement about promoting a contact to a user.
"How Parties Relate to Each Other" on page 307	Added information about the function of S_PARTY_PER and S_PARTY_REL tables.
"Position-Based Access Control" on page 310	In subsection on manager access control, deleted an incorrect note. Enhanced subsection on manager access control, primarily to add information about Manager List Mode.
"Setting Up Organizations" on page 324	Added information about the Employee Organization field for the Employee business component.
"Setting Up Divisions" on page 326	Updated description of Organization Type field.
"Responsibilities" on page 336	Revised for 7.5.3: Mentioned that default tab layouts are associated with responsibilities. Added note about requirement for restarting Application Object Manager after modifying visibility or responsibility settings.
"Associating a Responsibility with Organizations" on page 337	Added note about associating organizations with responsibilities.
"View Access Control Properties" on page 348	Added information about the view property Visibility Applet. Deleted incorrect note in subsection on manager access control.
"Associating Access Groups with Data" on page 369	Updated description of Cascade button.

Table 1. Changes Made in Version 7.5.3

Topic	Revision
“Managing Tab Layouts Through Responsibilities” on page 372	New for 7.5.3: Added new subsection about managing default tab layouts through responsibilities.
“Creating and Administering Roles” on page 377	Revised for 7.5.3: Updated section to remove references to managing tab layouts through roles. Default tab layouts are now managed through responsibilities.
“Configuring Drilldown Visibility” on page 385	Added information about drilldown visibility and visibility rules.
“User Authentication Issues” on page 393	Updated discussion of authentication requirements for using Server Manager.
“Seed Responsibilities” on page 401	Added reference to *Release Notes* for responsibilities provided in seed data.

Additional Changes

- For “Security Settings for the Web Browser” on page 47, moved most of the content to a deployment chapter in *Siebel Web Client Administration Guide*.
- In Chapter 10, “Access Control,” removed heading level “Supplemental Access Control” due to chapter restructuring. Added new section “Additional Access Control Mechanisms” on page 383 to contain some of the content previously included under “Supplemental Access Control.”
- Removed former Chapter 10, “Siebel Application Configuration File Names.”

January 2003 Bookshelf

Table 2. Changes Made in Version 7.5, Rev. A for January 2003 Bookshelf

Topic	Revision
"Bibliography of Security References" on page 35	New section that lists outside resources for security-related issues. Includes books and Web sites.
"Adding a Password for Updating Web Server Images" on page 46	New section that describes security issues for Web server image caching.
"Security Settings for the Web Browser" on page 47	New section that describes how Web browser security settings impact Siebel applications.
"Securing Siebel Reports Server" on page 58	New section on securing communications with Siebel Reports Server.
"Password Expiration" on page 213	New section about how password expiration is handled by an external LDAP directory or Active Directory.
"Configuring Drilldown Visibility" on page 385	New section on how to configure drilldown visibility within a business object or between business objects.
"Monitoring Application and User Activity" on page 389	New section on how to monitor log files, usage records, and statistics pages to troubleshoot potential security problems.
"Anonymous User" on page 188 "Unregistered Users and Anonymous Browsing" on page 219	Added clarification about the anonymous user requirement for applications that do not allow unregistered users.
"Anonymous Browsing" on page 189	Added information about the `LoginView` parameter and how it relates to the `AllowAnonUsers` parameter.
"Siebel Application Configuration File Parameters" on page 197	Added information about setting configuration file parameters for the Dedicated Web Client and Mobile Web Client.
"Defining Responsibilities and Adding Views and Users" on page 331	Added information about how to add new views to responsibilities if you are using a Dedicated Web Client or Mobile Web Client.

Table 2. Changes Made in Version 7.5, Rev. A for January 2003 Bookshelf

Topic	Revision
"User Authentication Issues" on page 393	Added troubleshooting information for "Web Authentication Failed" error messages.
"RC2 Encryption Administration" on page 81	Updated procedure for upgrading to the Siebel Strong Encryption Package.

About Security Resources for Siebel Applications 1

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

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

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

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

Classifications of security services include:

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

- **Access control.** Access control requires that access to information resources can be controlled by the target system.

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

Using Industry Standards

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

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

Supported standards include:

- **SSL.** Protection of Siebel eBusiness Applications by using the Secure Sockets Layer (SSL) capabilities of supported Web servers.
- **LDAP/ADSI.** Siebel Systems provides preconfigured integration with Lightweight Directory Access Protocol (LDAP) and Active Directory Services Interface (ADSI). For more information, see "Security Adapters for External Authentication" on page 27.
- **RSA.** Communication between Siebel components can be encrypted using RSA encryption algorithms.
  - For supported Windows platforms, Siebel Systems supports Microsoft Crypto.

  - For supported UNIX platforms or cross-platform environments, Siebel Systems supports RSA BSAFE. RSA BSAFE is FIPS 140-1 certified.

  NOTE: 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.

- **X.509.** Siebel applications use the SSL capabilities of supported Web servers to enable authentication based on X.509 client certificates.

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

User Authentication for Secure System Access

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

- Native database authentication
- Security adapters for external authentication

- Web Single Sign-On

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

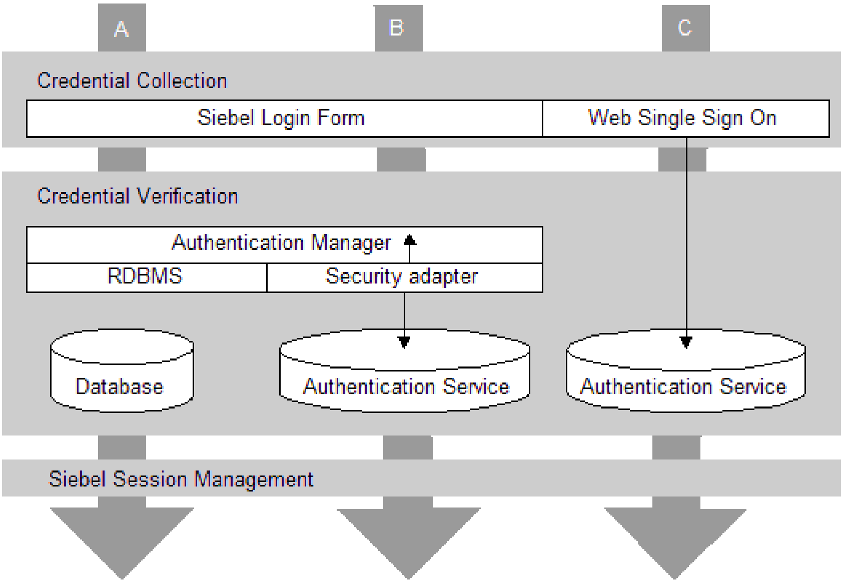


Figure 1. Methods of User Authentication Within a Siebel Site

Database Authentication

For employee applications, Siebel Systems provides internal mechanisms for credential collection and verification. The default login form collects Siebel username and password credentials. The underlying security systems of the database verify users’ credentials.

Each user must have a valid database account in order to access the Siebel application. The internal authentication deployment supports password encryption for protection against hacker attacks.

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

Security Adapters for External Authentication

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

NOTE: The exact valid character set for a Siebel username depends on the underlying authentication system. For external 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. Integration is currently certified and supported for IBM Directory Server, Microsoft Active Directory, Novell NDS eDirectory, and Sun ONE Directory Server.

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 is available for the RSA Secure ID token. This token is a portable token that provides users with a key that changes after a specified time interval, such as one minute. Only by supplying both the 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.

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

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, such as one of those listed below.

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.

End-to-End Encryption for Data Confidentiality

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

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

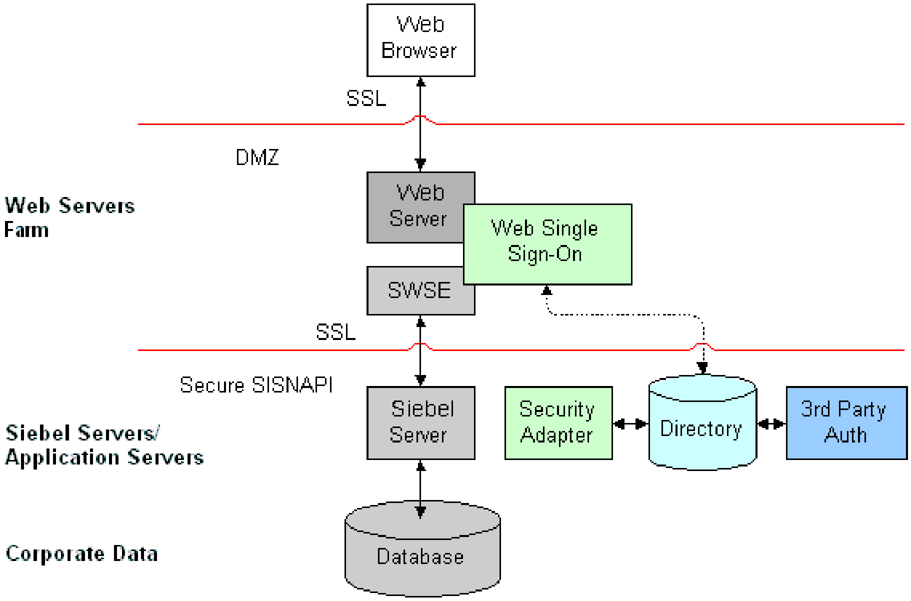


Figure 2. Data Encryption in the Siebel Environment

Client Browser to Web Server

Siebel Systems provides zero-footprint Web applications that run in a standard Web browser. When a user accesses a Siebel application, a Web session is established between the browser and the Siebel Server. 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.

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

Web Server to Siebel Server

Siebel software components communicate over the network using a Siebel TCP/IP-based protocol called SISNAPI (Siebel Internet Session API). Customers have the option to secure SISNAPI using Secure Sockets Layer (SSL) or embedded encryption from RSA or Microsoft Crypto. These technologies allow data to be transmitted securely between the Web server and the Siebel Server with less risk of intrusion.

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. To provide an additional level of security at this stage, Siebel applications support data encryption through integration with RSA Bsafe Crypto.

Database Storage

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

Authorization to Control Data Visibility

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

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

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

View-Level Access Control

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

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

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 372.

Record-Level Access Control

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

Siebel applications use three types of record-level access: position-based, organization-based, and access group-based. When a particular position, organization, or access group is assigned to a data record, only employees within that position, organization, or access group can view that record.

- A position represents a place in the organizational structure, much like a job title. Typically a single employee occupies a position; however, it is possible for multiple employees to share a position. Position access allows Siebel customers to classify users so that the hierarchy between them can be used for access to data.

  For example, a supervisor would have access to much of the data that a subordinate has access to; the same applies to others who report to the same 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 even created on an ad hoc basis, pulling together users from across different organizations and granting them access to the same data.

Auditing for Data Continuity

Siebel Systems supports various degrees of auditing.

- At the simplest level, each data record has created and last updated fields (when and by whom). Second, with configuration, you can generate an activity for additional levels of auditing. This is best used when there are limited needs for auditing (just a few areas to track).
- Siebel applications can maintain an audit trail of information that tells when business component fields have been changed, who made the change, and what has been changed. 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.)
- Business Process Administration allows you to configure workflow processes to save information on changes to specific business components.

- You can also attach scripts to the business component Write_Record event and save information about the transaction.

Secure Physical Deployment to Prevent Intrusion

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

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

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

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

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

Security for Mobile Solutions

Siebel Systems also provides a broad suite of mobile solutions that allow remote access to data within Siebel eBusiness Applications. These solutions support a wide variety of mobile platforms, that includes wireless phones, handhelds, and laptop computers. Siebel Systems provides security for customers using these devices to access Siebel applications. Siebel Systems also works with a range of alliance partners to provide the latest in security for mobile devices such as HP/Compaq, RIM, and Kyocera.

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.

Device User Authentication

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.

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.

Configuring for Security: Overview 2

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

Security Roadmap

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

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

1. During Siebel software installation, install Resonate Central Dispatch to manage port numbers and provide firewall protection on your network. See Chapter 3, "Physical Deployment and Auditing," and *Siebel Server Installation Guide*.

2. After you install your Siebel site, change the default passwords for Siebel accounts, according to the requirements for your authentication method. See "Changing Default Passwords" on page 39.

   - Change the SYSADM password.

   - Change the DBO table owner and password.

   - Add a password for updating Web server images. See "Adding a Password for Updating Web Server Images" on page 46.

3. Make sure communications and important data is encrypted. See Chapter 4, "Communications and Data Encryption."

   - Enable encryption for SISNAPI communications between Siebel components. See "Configuring for Encryption" on page 64.

- Make sure important data such as passwords or credit card numbers are encrypted. See "Password Encryption" on page 77 and "Business Component Encryption" on page 77.
- Make sure communication with Siebel Reports Server is secure. See "Securing Siebel Reports Server" on page 58.

4. Implement security adapter authentication or Web Single Sign-On to validate users. For more information, see Chapter 5, "User Authentication Overview."

   - Configure the Siebel Web Engine to use HTTPS protocol to transmit user credentials from the browser to the Web server. See "Secure Login" on page 169.
   - Require URLs to use HTTPS protocol for some (or all) views in your Siebel applications. See "Secure Views" on page 190.
   - Manage database access by creating a single Application User account and encrypt the Application User password. See "Application User" on page 175.
   - If you are using Web Single Sign-On, enable X.509 digital certificate authentication and change the default TrustToken setting. See "Digital Certificate Authentication" on page 191.
   - For LDAP/ADSI authentication, turn on password syntax check, password expiration, and user account lockout (if available). See "Account Policies" on page 212.

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

6. Create an audit trail to monitor database updates and changes. See "Auditing for Data Continuity" on page 56. Also refer to *Applications Administration Guide*.

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

   - Change the DBA password. See "Changing the Siebel Local (DBA) Password" on page 45.

- Enable encryption for Mobile Web Clients. See "Mobile Web Client: Encryption for Synchronization" on page 75.

Also refer to *Siebel Remote and Replication Manager Administration Guide*.

Changing Default Passwords

The Siebel installer and the seed data provided with Siebel Server and 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.

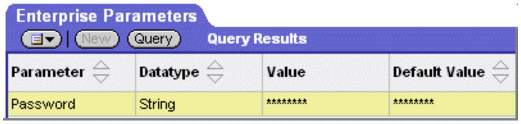
Before you change default passwords, review the following points:

- The Password and Confirm Password fields described in this section are unavailable in the Siebel application if you are using database authentication. If you are using LDAP or ADSI, the availability of these fields depends on whether the underlying security mechanism allows this functionality.
- The procedures in this section describe changing passwords at the Enterprise level. If you set and change passwords at this level, the changes will cascade down to 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 cascade to this component, unless the override is deleted at the Component level.

  For more information, refer to *Siebel Server Administration Guide*.

The following sections include procedures for changing account passwords. Figure 3 shows the `Password` parameter in Enterprise Parameters.



Parameter	Datatype	Value	Default Value
Password	String	********	********

Figure 3. Changing Passwords

Changing the SADMIN Password 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).

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

NOTE: Do not use ' or " (single or double quotation marks) as part of a SADMIN password. Because quotation marks are used as special characters in the siebns.dat file to delineate parameter values, using quotation marks within a password may cause the password to be truncated. For example, the password `abcde"f` would be truncated to `abcde`.

Same Login Name

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

To change the Siebel administrator password

1. Change the Windows domain login password.

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

2. Change the password for the Siebel Server system service in the Windows Control Panel.

   a. In the Windows NT Control Panel, double-click Services. In Windows 2000, choose Start > Programs > Administrative Tools > Services.

   b. Select the Siebel Server System Service and click Startup.

   c. Change the password in the Password and Confirm Password fields, and click OK.

3. Change the password in Enterprise Manager.

- **a** Log into a Siebel employee application (such as Siebel Call Center) and choose View > Site Map > Server Administration > Enterprise Configuration.
- **b** Click the Enterprise Parameters tab.
- **c** In the Enterprise Parameters list, locate the `Password` password.
- **d** In the Current Value field, type in the new password, and then click Save.

4 If you are using Resonate Central Dispatch, you may also want to change the password used to log into Resonate.

- **a** In a Siebel employee application, choose View > Site Map > Server Administration > Enterprise Configuration > Enterprise Parameters.
- **b** In the Enterprise Parameters list, select `Resonate password`. Then, type in the new password and click Save.

5 Change the password in the database.

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

6 If you changed the Resonate password, stop and restart the Resonate service.

7 Stop and restart the Siebel Server service.

Different Login Name

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

To change the Siebel administrator password

1 Complete Step 1 and Step 2 on page 40 (in the previous procedure).

2 Stop and restart the Siebel Server service.

Changing the SADMIN Password on UNIX

Use the following procedure to change the SADMIN password on a UNIX platform.

NOTE: Do not use ' or " (single or double quotation marks) as part of a SADMIN password. Because quotation marks are used as special characters in the siebns.dat file to delineate parameter values, using quotation marks within a password may cause the password to be truncated. For example, the password `abcde"f` would be truncated to `abcde`.

To change the SADMIN password

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
   ```

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

   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.

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

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

5. Restart all Siebel Servers.

   ```
   $SIEBEL_ROOT/ServerName/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) and Password

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

The Table Owner is used to reference table names when SQL statements are generated (for example, SELECT * FROM SIEBEL.S_APP_VER). The Table Owner password is used only when the schema is changed (this occurs with the Generate Triggers server component).

By default, Siebel applications store the Table Owner, but not the Table Owner password. This is because the Table Owner password is not required for Siebel applications to work. Therefore, changing the Table Owner password only has to be done at the database level, not within Siebel applications.

To change the Table Owner and password on Windows

1 Change the Table Owner in Enterprise Manager.

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

   b Choose View > Site Map > Server Administration > Enterprise Configuration.

   c Click the Enterprise Parameters tab.

   d In the Enterprise Parameters list, locate the `Table Owner` parameter.

   e In the Current Value field, type in the new `Table Owner` value, and then click Save.

2 Change the password in the database.

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

3 Restart the Siebel Server.

Checking for Failed Tasks

After changing the SADMIN password and the Table Owner, make sure all server tasks are still running.

To check for failed tasks

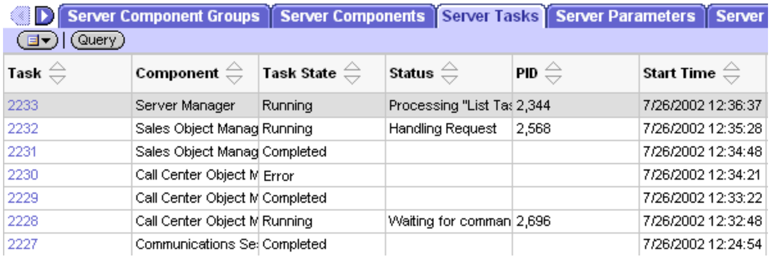
1 After the Siebel Server restarts:

   a Choose View > Site Map > Server Administration > Servers.

   b In the Siebel Servers list, select the appropriate Siebel Server.

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

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



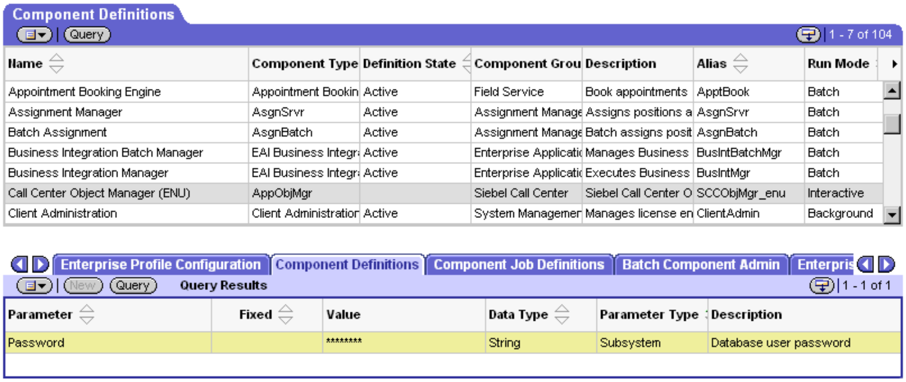
Task	Component	Task State	Status	PID	Start Time
2233	Server Manager	Running	Processing "List Ta:	2,344	7/26/2002 12:36:37
2232	Sales Object Manag	Running	Handling Request	2,568	7/26/2002 12:35:28
2231	Sales Object Manag	Completed			7/26/2002 12:34:48
2230	Call Center Object M	Error			7/26/2002 12:34:21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

2 For each Server Task that displays an error, update both the SYSADM and Table Owner for that task.

   a Choose View > Site Map > Server Administration > Enterprise Configuration.

b Click the Component Definitions tab and select the component that initiated the failed task.

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



Component Definitions

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

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

c When the list of Parameters for the component appears, locate the `Password` parameter and enter the new SADMIN password.

d Then locate the `Table Owner` parameter and enter the new Table Owner.

Changing the Siebel Local (DBA) Password

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

The following is an overview of how to change the DBA password in the SQL Anywhere environment. You can use this as a model for changing the password in your own environment.

For information about this topic and about running the Generate New Database component, extracting the database, and initializing a local database, see *Siebel Remote and Replication Manager Administration Guide*.

To change the local DBA password on Mobile Web Clients

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

   a. Change to the bin directory in the Siebel Server root directory:

   ```
   cd SIEBSRVR_ROOT\bin
   ```

   b. Start the utility by entering:

   ```
   dbisqlc -c v
   ```

2. Enter the following command:

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

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

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

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

3. Click Execute.

4. Run the Generate New Database component using the new DBA password.

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

Adding a Password for Updating Web Server Images

As part of the installation hardening process, it is recommended that administrators define a password for updating cached images on the Web server.

Each time the Siebel administrator restarts the Web server, the Web server contacts the Siebel Server and refreshes these images. However, administrators may find that entering this password in a command line is a more efficient way to perform image file refresh, particularly when deploying multiple Web servers.

Setting a password allows only Siebel administrators to refresh the application image files on your Web server by accessing updated images placed on the Siebel Server. If you do not set a password, an unauthorized user could invoke the UpdateWebImages command to update Web images.

To add this password:

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

To edit the eapps.cfg file

1. In the [SWE] section of the eapps.cfg file, add a line to specify the location of the Web image caching. For example, if you specify:

   ```
   WebPublicRootDir=m:\v752\eapps\public_enu
   ```

   then the Web images root directory would be in the images subdirectory (`m:\v752\eapps\public_enu\images`).

   The image root of the Siebel Server is fixed. For example, if the client root is set as `m:\752`, then the image root is `m:\752\images`.

2. Add a line to specify the Web update password. For example:

   ```
   WebUpdatePassword=abcdef
   ```

   Siebel administrators can then use this password to renew the image cache from a command line, without restarting the Web server. For example:

   ```
   http://host/eservice/
   start.swe?SWECmd=UpdateWebImages&PWEPassword=abcdef
   ```

Security Settings for the Web Browser

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

For detailed information about browser settings used in deploying Siebel clients, refer to *Siebel Web Client Administration Guide*.

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

Physical Deployment and Auditing 3

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

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

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

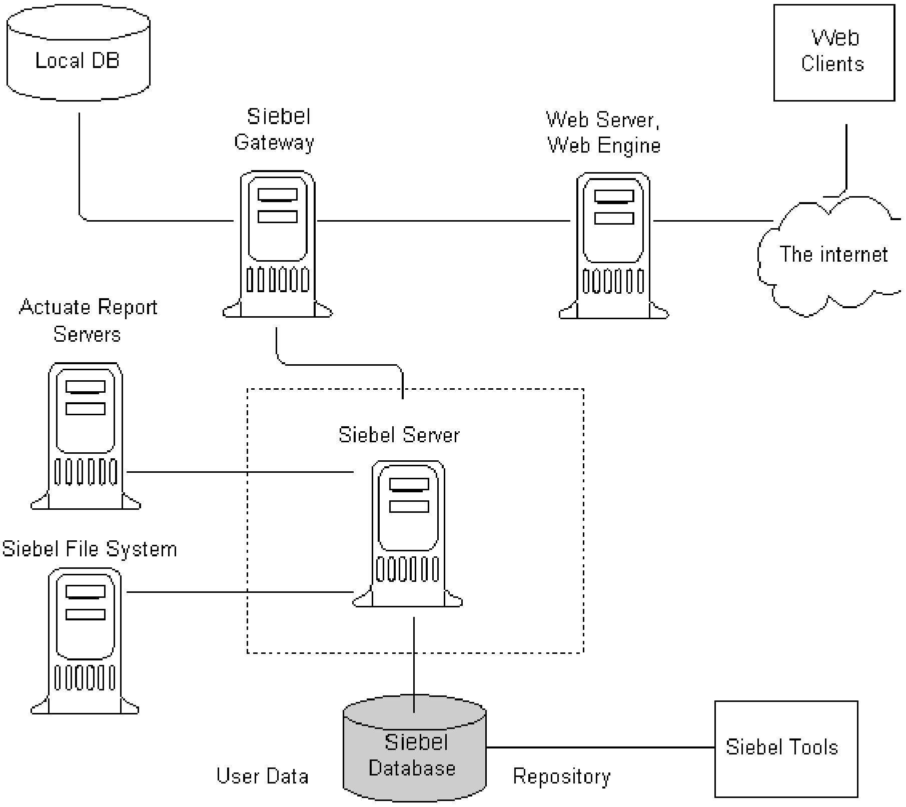


Figure 4. Siebel Network Components

Firewall Support

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

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

- **Proxy.** A proxy (also known as an application-level gateway) acts as an intermediary to prevent direct connection between a local corporate network and the outside world. Proxy services shield internal IP addresses from the Internet.

- **Network Address Translation (NAT).** NAT technology transparently rewrites the IP addresses of Internet connections as they move across the firewall boundary. This allows multiple computers in a local network to hide behind a single IP address on the Internet.

- **Virtual Private Networks (VPN).** VPN is a technique that allows computers outside the firewall to tunnel traffic through a firewall, then appear as if they are connected inside the firewall. VPN technology allows employees working at home or on the road to access many corporate intranets (for example, mail servers, file shares, and so on) which otherwise would not be sufficiently secured to be placed outside the firewall.

Recommended Placement for Firewalls

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

- The Internet zone where Web Clients reside.

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

- The Siebel Server zone (sometimes called the application server zone): components that reside inside this zone include Siebel Servers, the Siebel Gateway, a connection broker (such as Resonate Central Dispatch scheduler), and the authentication server.

- The Data Server zone where the Siebel Database and Siebel File System and Database Server reside. Typically, this is where the most critical corporate assets reside. Access to this zone should be limited to authorized application administrators and database administrators only.

Siebel network architecture allows you to install firewalls between each of these zones. However, for optimum performance, it is not recommended to install a firewall between the Siebel Server zone and the Data Server zone, or between the Siebel Database and the Siebel Database Server. Figure 5 shows the recommended placement for firewalls in Siebel networks.

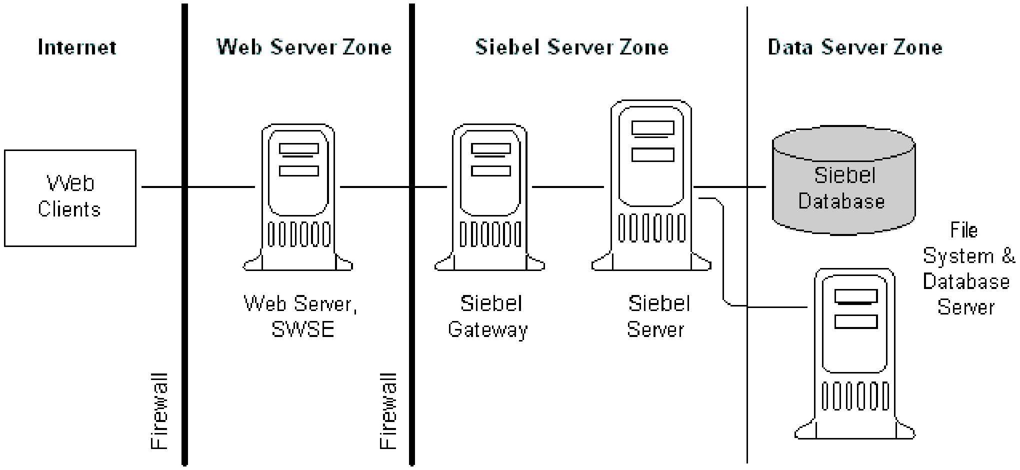


Figure 5. Firewalls in Siebel Networks

For additional security, it is recommended to install an additional Web server to act as a proxy to handle traffic between the Web Clients and the Web server that contains the Siebel Web Server Extension (SWSE).

Resonate Support

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

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

Additional Resonate security features include:

- **Denial of Service (DoS) Attack prevention.** In a DoS attack, Resonate helps handle the TCP connections. Incoming attacks can be cached at the scheduler before they ever reach the Siebel Server. Resonate Central Dispatch has a built-in mechanism to stop DoS attacks at the point of entry.
- **Virtual IP addressing.** Resonate's VIP shields hackers from accessing Siebel Servers directly. Because it 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 Resonate Scheduler to the Siebel Server rather than directly from the Web server to the Siebel Server.
- **NAT firewall.** Resonate allows you to install a Network Address Translation (NAT) firewall between the Siebel Server and the Web server.

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

Port Numbers

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

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

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

- To establish SSL communication for Siebel communications traffic between the Web browser and the Web server, specify an HTTPS port (default is 443) when you install the Siebel Web Server Extension.

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

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

  Once firewall access is available, users can be authenticated using LDAP or any other Siebel-supported method. For more information, see "User Authentication Overview" on page 89.
- Authorized vendors and remote users outside the firewall can use the standard Web server port (default is 80) to access Siebel Web applications. You can configure your firewall so that it will not pass traffic on anything other than port 80. If your Web server needs to support HTTP over SSL, you can open port 443.

  NOTE: Siebel Remote deployment options do not rely on Telnet connections to the server. Telnet connections for remote users can be configured in the Siebel environment. However, because of possible security risks, using such connections is not recommended.
- 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. For example, the default TCP port number for communications with an Oracle database is 1521.
- 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 UDP port numbers are 137 and 138.

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

Restricting Access

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

Physical Security of the Client Device

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

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 server component to access the Siebel File System. File System Manager processes these requests by interacting with the File System directory.

To prevent direct access to Siebel files from outside the Siebel application environment, only the Siebel Service owner should have access rights to the Siebel File System directory. The Siebel Server processes and components use the Siebel Service owner account to operate.

NOTE: For Siebel Dedicated Web Client, access to the Siebel File System may be achieved either through the File System Manager or through direct connection from each individual client. For more information, refer to *Siebel Web Client Administration Guide*.

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 has accessed an item, which operation was performed, when it was performed, and how the value was changed. Therefore, it is useful for maintaining security, 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 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.

For Siebel Remote and Siebel Replication Manager users making changes to records, Audit Trail works for every Siebel Web deployment and configuration option, including replication and synchronization. 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 Actuate Reports Server, Siebel Application Object Manager, and Siebel Web Client.

NOTE: Communication among Actuate components is outside the scope of the Siebel applications environment. For more information, consult the Actuate product documentation in the third-party documentation section of the *Siebel Bookshelf*.

Reports Components

The Siebel Reports Server consists of the following components:

- **Actuate e.Reporting Server.** Generates and manages live report documents. Actuate e.Reporting Server also contains the Report Encyclopedia, a shared repository that stores report items along with related data, such as access privileges and request queues.

- **Actuate Management Console.** Manages one or more Actuate e.Reporting Servers and Report Encyclopedias. Actuate Management Console also controls user privileges. This replaces the Actuate Administrator Desktop.

- **Actuate Active Portal.** Provides access to the Siebel Reports Server from the World Wide Web using JavaScript and Java Server Page (JSP) tags. Using Actuate Active Portal you can access and work with reports through any Web browser.

- **Actuate e.Report Designer Professional (Optional).** Used by professional developers of structured content to design, build, and distribute report object designs and components throughout the enterprise. The Actuate Basic Language and Actuate Foundation Class Library support customizing 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.

- **Siebel Report Server Access.** A Siebel application integration component that provides access to Siebel data for report generation. This component also includes Siebel Reports executables, Siebel Active Portal templates, and Active Portal security extension library.

Configuring Reports Server for Security

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

- Communication between the Siebel Web Client and Actuate Report Cast

  This communication takes place during report viewing. When the Web Client communicates with Actuate Report Cast, a cookie that contains the encrypted Report Server login parameters is passed through the HTTP headers. Because the login parameters are encrypted, this part of the communication is secure by default.

  However, the report itself is delivered in DHTML through Actuate Report Cast 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, refer to the postinstallation tasks described in the *Siebel Reports Administration Guide*.

- Communication with the Application Object Manager

  When report generation is initiated in the Actuate e.Reporting Server, this server uses Siebel Reports Server Access to communicate with the Application Object Manager. The e.Reporting Server establishes a separate session in the Object Manager and obtains data for report generation.

  To secure this communication, 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, refer to the postinstallation tasks described in the *Siebel Reports Administration Guide*.

Communications and Data Encryption 4

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

Types of Encryption

Encryption is a method of encoding data for security purposes.

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

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

- **SSL for Web client connections.** For data security over the Internet, Siebel applications use the Secure Sockets Layer (SSL) capabilities of its supported Web server platforms to secure transmission of data between the Web browser and the Web server.

  Siebel applications can be configured to run completely under HTTPS, have specific pages run under HTTPS, or simply handle login requests under HTTPS.

- **SSL for connection to LDAP/ADS.** Secure Sockets Layer (SSL) can be used for connection to LDAP/ADS directories.

  NOTE: With SSL enabled between the Siebel Server and the LDAP directory, only Sun ONE Directory Server has been completely tested by Siebel Systems. IBM Directory Server and Novell NDS eDirectory have not been tested with SSL. Siebel Systems cannot certify that SSL connectivity to these directories will work correctly.

- **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 (SSL) or on Microsoft Crypto API or RSA algorithms, and works across multiple operating system platforms.

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

- **Database encryption.** Siebel 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 using the RC2 Encryptor. RC2 encryption can be enabled for business component fields using Siebel Tools. For more information, see “Business Component Encryption” on page 77 and “RC2 Encryption Administration” on page 81.

- **Password encryption.** Siebel administrators can also enable password and credentials encryption. This invalidates the user ID and password to unauthorized external applications and prevents direct SQL access to the data by anything other than Siebel eBusiness Applications. For more information, see “Password Encryption” on page 77.

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

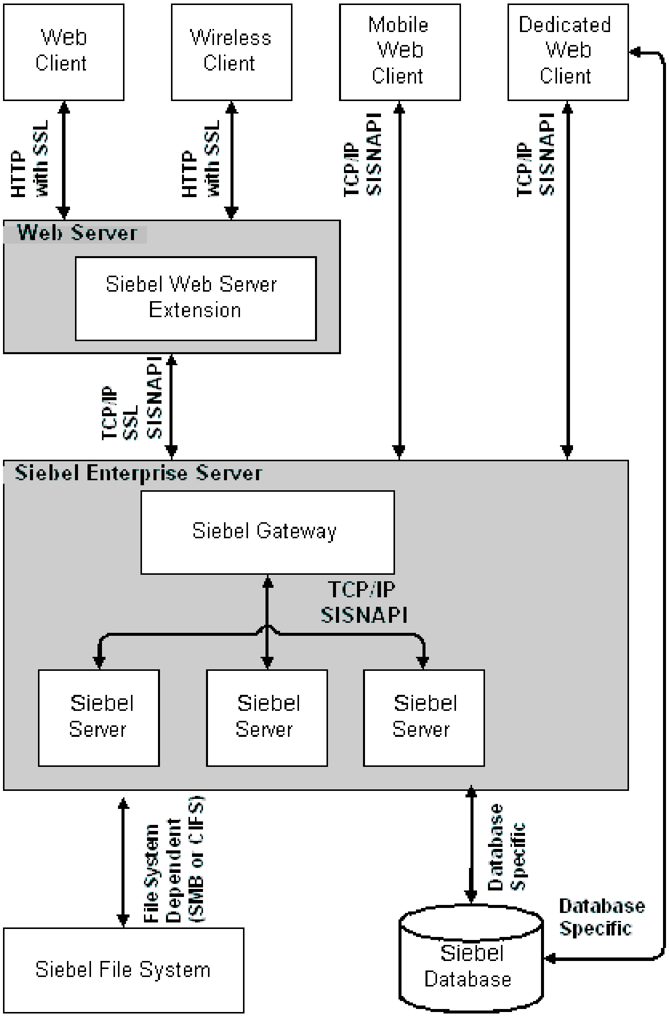


Figure 6. Communications Encryption in the Siebel Application Environment

Configuring for Encryption

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

Encryption is configured for data traffic between the Web server, Siebel Server, and Siebel Web Client.

NOTE: Encryption as described in this section is not used to encrypt data in the database, as described in "Business Component Encryption" on page 77 and "RC2 Encryption Administration" on page 81. Also, it is not used for communication with the database—for such encryption, check with your database vendor.

Configuring Siebel Enterprise for Microsoft Crypto or RSA Encryption

This section describes how to configure your Siebel Enterprise to use Microsoft Crypto or RSA encryption for SISNAPI (Siebel Internet Session API) communications between the Siebel Server and the Siebel Web Server Extension, and between Siebel Servers.

You also use the Siebel Software Configuration Wizard to configure the Siebel Web Server Extension. After you configure the Siebel Enterprise as described below, repeat this procedure for the Siebel Web Server Extension, setting the same encryption type.

To enable Microsoft Crypto or RSA encryption for the Siebel Enterprise

1. Start the Siebel Software Configuration Wizard.

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

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

   - **MSCRYPTO.** Microsoft 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.
- **NONE.** Specify this option if you will not use encryption, or if you will use SSL instead of Microsoft Crypto or RSA encryption.

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 RSA or SSL.

3. Review the settings, specify to finish configuration, then restart the server.

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 Siebel Enterprise or Siebel Server for SSL Encryption

This section describes how to configure your Siebel Enterprise or Siebel Server to use Secure Sockets Layer (SSL) encryption or authentication for SISNAPI (Siebel Internet Session API) communications between Siebel Servers and the Web server, and between Siebel Servers.

Configuring at the Siebel 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 Siebel Web Server Extension to use SSL, as described in "Configuring Siebel Web Server Extension for SSL Encryption" on page 70.

Configuring SSL for Siebel Server and the Siebel Web Server Extension also configures 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 issued by certificate authorities. 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 Name Server. If you also configure the Siebel Web Server Extension 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.

Running the SSL Configuration Utility for Siebel Server

This section describes running the Siebel Software Configuration Utility (Siebel Server SSL).

NOTE: The prompts for the SSL configuration utility are the same whether you run it in GUI mode (Windows) or console mode (UNIX). However, many of the specific user interface elements are different in these two modes.

CAUTION: The following procedure must be performed after installing all applicable maintenance releases. For more information, refer to the *Maintenance Release Guide* for your Siebel products.

To enable SSL encryption for the Siebel Server

1. On a Siebel Server machine, start the Siebel Software Configuration Utility (Siebel Server SSL version).

   - For Microsoft Windows platforms, open an MS-DOS window and enter the following command to run this utility in a graphical 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 configuration utility (for example, ENU for U.S. English)

   - For UNIX platforms, enter the following commands to run this utility 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 configuration utility (for example, ENU for U.S. English)

2 Enter the hostname of the Siebel Gateway machine and the name of the Siebel Enterprise applicable to the component you want to configure.

3 Specify the configuration type: whether to configure SSL for the Siebel Enterprise or for a Siebel Server.

NOTE: If you specify Siebel Enterprise SSL, all settings, including the key filename and password and certificate filenames, will be inherited by all Siebel Servers in the Enterprise. 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.

4 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.

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

The certificate file must use either ASN or PEM format. The certificate authority file identifies the trusted authority who issued the certificate.

These files are typically located on each Siebel Server machine for which you configure Siebel Server SSL. (You need not authenticate or encrypt communications between components on the same machine.)

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

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

The private key file must use PEM format. This file is typically located on each Siebel Server machine for which you configure Siebel Server SSL.

The password you specify will be stored in encrypted form.

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

7 Specify whether you require peer authentication.

Peer authentication means that this Siebel Server must authenticate itself with a certificate against the client (that is, SWSE or another Siebel Server that connects to this one), whenever a connection is established. Peer authentication is false by default.

NOTE: You must set peer authentication for a Siebel Server if you also set peer authentication for the connecting client (that is, SWSE or another Siebel Server that connects to this one).

The equivalent parameter in the Name Server is `PeerAuth` (`Peer Authentication`).

8 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` (`Validate peer certificate`).

9 Review the settings, specify to finish configuration, and then restart the server.

Repeat this procedure for each Siebel Server in your application environment, as necessary. Make sure you configure all applicable Siebel Servers and also configure the Siebel Web Server Extension. Set the same encryption type for all components.

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:

- Run the Siebel Server Manager and set the `CommType` parameter (`Communication Transport`) to `SSL` for each Application Object Manager that is to use SSL. (TCP/IP is used by default.)
- If you previously used Microsoft Crypto or RSA encryption, run the Siebel Software Configuration Wizard, as described in "Configuring Siebel Enterprise for Microsoft Crypto or RSA Encryption" on page 64. Specify `NONE` as the encryption type, instead of `MSCRYPTO` or `RSA`.

  Or, use Siebel Server Manager to change the value of the `Crypt` parameter (`Encryption Type`) to `NONE`. Specify this setting at the Enterprise level.

Configuring Siebel Web Server Extension for SSL Encryption

This section describes how to configure your Siebel Web Server Extension (SWSE) to use Secure Sockets Layer (SSL) encryption or 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 Siebel Enterprise or Siebel Server for SSL Encryption" on page 66.

Performing this procedure adds parameters to the eapp.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 = FALSE
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 Application Object Manager 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://hostname:2320/siebel/SSEObjMgr_enu/
servername
```

Running the SSL Configuration Utility for SWSE

This section describes running the Siebel Software Configuration Utility (Siebel Web Server Extension SSL).

NOTE: The prompts for the SSL configuration utility are the same whether you run it in GUI mode (Windows) or console mode (UNIX). However, many of the specific user interface elements are different in these two modes.

CAUTION: The following procedure must be performed after installing all applicable maintenance releases. For more information, refer to the *Maintenance Release Guide* for your Siebel products.

To enable SSL encryption for the Siebel Web Server Extension

1. On the Web server machine, start the Siebel Software Configuration Utility (Siebel Web Server Extension SSL version).

   - For Microsoft Windows platforms, open an MS-DOS window and enter the following command to run this utility in a graphical mode:

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

     where:

     - *SWEAPP_ROOT* is the Siebel Web Server Extension 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, enter the following commands to run this utility in console mode:

```
cd SWEAPP_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 SWEAPP_ROOT/bin
```

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

where:

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

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

The certificate file must use either ASN or PEM format. The certificate authority file identifies the trusted authority who issued the certificate.

These files are typically located on each SWSE machine for which you configure SSL.

The equivalent parameters in the eapps.cfg file are `CertFileName` and `CACertFileName`.

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

The private key file must use PEM format. This file is typically located on each SWSE machine for which you configure SSL.

The password you specify will be stored in encrypted form.

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

4. Specify whether you require peer authentication.

   Peer authentication means that the SWSE must authenticate itself with a certificate against the Siebel Server whenever a connection is initiated. Peer authentication is false by default.

   NOTE: If you set peer authentication for the SWSE, you must also set it for any Siebel Server that will connect to it.

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

5. 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`.

6. Review the settings, specify to finish configuration, and then restart the Web server.

   Repeat this procedure for each Siebel Web Server Extension in your application environment. Make sure you also configure all applicable Siebel Servers.

Configuring Web Clients for Encryption

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

Siebel eBusiness Applications support the following types of clients:

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

  This type of client uses configuration files located on the server. Encryption settings you make to the Siebel Web Server Extension are automatically recognized by this Web Client.

  For more information, see "Configuring Siebel Enterprise for Microsoft Crypto or RSA Encryption" on page 64.

- **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 "Mobile Web Client: Encryption for Synchronization" on page 75.

- **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.*

For more information about the first three clients listed above, see *Siebel Web Client Administration Guide*.

About Session Cookies

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

These 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 which started at the login page.

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

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

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

For more information about session cookies, refer to *Siebel Web Client Administration Guide*.

Mobile Web Client: Encryption for Synchronization

You can turn on encryption during the transfer of DX files 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 configuration file (for example siebel.cfg, used by Siebel Sales) to determine the type of encryption to use during synchronization. Encryption is the fifth element in the `DockConnString` parameter.

NOTE: Secure Sockets Layer (SSL) is not a supported encryption method for Siebel Mobile Web Client or Dedicated Web Client.

For information about authentication for Siebel Mobile Web Client and Siebel Remote, see Chapter 7, "Web Single Sign-On and Remote Authentication."

To enable encryption on the Mobile Web Client

1. Open the 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, non-text characters to the file. For example, use Microsoft Notepad instead of Microsoft Word or WordPad.

- Configuration files for a client are stored in the client's bin\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, esales.cfg).

  For a list of configuration files for Siebel applications, refer to *Siebel Server 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. It indicates the type of encryption used during synchronization.

   An example of a `DockConnString` 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, refer to *Siebel Remote and Replication Manager Administration Guide* and *Siebel Web Client Administration Guide*.

Password Encryption

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

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

Password encryption is useful for preventing unauthorized users from bypassing Siebel applications and logging directly into the Siebel Database using an RDBMS tool such as SQL*Plus.

For more information on user password encryption, see "User Password Encryption" on page 170. For more information on credentials password encryption, see "Credentials Password Encryption" on page 173.

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

- The password encryption utility does not automatically store hashed passwords in the Siebel Database or directory. Instead, the administrator is responsible for setting up database accounts using the hashed passwords.
- Instead of using a Siebel-supplied algorithm, customers can access their own encryption or hash algorithms, using the Siebel Security Adapter Software Developers Kit. For more information, see "Security Adapters for External Authentication" on page 27.

Business Component Encryption

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

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

- 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 uses 25 characters when encrypted, data 30 characters long uses 44 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.
- Any business component field that is to store encrypted data must be active.

For more information about performing some of the tasks described in this section, see *Siebel Tools Reference*.

Siebel Systems provides the RC2 Encryptor, based on RSA encryption, to allow you to encrypt data fields. For information about using the RC2 Encryptor to add encryption keys to the keyfile and change the keyfile password, see "RC2 Encryption Administration" on page 81.

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

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	`RC2 Encryptor`	Sets the type of encryption to use for the field.

Field User Property	Value	Description
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 3 shows some examples of Key Index Fields for business components.

Table 3. Encryption Key Index Fields

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

RC2 Encryption Administration

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

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

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

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

NOTE: Siebel Systems does not support RC2 encryption for numeric data, but you can use the encryptor for information such as credit card numbers, which are stored as strings in the database. For more information on encrypting numeric data, see “Encryption Issues” on page 398.

CAUTION: If you are upgrading from 56-bit encryption to 128-bit encryption, make sure you read “If You Are Upgrading” on page 86 before installing the Siebel Strong Encryption Package. For more information on the Siebel Strong Encryption Package, see the *Upgrade Guide* for the operating system you are using.

Using Key Database Manager

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

Running Key Database Manager

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

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

To run the Key Database Manager

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

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

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

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

   For descriptions of the flags and parameters, see Table 4 on page 83.

3. When prompted, enter the keyfile password.

   To add a new encryption key, see "Adding New Encryption Keys" on page 84.

   To change the keyfile password, see "Changing the Keyfile Password" on page 85.

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

5. Restart any server components that were shut down in Step 1 on page 83.

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

Table 4 lists the flags and parameters for the Key Database Manager utility, keydbmgr.exe.

Table 4. 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 configuration file, such as siebel.cfg

Adding New Encryption Keys

You can add new encryption keys to the keyfile. The 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. Run the keydbmgr.exe utility from the bin subdirectory in the Siebel Server root directory.

   For information, see "Running Key Database Manager" on page 82.

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

   The key must be at least 7 characters in length.

4. Exit the Key Database Manager utility.

   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.

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

   NOTE: Field-level RC2 encryption is not supported for Mobile Web Clients or Dedicated Web Clients.

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

Changing the Keyfile Password

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

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

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

To change the keyfile password

1. Run the keydbmgr.exe utility from the bin subdirectory in the Siebel Server root directory.

   For more information, see "Running Key Database Manager" on page 82.

2. To change the keyfile password, enter 1.

3. Enter the new password.

4. Confirm the new password.

5. Quit the Key Database Manager utility.

   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 root directory.

   NOTE: Field-level RC2 encryption is not supported for Mobile Web Clients or Dedicated Web Clients.

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

If You Are Upgrading

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

Before you install the Strong Encryption Package, perform the steps below.

To prepare for installing the Strong Encryption Package

1. Make a backup of your existing keyfile (keyfile.bin).
2. Run the Key Database Manager (keydbmgr.exe) and change the keyfile password.
3. Install the Siebel Strong Encryption Package. Follow the installation instructions included with the package.
4. Run the keydbupgrade utility.
5. Use the srvrmgr program to update the database password for the Enterprise Server.

   ```
   change ent param password=keyfile_password
   ```

6. Restart the server.

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

Encrypted Data

Siebel applications provide RC2 encryption to encrypt field data for sensitive information such as credit card numbers. For Unicode, you *must* use RC2 rather than the Standard Encryptor, which is no longer supported.

For details, see "Business Component Encryption" on page 77 and "RC2 Encryption Administration" on page 81. For information about upgrading to RC2 encryption from the Standard Encryptor to RC2, refer to *Upgrade Guide*.

User Authentication Overview 5

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

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

Additional sections in this book are provided with information on:

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

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

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

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

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

- **Seed data.** When you install your Siebel eBusiness Applications, you are provided seed data that is related to authentication, to user registration, and to user access to Siebel applications. For detailed information on the seed data that is provided and for procedures for viewing and editing seed data, see "Seed Data" on page 399.
- **Configuration parameters related to authentication.** Configuration parameter values determine how your authentication architecture components interact. For information about the purposes of configuration parameters and procedures for setting their values, see "Configuration Parameters Related to Authentication" on page 192.
- **Authentication options.** Each authentication strategy has options in the way it can be implemented. For information about the authentication options and procedures for implementing them, see "Authentication Options" on page 167.

About User Authentication

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

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

- **Database authentication.** This approach relies on the underlying application database for user authentication.

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

You may choose the approach for user authentication individually for each application in your environment based on the specific application requirements. However, there are administrative benefits to using a consistent approach across all of your Siebel applications because a consistent approach lowers the overall complexity of the deployment.

Table 5 highlights the capabilities of each authentication approach to help guide your decision. Several options are available for each basic strategy.

Table 5. Comparison of Authentication Approaches

Desired Deployment or Functionality	Database	Security Adapter	Web SSO	Comments
Does not require additional infrastructure components.	X			
Centralizes storage of user credentials and roles.		X	X	
Limits number of database accounts on the application database.		X	X	
Supports dynamic user registration. Users are created in real-time through self-registration or administrative views.		X	(X)	For Web SSO, user registration is the responsibility of the third-party authentication architecture. It is not logically handled by the Siebel architecture.

Table 5. Comparison of Authentication Approaches

Desired Deployment or Functionality	Database	Security Adapter	Web SSO	Comments
Supports account policy. 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 IBM DB2 Universal Database. 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	

Siebel Authentication Manager

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

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

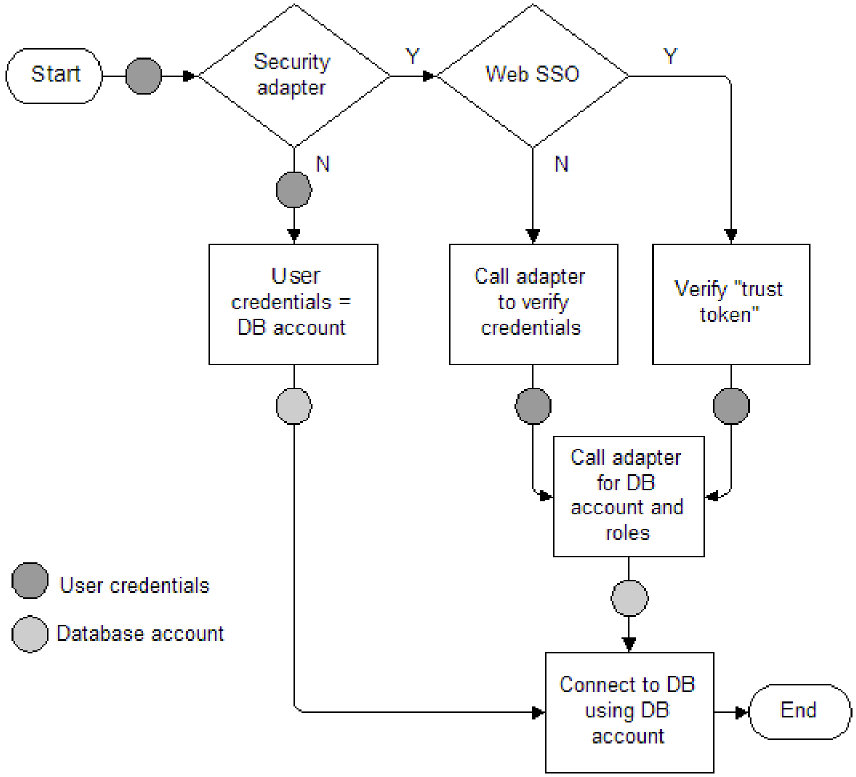

Start
Security adapter
Y
N
Web SSO
Y
N
User credentials = DB account
Call adapter to verify credentials
Verify "trust token"
Call adapter for DB account and roles
User credentials
Database account
Connect to DB using DB account
End

Figure 7. Siebel Authentication Manager Process

Authentication Manager Overview

The authentication manager receives user credentials from a source determined by the authentication strategy that is implemented. Figure 7 on page 93 provides a high-level view of the logic that determines the way the authentication manager processes the user credentials it receives.

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

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

Authentication Manager Process Detail

Figure 8 on page 96 presents the detailed logic of the process flow when the authentication manager is presented credentials and a request for access to a Siebel application.

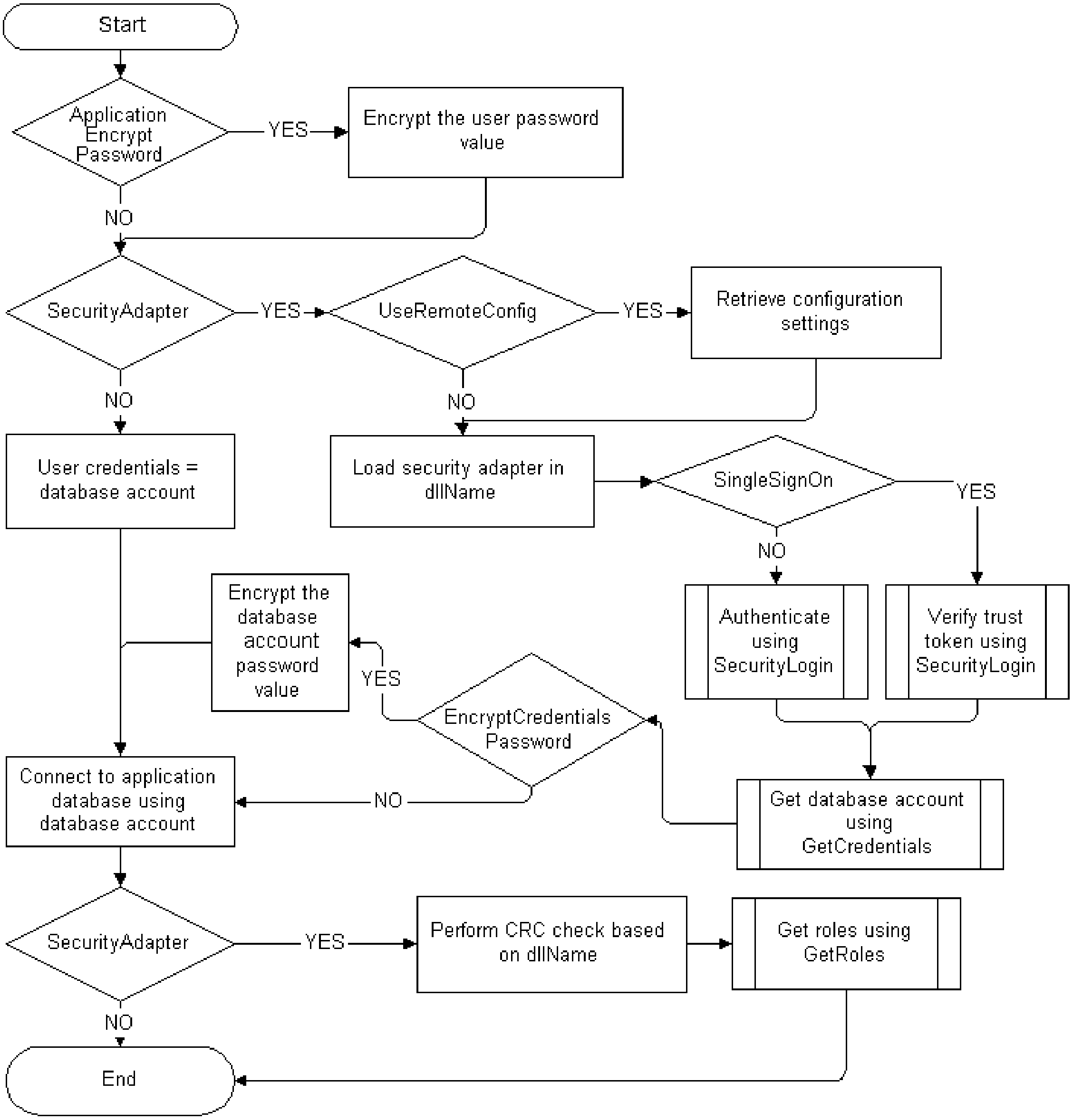

Start
Application Encrypt Password
YES
Encrypt the user password value
NO
SecurityAdapter
YES
UseRemoteConfig
YES
Retrieve configuration settings
NO
NO
User credentials = database account
Load security adapter in dllName
SingleSignOn
YES
NO
Encrypt the database account password value
YES
EncryptCredentials Password
Authenticate using SecurityLogin
Verify trust token using SecurityLogin
Connect to application database using database account
NO
Get database account using GetCredentials
SecurityAdapter
YES
Perform CRC check based on dllName
Get roles using GetRoles
NO
End

Figure 8. Authentication Manager Process Flow

Database Authentication Overview

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

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

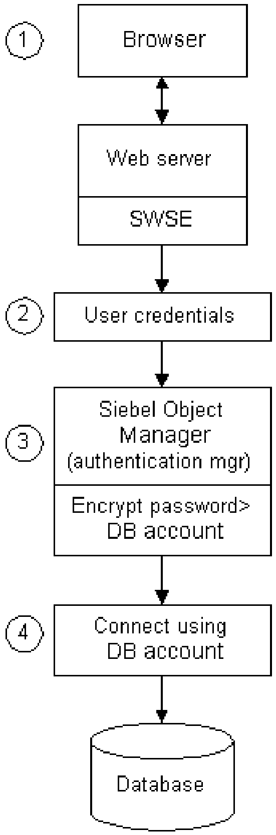


Figure 9. Database Authentication

Database Authentication Process

The steps in a database authentication process are:

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

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

Features Not Available for Database Authentication

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

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

Implementing Database Authentication

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

To allow database authentication to be implemented, you must make sure that the `Security Adapter Name` parameter at all applicable levels in the Name Server does not indicate that a security adapter is being used.

For information about setting Name Server parameter values and the purposes of the parameters, see "Name Server Parameters" on page 205.

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

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

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

  For information about adding users to the database, see "Internal Administration of Users" on page 262.

The following options are available if you implement database authentication:

- **User Password Encryption.** Maintains an unexposed, encrypted password to a database account, while an unencrypted version of the password is provided to the user for logging in. When enabled, a simple encryption algorithm is applied to the password before it is sent to the database.
- **Secure Login.** Transmits user credentials entered to a login form over Secure Sockets Layer (SSL).

Security Adapter Authentication 6

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

Siebel Security Adapters

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

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

In general, 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.
- The user is granted access to the Siebel application and the Siebel Database.

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

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

You can implement a security adapter other than the Siebel LDAP adapter or ADSI adapter. To support the functionality described in this section for the Siebel adapters, the adapter you implement must support the Siebel Security Adapter Software Development Kit. For more information, see "Security Adapters for External Authentication" on page 27.

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

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

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

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

Requirements for Directory

You must provide your own directory product, whether it is one of the servers supported by Siebel security adapters or another directory of your choice.

If you provide one of the Siebel-supported servers, you may use a Siebel-compliant security adapter or another adapter of your choice.

If you provide a directory other than those supported by the Siebel security adapters, then you are responsible for supporting the directory with the security adapter you implement. For specific information about third-party products supported by Siebel eBusiness Applications, see *System Requirements and Supported Platforms* for your Siebel application.

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

- **Siebel user ID.** This attribute value must match the value in the user ID field for the user's Person record in the Siebel Database. It is used to identify the user's database record for access control purposes.
- **Database account.** This attribute value must be of the form `username=`*`U`* `password=`*`P`*, 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.
- **Username.** This attribute value is the key passed to the directory which identifies the user. In a simple implementation, it may be the Siebel user ID, and so it may not need to be a separate attribute.
- **Password.** The storage of a user's login password differs between LDAP servers and Active Directory Server (ADS).
    - **LDAP.** If the user authenticates through the directory, such as in a security adapter authentication implementation, then the login password must be stored in an attribute.

      If the user is authenticated by an external authentication service, as might be the case in a Web SSO implementation, a password attribute is not required.

- **ADS.** ADS does not store the password as an attribute. The password can be entered at the directory level as a function of the client, or the Siebel ADSI security adapter can use ADS methods to create or modify a password.

  If the user authenticates through the directory, such as in a security adapter authentication implementation, then the login password must be stored. If the user is authenticated by an external authentication service, as might be the case in a Web SSO implementation, a password is not required.

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

An additional piece of information, *roles*, is supported by the Application Object Manager, 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 about this type of role, see "Roles" on page 167.

User Privileges

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

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

  For information about the application user, see "Application User" on page 175.

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

  For information about the anonymous user, see "Anonymous User" on page 188.

  For information about user self-registration, see "Implementing Self-Registration" on page 226.

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

  For information about internal and external registration of users, see "Internal Administration of Users" on page 262 and "Delegated (External) Administration of Users" on page 274.

ADSI Adapter Requirements

If you are running the Application Object Manager on supported Microsoft Windows platforms, you must meet the requirements described here.

- You must confirm that an ADSI client, supported by the Siebel ADSI adapter, is installed. If a supported client is not installed, then you must manually install one. Information about verifying this installation is provided below.

- In order to allow users to set or change passwords, the ADSI client 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 Windows 2000 domain forest, configuring trust relationships, or 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 "Secure Adapter Communications" on page 182.

- DNS servers on your network must be properly configured with DNS entries for the Active Directory server. Client machines using the ADSI security adapter must be configured to be able to retrieve these entries from the appropriate DNS servers.

For information about ADSI client versions supported by Siebel security adapters, see *System Requirements and Supported Platforms* for your Siebel application. See also the documentation for ADSI.

To confirm successful installation of a Siebel-supported ADSI client

1. Navigate to the system32 subdirectory of the installation location for the operating system (for example, C:\WINDOWS or C:\WINNT).
2. Verify that all of the DLLs for the supported ADSI clients listed in *System Requirements and Supported Platforms* for your Siebel application are present in the subdirectory.

   For example, Windows 2000 requires the files adsiis.dll and adsiisex.dll.
3. For each DLL, right click on the file and choose Properties.
4. Click the Version tab to see the version number.

Siebel Security Adapters and the Siebel Dedicated Web Client

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

- Application Object Managers
- Application configuration files
- Authentication manager

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

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

  For information about setting parameters in Siebel application configuration files on both the Siebel Server and the Siebel Dedicated Web Client, see "Siebel Application Configuration File Parameters" on page 197.

  For information about remote configuration, see "Remote Configuration" on page 180.

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

  For information about checksum validation, see "Checksum Validation" on page 179.

- In a security adapter authentication implementation, you must set Siebel system preferences if you want to implement:

  - Security adapter authentication of Siebel Dedicated Web Client users

  - Propagation of user data from the Siebel Dedicated Web Client to the directory

  For information about setting authentication-related Siebel system preferences, see "System Preferences" on page 209.

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

Security Adapter Deployment Options

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

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

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

For information about the authentication options and procedures for implementing them, see "Authentication Options" on page 167.

LDAP and ADSI Security Adapter Authentication

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

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

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

Figure 10 shows a security adapter authentication architecture.

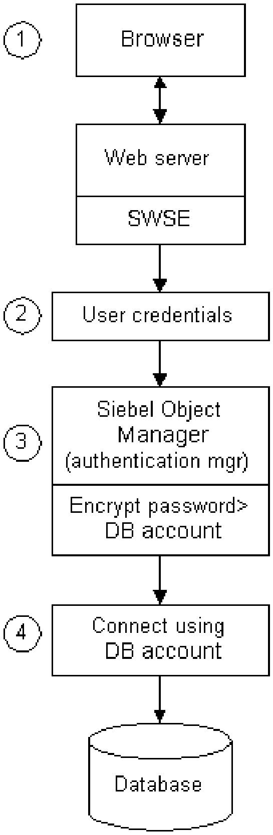


Figure 10. Security Adapter Authentication

The steps in the security adapter authentication process are:

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

Security adapter authentication can offer the following benefits:

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

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

Implementing LDAP and ADSI Security Adapter Authentication

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

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

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 from the Mobile Web Client, mobile users must use database authentication.

For information about authentication options for local database synchronization for mobile users, see *Siebel Remote and Replication Manager Administration Guide*.

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

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

Task Overview

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

- Set up a directory from which a database account and a Siebel user ID can be retrieved for each user.
- Set up a security adapter as a plug-in to the Application Object Manager.
- Edit the eapps.cfg file to provide authentication parameter values.
- Edit the configuration file for each Application Object Manager to provide authentication parameter values.
- Edit authentication-related parameters in the Name Server of the Siebel Gateway.

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

Siebel Systems provides an LDAP/ADSI Configuration Utility to help you configure a directory service for your Siebel applications. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 159.

Siebel Security Adapter Authentication and Siebel Dedicated Web Client

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

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

For information about setting authentication-related Siebel system preferences, see "System Preferences" on page 209.

Deployment Options for Security Adapter Authentication

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

In addition to the options described here, you can also implement any of the options that are described in "Security Adapter Deployment Options" on page 107.

- **Adapter-defined user name.** You can configure a Siebel application so that the username presented by the user is a value other than the Siebel user ID; for example, a Social Security number. The security adapter returns the Siebel user ID of the authenticated user and a database account from the directory to the authentication manager.
- **Shared database account.** A designated entry in the directory contains a database account that is shared by other users.
- **Secure adapter communications.** You can use a Secure Sockets Layer (SSL) to transmit data between a Siebel LDAP or ADSI security adapter and the directory.
- **Secure Login.** Transmit user credentials entered to a login form over Secure Sockets Layer (SSL).

For information about authentication options and procedures for implementing them, see "Authentication Options" on page 167.

Setting Up Security Adapter Authentication: A Scenario

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

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

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

These instructions implement the following basic configuration:

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

To implement authentication options not included in this implementation, see "Authentication Options" on page 167.

For information about special considerations to implementing user authentication, see "User Authentication Issues" on page 393.

If you use a non-Siebel security adapter, it must support the Siebel Security Adapter Software Developers Kit, described in "Security Adapters for External Authentication" on page 27. You must adapt the applicable parts of the following implementation to your security adapter.

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

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

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

Process of Implementing External Authentication

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

- Create a database login. See "Creating a Database Login" on page 116.
- Set up the attributes for users in the directory. See "Setting Up the Directory" on page 116.
- Create three users in the directory: a regular user, the anonymous user, and the application user. See "Creating Users in the Directory" on page 118.
- Add user records in the Siebel Database corresponding to two users in the directory. See "Adding User Records in the Siebel Database" on page 119.
- Edit eapps.cfg file parameters. See "Editing Parameter Values in the eapps.cfg File" on page 121.
- Edit the Siebel application's configuration file parameters. See "Editing Parameter Values in the Application Configuration File" on page 124.
- Edit the Name Server parameters. See "Editing Name Server Parameters" on page 128.
- Set system preferences. See "Setting System Preferences" on page 128.

- Restart the Siebel Server and the Web server. See "Restarting Servers" on page 129.
- Test the implementation. See "Testing the External Authentication System" on page 129.

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 399. 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 Directory

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

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

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

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

- Data: Siebel user ID. Suggested attribute: uid for LDAP or sAMAccountName for ADS.
- Data: Database account. Suggested attribute: dbaccount.

- Data: Password. Suggested attribute for LDAP only: userPassword. ADS does not use an attribute to store a user's password.

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

NOTE: To perform user management in the ADS directory through the Siebel client, it is strongly recommended that you configure ADS at the server level for SSL communications between the Active Directory client and server. This is different from SSL communications between the security adapter and the directory, which is configured through Siebel applications and is discussed in "Secure Adapter Communications" on page 182.

Creating Users in the Directory

Create three users in the directory, as described in Table 6. The attribute names, such as uid and userPassword in an LDAP directory, are those suggested in this example. Your entries may vary depending on the way that you make attribute assignments in "Setting Up the Directory" on page 116.

Table 6. Directory Records

Type of User	Siebel User ID Attribute (Uid for LDAP or sAMAccountName for ADSI)	Password (UserPassword Attribute for LDAP or ADS Password for ADSI)	Database Account Attribute (Dbaccount)

Anonymous user	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 "Anonymous User" on page 188.
		GUESTPW or a password of your choice	username = LDAPUSER
			password = *P*

Application user	APPUSER or a name of your choice	APPUSERPW or a password of your choice	Database account is not required for the application user.
A test user	TESTUSER or a name of your choice	TESTPW or a password of your choice	Database account is not required for any user record, except the anonymous user.

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

This example implements a shared credential. The database account for all users is stored in one object in the directory. In this example, the shared database account is stored in the anonymous user record. The database account must match the database account you reserve for externally-authenticated users described in "Creating a Database Login" on page 116. The P symbol represents the password in that database account.

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

For information about formatting requirements for the database account attribute entry, see "Requirements for Directory" on page 102.

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

Optionally, complete other attribute entries for each user.

Adding User Records in the Siebel Database

You must create a record in the Siebel Database that corresponds to the test user you create in "Creating Users in the Directory" on page 118.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in Table 24 on page 400. This record must also match the anonymous user you created in "Creating Users in the Directory" on page 118.

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 262.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.

2. From the application-level menu, choose View > Site Map > User Administration > Users.

   The All Users list appears.

3. In the All Users list, click the menu button and choose New Record.

   A new All Users form appears.

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

Field	Suggested Entry	Guideline
Last Name		Required. Enter any name.
First Name		Required. Enter any name.
User ID	TESTUSER	Required. This entry must match the uid (LDAP) or sAMAccountName (ADS) attribute value for the test user in the directory. If you used another attribute, it must match that value.

Field	Suggested Entry	Guideline
Responsibility		Required. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. If an appropriate seed responsibility does not exist, such as for a Siebel employee application, assign an appropriate responsibility that you create.
New Responsibility		Optional. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. This responsibility is automatically assigned to new users created by this test user.

5 Verify that the seed data User record exists for anonymous users of the Siebel application you implement, as described in Table 24 on page 400.

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 24 on page 400. You can complete other fields, but they are not required.

Editing Parameter Values in the eapps.cfg File

Provide the parameter values in the eapps.cfg file, as indicated by the guidelines in Table 7.

For information about editing eapps.cfg parameters and about the purposes for the parameters, see “Parameters in the eapps.cfg File” on page 192.

Table 7. Parameter Values in eapps.cfg File

Section	Parameter	Suggested Entry	Guideline

[defaults]	`SingleSignOn`
	`TrustToken`
	`UserSpec`
	`UserSpecSource`
			If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Table 7. Parameter Values in eapps.cfg File

Section	Parameter	Suggested Entry	Guideline
The section particular to your application, such as [/eservice], [/echannel], or [/callcenter]	`AnonUserName`		Enter the user ID of the seed data User record provided for the application that you implement or of the User record you create for the anonymous user. This entry also matches the uid (LDAP) or sAMAccountName (ADS) entry for the anonymous user record in the directory. For example, enter `GUESTCST` for Siebel eService.
	`AnonPassword`		Enter the password you created in the directory for the anonymous user.
	`AnonUserPool`	100, or another positive number	

	`SingleSignOn`
	`TrustToken`
	`UserSpec`
	`UserSpecSource`
	`ProtectedVirtualDirectory`
			If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Editing Parameter Values in the Application Configuration File

Provide the parameter values as indicated by the guidelines in Table 8 in the configuration file for the Siebel application you are implementing. For a list of Siebel application configuration files, refer to *Siebel Server Administration Guide*.

NOTE: You can use a text editor to make changes to an application configuration file or you can use the LDAP/ADSI Configuration Utility to make these changes. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 159.

For information about editing an application's configuration file and about the purposes for the parameters, see "Siebel Application Configuration File Parameters" on page 197.

Table 8. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
[SWE]	`AllowAnonUsers`	Enter `TRUE` for LDAP and ADSI.
	`SecureLogin`	Enter `TRUE` or `FALSE`. If `TRUE`, the login request (HTTP POST) from the login form is transmitted using HTTPS. For information about other requirements for secure login, see "Secure Login" on page 169.
[SecurityAdapters]	Add a line for each security adapter you may implement; most likely there is only one.	■ LDAP suggested entry is `LDAP`. ■ ADSI suggested entry is `ADSI`.
The section for the particular security adapter you implement, for example [LDAP] or [ADSI]	`DllName`	■ For LDAP, enter `sscfldap`. You do not need to include the file extension (for example `sscfldap.dll`). If you enter `sscfldap` here, it is converted internally to the actual filename for your operating system. ■ For ADSI, enter `sscfadsi.dll`.

Table 8. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
	`ServerName`	LDAP and ADS, enter the name of the machine on which the LDAP or ADS server runs. For more information, see "Siebel Application Configuration File Parameters" on page 197.
	`Port`	■ The LDAP suggested entry is `389`. Typically, use port 389 for standard transmission or port 636 for secure transmission. ■ For ADSI, you set the port at the ADS directory level, not as a configuration parameter. If this parameter is present, comment it out, or you can delete the line from the file.

	`BaseDN`	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.
		■ LDAP suggested entry (including quotes):
		`"ou=People, o=`*`domain_name`*`"`
		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 subdirectory in which users are stored.
		■ ADSI suggested entry (including quotes):
		`"CN=Users, DC=`*`machine_name`*`, DC=`*`domain_name`*`, DC=com"`
		Domain Controller (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for the user objects in the directory. Therefore, adjust the number of DC and CN entries to represent your architecture.

Table 8. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters
	`UserNameAttributeType`	■ The LDAP suggested entry is `uid` ■ The ADSI suggested entry is `sAMAccountName` If you use a different attribute in the directory for the Siebel user ID, enter that attribute name.
	`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 Siebel ADSI adapter. If this parameter is present, comment it out, or delete the line from the file.
	`CredentialsAttributeType`	The LDAP and ADSI suggested entry is `dbaccount` If you used a different attribute in the directory for the database account, enter that attribute name.

	`ApplicationUser`	■ LDAP suggested entry (including quotes):
		`"uid=APPUSER, ou=People, o=`*`domain_name`*`"`
		■ ADSI suggested entry (including quotes):
		`"CN=APPUSER, CN=Users, DC=`*`machine_name`*`, DC=`*`domain_name`*`, 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.

	`ApplicationPassword`	For LDAP and ADSI, enter `APPUSERPW` or the password assigned to the application user.

Table 8. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel LDAP and ADSI Adapters

	`SharedCredentialsDN`	■ LDAP suggested entry (including quotes):
		`"uid=anonymous user User ID, ou=People, o=`*`domain_name`*`"`
		For example:
		`"uid=GUESTCST, ou=People, o=siebel.com"`
		■ ADSI suggested entry (including quotes):
		`"CN=anonymous user User ID, CN=Users, DC=`*`machine_name`*`, DC=`*`domain_name`*`, DC=com"`
		For example:
		`"CN=GUESTCST, CN=Users, DC=qa1, DC=siebel, DC=com"`

	`RolesAttributeType`
	`SslDatabase`
	`UseSSL`
	`EncryptCredentialsPassword`
	`EncryptApplicationPassword`
	`SingleSignOn`
	`TrustToken`
	`UseAdapterUsername`
	`SiebelUsernameAttributeType`
	`UseRemoteConfig`
		If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Editing Name Server Parameters

Set each Name Server parameter listed in Table 9 for the component that corresponds to the Application Object Manager for the application you are implementing, such as Call Center Object Manager or eService Object Manager. Set the parameters at the component level and follow the guidelines provided in the table.

For information about setting Name Server parameters, see "Name Server Parameters" on page 205.

Table 9. Name Server Parameters

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

Setting System Preferences

Set each system preference using the guidelines in Table 10.

For information about setting system preferences, see "System Preferences" on page 209.

Table 10. System Preferences

System Preference	Suggested Entry	Guideline
SecExternalUserAdministration	FALSE	An entry of FALSE allows administration of the directory through the Siebel application.
SecThickClientExtAuthent	FALSE	You set this system preference to TRUE to allow Dedicated Web Clients to use a security adapter.
Security Adapter CRC		Calculate the checksum value for your security adapter DLL as described in "Checksum Validation" on page 179. Enter the calculated value here.

Restarting Servers

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

- **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 service.** In the Windows NT Control Panel, double-click Services. In Windows 2000, choose Start > Programs > Administrative Tools > Services.

Testing the External Authentication System

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

- Provide a Web page on which the user can log in.

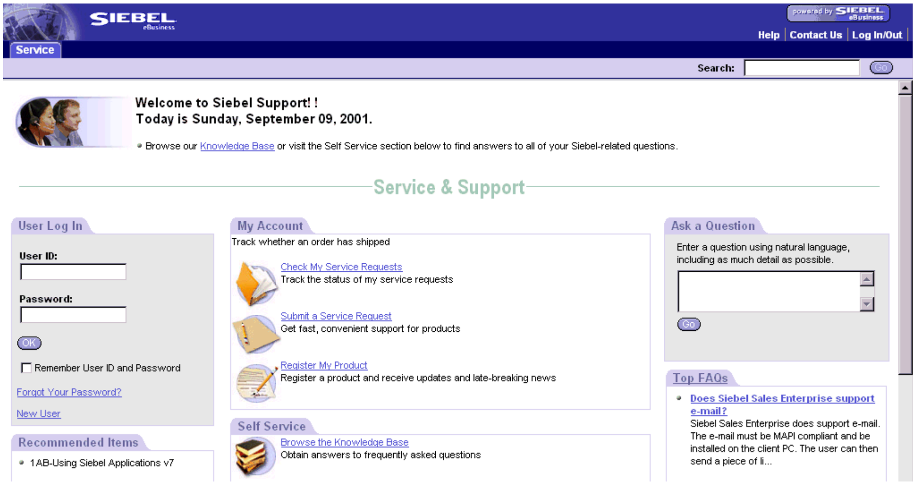
- Allow an authenticated user to log in.
- Allow a user to browse anonymously, if applicable to your Siebel application.
- Allow a user to self-register, if applicable to your Siebel application.

To test your external authentication system

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

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

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



Welcome to Siebel Support! !
Today is Sunday, September 09, 2001.

- Browse our Knowledge Base or visit the Self Service section below to find answers to all of your Siebel-related questions.

Track whether an order has shipped

Check My Service Requests
Track the status of my service requests

Submit a Service Request
Get fast, convenient support for products

Register My Product
Register a product and receive updates and late-breaking news

Browse the Knowledge Base
Obtain answers to frequently asked questions

- 1AB-Using Siebel Applications v7

Enter a question using natural language, including as much detail as possible.

- **Does Siebel Sales Enterprise support e-mail?**
  Siebel Sales Enterprise does support e-mail. The e-mail must be MAPI compliant and be installed on the client PC. The user can then send a piece of li...

2 If you see screen tabs, such as the ones shown for Siebel eService, click on various tabs to access screens intended for anonymous browsing. Employee applications, such as Siebel Call Center, typically do not allow anonymous browsing, while most other Siebel applications do.

3 Navigate back to the Web page that contains the login text boxes, and then log in with the user ID and the password for the test user you created. Enter `TESTUSER` or the user ID you created and `TESTPW` or the password you created.

   More screen tabs should appear, indicating that the test user is authenticated successfully and the user record in the database is providing views through the expanded responsibility of this registered user.

4 Click Logout.

5 Repeat Step 1 on page 130 to access the login page again. If a New User button is present, click it. If a New User button is not present, your Siebel application, without additional configuration, does not allow users to self-register.

   The Personal Information form appears.

6 Complete the required fields on the Personal Information form, 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 login name.
Password	Optional (though required for some authentication implementations). Required. Enter a simple contiguous login password and record it.
Verify Password	Required.
Challenge Question	Required. Enter a phrase for which there is an "answer." If you later click 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 131.

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

Web Single Sign-On and Remote Authentication 7

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

Overview of 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.

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

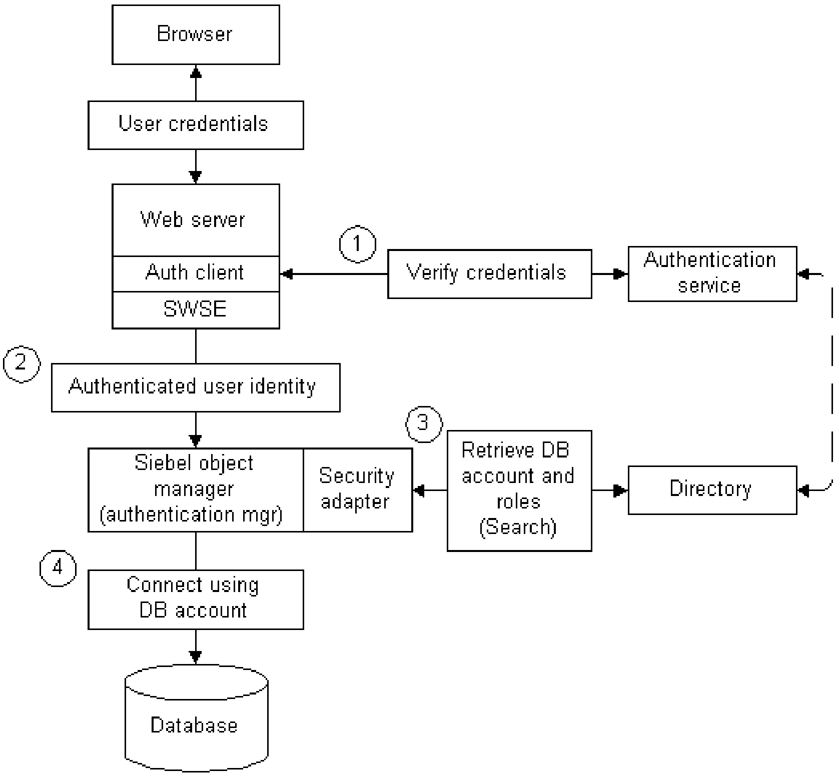


Figure 11. Web SSO Authentication

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 Siebel Web Server Extension (SWSE) passes the authenticated user's username to the authentication manager, a component of the Application Object Manager. The username can be the Siebel user ID or another attribute.

3. The security adapter provides the authenticated user's username to a directory, from which the user's Siebel user ID, a database account, and, optionally, roles are returned to the authentication manager.

4. The Object Manager uses the returned credentials to connect the user to the database and to identify the user.

Because Web SSO deployments assume that user authentication and user management are the responsibility of the third-party security infrastructure, the following capabilities are not available, as Siebel eBusiness Applications features, in a Web SSO environment:

- User self-registration
- Delegated administration of users
- Login forms
- Logout links or the Log Out menu item in the File application-level menu
- Change password

Your Siebel applications may require configuration changes to hide such functionality. For more information, refer to *Siebel Tools Reference*.

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

NOTE: For a particular Siebel application, when users connect from the Siebel Dedicated or Mobile 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, however, mobile users must use database authentication.

For information about authentication options for local database synchronization for mobile users, see *Siebel Remote and Replication Manager Administration Guide*.

Task Overview

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

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

- Create user records in the authentication service, in the directory, and in the Siebel Database.
- Set up a security adapter as a plug-in to the Application Object Managers.
- Edit the eapps.cfg file to provide authentication parameter values.
- Edit the configuration file for each Application Object Manager to provide authentication parameter values.
- Edit authentication-related parameters in the Name Server of the Siebel Gateway.
- Set system preferences.
- Restart the Siebel Server and the Web server.
- Test the implementation.

Deployment Options for Web SSO

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

- **User specification source.** You must specify the source from which the Siebel Web Engine derives the user's identity key: a Web server environment variable or an HTTP request header variable.
- You can also implement any of the options that are described in "Security Adapter Deployment Options" on page 107.

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

For information about authentication options and procedures for implementing them, see "Authentication Options" on page 167.

For information about special considerations to implementing user authentication, see "User Authentication Issues" on page 393.

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 Siebel accepts the authentication result in the form of Web SSO.

For information on implementing digital certificate authentication for Web SSO, see "Digital Certificate Authentication" on page 191.

Setting Up Web SSO: A Scenario

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

Make sure you implement Web SSO in a development environment before deploying it in a production environment. You can repeat the appropriate instructions here to provide Web SSO access to additional Siebel applications. To implement other options, see "Authentication Options" on page 167.

These instructions implement the following basic configuration:

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

  - It provides the Siebel user ID and the database account for authenticated Web server users.

- The Siebel ADSI adapter is used to communicate between the authentication manager and the ADS.
- The Siebel Server, which includes the Application Object Managers 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 Adapters for External Authentication" on page 27. You must adapt the applicable parts of the following implementation to your security adapter.

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

- Your Web server and the ADS are installed on different machines.
- The Siebel applications, including the Siebel Gateway and the Siebel Server, are installed. The Siebel Server, including affected Application Object Managers, is installed on the Web server machine.

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

Process of Implementing Web SSO

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

- Create protected virtual directories for Siebel applications on the Web server machine. See "Creating Protected Virtual Directories" on page 140.
- Create a database login for users who are authenticated externally. See "Creating a Database Login" on page 143.

- Set up the ADS. See “Setting Up the Active Directory Server” on page 143.
- 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 145.
- 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 146.
- Edit eapps.cfg file parameters. See “Editing Parameter Values in the eapps.cfg File” on page 148.
- Edit the Siebel application’s configuration file parameters. See “Editing Parameter Values in the Application Configuration File” on page 149.
- Edit the Name Server parameters. See “Editing Name Server Parameters” on page 153.
- Set system preferences. See “Setting System Preferences” on page 154.
- Restart the Siebel Server and the Web server. See “Restarting Servers” on page 155.
- Test the implementation. See “Testing the Web SSO Authentication” on page 155.

Creating Protected Virtual Directories

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

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

- Create the virtual directory.

- Specify to the Web server a particular DLL file that allows the Siebel Web Server Extension 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 by doing *one* of the following:

- Windows NT: From the Start menu choose Programs > Windows NT 4.0 Option Pack > Microsoft Internet Information Service > Internet Service Manager.
- Windows 2000: From the Start menu 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 Siebel Web Server Extension).

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 Siebel Web Server Extension to communicate with the Web server

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

The Properties dialog box appears.

2 Click Configuration.

The Application Configuration dialog box appears.

3 Click Add.

The Add/Edit Application Extension Mapping dialog box appears.

4 Click Browse, navigate to and select the sweiis.dll file in the *SWEAPP_ROOT*\bin directory, and then click Open (where *SWEAPP_ROOT* is the directory in which you installed the Siebel Web Server Extension).

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

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

You must perform separate configuration tasks for the following purposes:

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

Configuring the Active Directory Server as the Directory

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

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

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

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

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

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

Configuring 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 11. The attribute names, sAMAccountName and userPassword, are those suggested in this example. Your entries may vary depending on how you make attribute assignments in "Setting Up the Active Directory Server" on page 143.

Table 11. 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 399, for a Siebel customer or partner application. For example, if you implement Siebel eService, enter GUESTCST.
	■ You can create a new user record or adapt a seed anonymous user record for a Siebel employee application.
		GUESTPW or a password of your choice	username = LDAPUSER
			password = *P*

Application user	APPUSER or a name of your choice	APPUSERPW or a password of your choice	Database account is not required for application user.

A test user	TESTUSER or a name of your choice	TESTPW or a password of your choice	username = LDAPUSER
			password = *P*

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

The database account for all three users is the same, and must match the database account reserved for externally-authenticated users described in "Creating a Database Login" on page 143. *P* represents the password in that database account. For information about formatting the database account attribute entry, see "Requirements for Directory" on page 102.

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

Complete other attribute fields for each user as are needed.

Adding User Records in the Siebel Database

You must create a record in the Siebel Database that corresponds to the test user you create in "Creating Users in the Directory" on page 145.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in Table 24 on page 400. This record must also match the anonymous user you create in "Creating Users in the Directory" on page 145.

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 262.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.

2. From the application-level menu, choose View > Site Map > User Administration > Users.

   The All Users list appears.

3 In the All Users list, click the menu button and choose New Record.

A new All Users form appears.

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

Field	Suggested Entry	Guideline
Last Name		Required. Enter any name.
First Name		Required. Enter any name.
User ID	TESTUSER	Required. This entry must match the 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 24 on page 400.

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 24 on page 400. You can complete other fields, but they are not required.

Editing Parameter Values in the eapps.cfg File

Provide the parameter values in the eapps.cfg file as indicated by the guidelines in Table 12.

For information about editing eapps.cfg parameters and about the purposes for the parameters, see "Parameters in the eapps.cfg File" on page 192.

Table 12. Parameter Values in eapps.cfg File

Section	Parameter	Suggested Entry	Guideline
[defaults]			The values of the parameters in this section are overridden by the parameter values you set in the sections for individual applications.
The section particular to your application, such as [/eservice], [/echannel], or [/callcenter]	`AnonUserName`		Enter the user ID of the seed data User record provided for the application that you implement or of the User record you create for the anonymous user. This entry also matches the sAMAccountName entry for the anonymous user record in the directory. For example, enter `GUESTCST` for Siebel eService.
	`AnonPassword`		Enter the password you created in the directory for the anonymous user.
	`SingleSignOn`	`TRUE`	
	`TrustToken`		Enter `HELLO`, or a contiguous string of your choice.
	`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.

Table 12. Parameter Values in eapps.cfg File

Section	Parameter	Suggested Entry	Guideline
	`ProtectedVirtualDirectory`		Generally, you would enter the name of the protected virtual directory that you created in "Creating Protected Virtual Directories" on page 140. For more information on usage for this parameter, see "Parameters in the eapps.cfg File" on page 192.
	`AnonUserPool`		If this parameter is present, comment it out with a semicolon at the beginning of the line. Alternatively, you can delete this parameter line from the file.

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

Editing Parameter Values in the Application Configuration File

Provide the parameter values as indicated by the guidelines in Table 13 in the configuration file for the Siebel application you are implementing. For a list of Siebel application configuration files, refer to *Siebel Server Administration Guide*.

NOTE: You can use a text editor to make changes to an application configuration file or you can use the LDAP/ADSI Configuration Utility to make these changes. For more information, see "Using the LDAP/ADSI Configuration Utility" on page 159.

For information about editing an application's configuration file and about the purposes for the parameters, see "Siebel Application Configuration File Parameters" on page 197.

Table 13. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI 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 "Secure Login" on page 169.
[SecurityAdapters]	Add a line for each security adapter you may implement; most likely there is only one.	Suggested entry `ADSI = ADSI`

Table 13. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
The section for the particular security adapter you implement, for example [ADSI]	`DllName`	Enter `sscfadsi.dll`
	`ServerName`	Enter the name of the machine on which the ADS server runs. *Note:* 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 Siebel ADSI security adapter.
	`Port`	You set the port at the ADS directory level, not as a configuration parameter. If this parameter is present, comment it out, or you can delete the line from the file.
	`BaseDN`	■ The Base Distinguished Name is the root of the tree under which users are stored. Users can be added directly or indirectly below this subdirectory. ■ Suggested entry (including quotes): `"CN=Users, DC=machine, DC=domain, 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.

Table 13. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
	`UserNameAttributeType`	■ Suggested entry: `sAMAccountName` If you use a different attribute in the directory for the Siebel user ID, enter that attribute name.
	`PasswordAttributeType`	ADS does not store the password in an attribute, so this parameter is not used with the Siebel ADSI adapter. If this parameter is present, comment it out, or delete the line from the file.
	`CredentialsAttributeType`	Suggested entry: `dbaccount` If you used a different attribute in the directory for the database account, enter that attribute name.
	`ApplicationUser`	■ Suggested entry (including quotes): `"CN=APPUSER, CN=Users, DC=machine, DC=domain, 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.
	`ApplicationPassword`	Enter `APPUSERPW` or the password you assigned to the application user.
	`SingleSignOn`	Enter `TRUE`.

Table 13. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for Siebel ADSI Adapter
	`TrustToken`	Enter the TrustToken value that you provided for the same variable in the eapps.cfg file.

	`RolesAttributeType`
	`SslDatabase`
	`UseSSL`
	`EncryptCredentialsPassword`
	`EncryptApplicationPassword`
	`SharedCredentialsDN`
	`UseAdapterUsername`
	`SiebelUsernameAttributeType`
	`UseRemoteConfig`
		If these parameters are present, comment out each with a semicolon at the beginning of the line. Alternatively, you can delete these parameter lines from the file.

Editing Name Server Parameters

Set each Name Server parameter listed in Table 14 on page 154 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 "Name Server Parameters" on page 205.

Table 14. Name Server Parameters

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

Setting System Preferences

Set each system preference using the guidelines in Table 15.

For information about setting system preferences and the purposes for the preferences, see "System Preferences" on page 209.

Table 15. System Preferences

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

Restarting Servers

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

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

Testing the 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.

Remote Authentication

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

Some things to remember about remote users includes:

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

To synchronize

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

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

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

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

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

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

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

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

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

The Siebel Remote Synchronization Manager authenticates incoming Mobile Web Client requests to make sure that a Mobile Web Client is valid. The Siebel Remote Synchronization Manager validates the Mobile Web Client'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.

The Siebel Remote 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, the Synchronization Manager reconnects the Mobile Web Client to another Siebel Remote server and updates the client's local configuration information.

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

- **None.** Does not validate the Mobile Web Client's password. This is the default setting.

- **Database.** Uses the Mobile Web Client's user name and password to connect Mobile Web Clients to the server database.

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

- **Siebel.** Validates the Mobile Web Client's password against the password stored in the Mobile Web Client's screen.

- **AppServer.** Verifies that the password is the same as the user's operating system password on the Siebel Server.

4 Once the remote user is authenticated, synchronization begins.

Authentication Details 8

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

Using the LDAP/ADSI Configuration Utility

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

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

CAUTION: The LDAP/ADSI Configuration Utility overwrites rather than appends configuration files. To prevent losing important configuration information, use the utility to create a new file, then copy the results to the desired *.cfg file for your Siebel application.

To run the LDAP/ADSI Configuration Utility

1 Do one of the following:

- In a Windows implementation, choose Start > Run, then type:

  ```
  SIEBSRVR_ROOT\ADMIN\CONFIG\config.exe
  ```

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

```
SIEBSRVR_ROOT/ADMIN/CONFIG/config
```

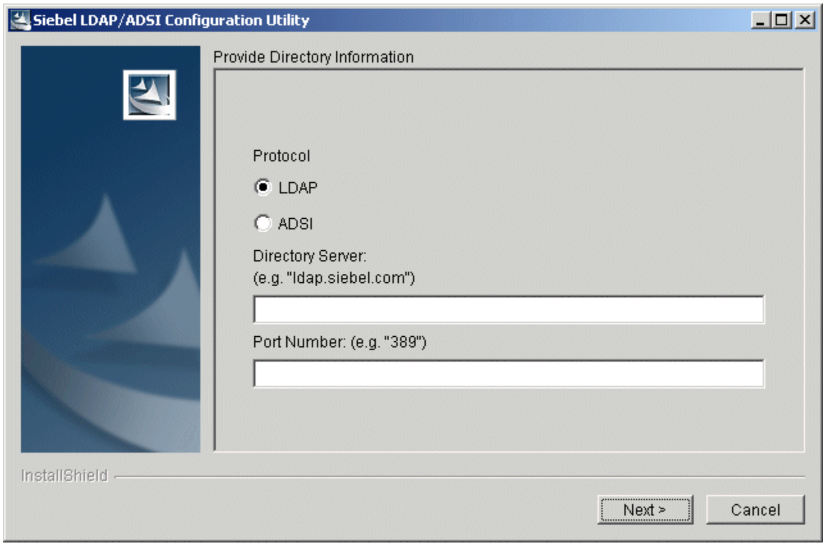
where *SIEBSRVR_ROOT* is the installation directory for the Siebel Server.

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

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

2 A series of screens appears with a list of LDAP/ADSI configuration settings.

The following figure shows an example of an LDAP/ADSI configuration screen.



Siebel LDAP/ADSI Configuration Utility

Provide Directory Information

Protocol

● LDAP

○ ADSI

Directory Server:
(e.g. "ldap.siebel.com")

Port Number: (e.g. "389")

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

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

3. Enter configuration information pertaining to directories:

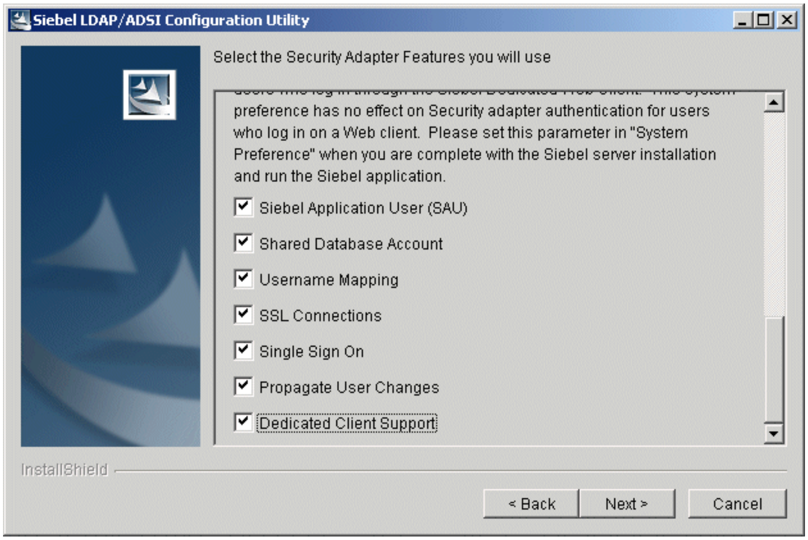
   - **Protocol.** The type of directory you are configuring: LDAP or ADSI
   - **Directory Server.** For LDAP, this is the name of the Directory Server (for example, ldap.siebel.com). For ADSI, you can specify a Domain Name in this field. (For domains that contain more than one directory server, specifying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

4. Enter configuration information pertaining to attribute mapping:

   - **Username Attribute.** The Siebel user ID attribute (`UserNameAttributeType`) used by the directory. The suggested entry for an LDAP directory is `uid`. The suggested entry for ADSI is `sAMAccountName` (maximum length of 20 characters). If your directory uses a different attribute for the Siebel user ID, enter that attribute instead.
   - **Database Account Attribute.** The `CredentialsAttributeType` used by the directory. For LDAP and ADSI, the suggested entry is `dbaccount`. If your directory uses a different attribute for the database account, enter that attribute instead.
   - **Roles Attribute.** The attribute type for roles stored in the directory (`RolesAttributeType`). This setting is required only if you use roles in your directory. For more information on roles, see "Roles" on page 167.

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

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



Siebel LDAP/ADSI Configuration Utility

Select the Security Adapter Features you will use

preference has no effect on Security adapter authentication for users who log in on a Web client. Please set this parameter in "System Preference" when you are complete with the Siebel server installation and run the Siebel application.

☑ Siebel Application User (SAU)

☑ Shared Database Account

☑ Username Mapping

☑ SSL Connections

☑ Single Sign On

☑ Propagate User Changes

☑ Dedicated Client Support

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

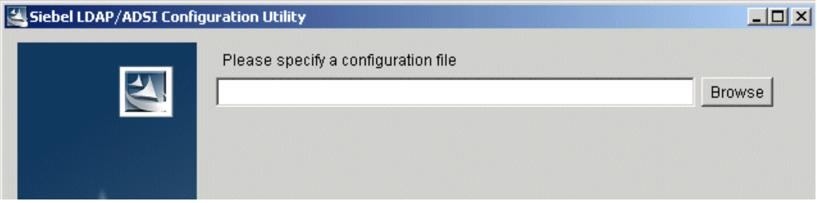
Option	Description	Required Settings
Siebel Application User (SAU)	Allows you to specify a single directory account that the Siebel application uses to search, update or read directory entries. Creating an SAU account allows you to limit directory access by individual end users. For more information, see "Application User" on page 175.	This option requires a user name and password for the account: ■ SAU Distinguished Name This is the full distinguished name of the Siebel Application User (ApplicationUser). Make sure you include the quotes in the name. ■ SAU Password This is the password you specify for the Siebel Application User. If you create a Siebel Application User, make sure you also add this name and password to the directory.
Shared Database Account	This option simplifies directory administration by enabling multiple-user entries in a directory to share the same database account. Without this option, a database account must be created for each user entry in the directory. For more information, see "Shared Database Account" on page 183.	This option requires specifying the following information: ■ Distinguished Name for the Shared Database Account This is the distinguished name (SharedCredentialsDN) for the directory entry that is used to share the database account. For example: `"uid=SHAREDENTRY, ou=People, o=xzy.com"` ■ Shared Database Account Attribute This is the attribute (CredentialsAttributeType) used to store the database account in the directory (for example, `dbaccount`).

Option	Description	Required Settings
Username Mapping	This option allows users to be authenticated by something other than the Siebel user ID (for example, a social security number, phone number, or email address). As with Siebel user ID, this identifier must be unique. For more information, see "Adapter-Defined User Name" on page 184.	This option requires specifying: ■ Username Attribute This is the name of the attribute used to authenticate users. The security adapter references this attribute instead of the Siebel user ID attribute (for example, `email_ID`). ■ Username Field (in Siebel) This is the name of the field in the Siebel interface (`OM - Username BC Field Name`) that stores the Username Attribute (for example, `Email Address`). ■ Siebel User ID Attribute This is the attribute `SiebelUsernameAttributeType` used by the security adapter to retrieve the Siebel user ID for an authenticated user (for example `uid`).
Single Sign-On	This option sets Web SSO. With Web SSO, users can access multiple applications from a single login page. When Web SSO is enabled, user credentials are verified by a third-party authentication service instead of the security adapter.	Selecting this option sets the `SingleSignOn` attribute to `TRUE`. This option also requires specifying: ■ Shared Secret This is the value of the `TrustToken` attribute used by the security adapter and the Web server to prevent Siebel Web Engine spoofing attacks (for example, `HELLO`). The value you enter must match the `TrustToken` value used by the Web server.
	Note: The LDAP/ADSI utility only sets the Web SSO parameters in a Siebel application configuration file. You must also set the parameters in your eapps.cfg file. For more information about setting up Web SSO, see "Implementing Web SSO Authentication" on page 136.	

Option	Description	Required Settings
Propagate User Changes	This option displays instructions on how to enable Siebel applications to propagate user changes to the directory. When this option is enabled, the directory is updated automatically when users are added or passwords changed in a Siebel application.	To enable this option, use the Application Administration screen in your Siebel application to set the system preference SecExternalUserAdministration to FALSE. For more information, see "System Preferences" on page 209.
Dedicated Client Support	This option displays instructions on how to enable security adapter authentication for users who log in through the Siebel Dedicated Web Client.	To enable this option, use the Application Administration screen in your Siebel application to set the system preference SecThickClientExtAuthent to TRUE. For more information, see "System Preferences" on page 209.

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

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


Siebel LDAP/ADSI Configuration Utility
Please specify a configuration file
Browse

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

For more information on where configuration files are located for Siebel eBusiness Applications, see "Siebel Application Configuration File Parameters" on page 197.

7 Click Next to add configuration information to the file you specify.

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

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

Authentication Options

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

For information about:

- Parameters in the eapps.cfg file, see "Parameters in the eapps.cfg File" on page 192.
- Application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.
- Name Server parameters, see "Name Server Parameters" on page 205.
- System preferences, see "System Preferences" on page 209.
- Seed data, see "Seed Data" on page 399.

Roles

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

- Siebel security adapter authentication
- Web SSO

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

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

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

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

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

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

- In the [*adapter_name*] section, for example [LDAP], set

  ```
  RolesAttributeType= attribute_in_which_roles_are_stored
  ```

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

Roles are discussed in a usage context in "Requirements for Directory" on page 102.

NOTE: Do not confuse roles defined by an LDAP or ADS directory with roles defined in the Siebel application interface. Roles in LDAP or ADS directories are collections of responsibilities that strictly enforce access to views and data records within Siebel applications. Roles defined in the application interface allow application administrators to increase the usability and deployability of the application by tailoring the product to groups of users. For more information about roles defined in an application interface, see "Creating and Administering Roles" on page 377.

Secure Login

With secure login, you can specify to the Siebel Web Engine to transmit user credentials from the browser to the Web server over HTTPS.

Secure login can be implemented in the following authentication strategies:

- Database authentication
- Siebel security adapter authentication
- Web SSO

To implement secure login

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

  ```
  SecureLogin = TRUE
  ```

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

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

Secure login is discussed in a usage context in "Implementing Database Authentication" on page 98, and in "Deployment Options for Security Adapter Authentication" on page 113.

User Password Encryption

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

User password encryption can be implemented in the following authentication strategies:

- Database authentication
- Siebel security adapter authentication

NOTE: You can implement user password encryption with the Siebel encryption utility. This utility and applicable installation instructions are available from Siebel Technical Support.

Password encryption has the following implications for Siebel Server components:

- With database authentication, encrypted passwords are stored in the Siebel Database. Siebel Server components that log into the database must use the encrypted password value stored in the database. For example, when you run the Generate Triggers (GenTrig) component, the value provided for the `PrivUserPass` parameter (used with the `PrivUser` parameter) must be the encrypted password value. Otherwise, component login will fail.
- If `Application Encrypt Password` is set to `TRUE` at the server level, the password must also be encrypted for the Server Request Broker and Server Request Processor components. Otherwise, component login will fail.

User password encryption supports the following principles:

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

- The unencrypted version of the password is given to a user to use when logging in.

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

- The user logs in with user credentials that include the unencrypted password.
- The authentication manager receives the user credentials, and passes them to the Application Object Manager.
- The Application Object Manager encrypts the password (`T>?Be`).
- In an external authentication environment:
  - The user credentials, including the encrypted password are passed to the security adapter through the authentication manager.
  - The security adapter verifies that the encrypted password matches the encrypted password stored in the directory for the user, and then returns the database account and the Siebel user ID to the Application Object Manager through the authentication manager.
- In a database authentication environment, the Application Object Manager verifies that the database account identified by the user credentials exists and that the encrypted user password matches the password for the database account (`T>?Be`).
- The Application Object Manager connects the user to the database and the Siebel application.

To implement user password encryption

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

     ```
     encrypt password
     ```

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

     ```
     encrypt siebel
     ```

     The confirmation from the utility is similar to:

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

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

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

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

- To encrypt multiple passwords using a batch file:

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

  ```
  encrypt @passwords.txt
  ```

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

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

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

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

4. Set the `Application Encrypt Password` parameter in the Name Server to `TRUE` at one of the following levels.

   - To implement user password encryption for a single application, set the parameter at the component level for the Application Object Manager, such as Call Center Object Manager.

   - To implement user password encryption for all applications on a particular Siebel Server, set the parameter at the server level for the particular Siebel Server.

   For information about setting Name Server parameters, see “Name Server Parameters” on page 205.

5. If you encrypted the password for the anonymous user, you must also modify the `AnonPassword` parameter in the eapps.cfg file.

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

User password encryption is discussed in a usage context in "Implementing Database Authentication" on page 98 and in "Security Adapter Deployment Options" on page 107.

Credentials Password Encryption

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

Credentials password encryption can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

NOTE: You can implement credentials password encryption with the Siebel encryption utility. This utility and applicable installation instructions are available from Siebel Technical Support.

Credentials password encryption supports the following principles:

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

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

- The authenticated user's database account, stored in the directory, is passed to the authentication manager by the security adapter.
- The Application Object Manager receives the user credentials from the authentication manager.

- The Application Object Manager encrypts the password (`T>?Be`).
- The Application Object Manager verifies that the database account identified by the user credentials exists and has a password that matches the encrypted version (`T>?Be`).
- The Application Object Manager connects the user to the database and the Siebel application.

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

To implement credentials password encryption

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

     ```
     encrypt password
     ```

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

     ```
     encrypt siebel
     ```

     The confirmation from the utility is similar to:

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

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

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

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

   - To encrypt multiple passwords using a batch file:

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

```
encrypt @passwords.txt
```

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

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

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

   In the [*adapter_name*] section, for example [LDAP]:

   ```
   EncryptCredentialsPassword = TRUE
   ```

   For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

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

   For information about required attributes in the directory, see "Requirements for Directory" on page 102.

Credentials password encryption is discussed in a usage context in "Security Adapter Deployment Options" on page 107.

Application User

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

- Siebel security adapter authentication
- Web SSO

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

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

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

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.

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

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

It is strongly recommended that you implement an application user.

To implement an application user

1. In the directory, define a user that uses the same attributes as other users. Assign values in appropriate attributes that contain the following information:
    - **Username.** Assign a name of your choice. If you implement an adapter-defined username, use that attribute. Otherwise, use the attribute in which you store the Siebel user ID, although the application user does not have a Siebel user ID.

- **Password.** Assign a password of your choice. You can opt to enter an encrypted password if you implement application password encryption. If you implement an ADS directory, you specify the password using ADS user management tools, not as an attribute.

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

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

   - In the [*adapter_name*] section, for example [LDAP]:

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

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

   - If you implement application user password encryption:

     ```
     EncryptApplicationPassword = TRUE
     ```

For information about setting Siebel application configuration file parameters, see “Siebel Application Configuration File Parameters” on page 197.

For information about application user password encryption, see “Application User Password Encryption” that follows.

The application user is discussed in a usage context in “Implementing LDAP and ADSI Security Adapter Authentication” on page 111 and in “Implementing Web SSO Authentication” on page 136.

Application User Password Encryption

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

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

For information about the application user, see "Application User" on page 175.

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

To implement application user password encryption

1. Create a password and enter it in the attribute in the directory in which the application user's password is stored. If you implement an ADS directory, you specify the password using ADS user management tools, not as an attribute.

2. From a command line run mangle.exe, located in the *SIEBSRVR_ROOT*\bin subdirectory, on the password from Step 1. For example, enter:

   ```
   mangle password
   ```

   The command line returns the encrypted version of the password.

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

   - In the [*adapter_name*] section, for example [LDAP]:

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

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

     ```
     EncryptApplicationPassword = TRUE
     ```

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

Application user password encryption is discussed in a usage context in "Deployment Options for Security Adapter Authentication" on page 113.

Application User and Password Expiration Policies

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

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

Checksum Validation

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

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

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

Checksum validation supports the following principles:

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

To implement checksum validation

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

```
Checksum -f filename
```

The utility returns the checksum value. For example,

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

would return something similar to:

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

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

2 Set the Security Adapter CRC Siebel system preference to the checksum value that is calculated in Step 1 on page 179.

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

For information about setting Siebel system preferences, see "System Preferences" on page 209.

Checksum validation is discussed in a usage context in "Security Adapter Deployment Options" on page 107.

Remote Configuration

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

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

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

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

The 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 eservice.cfg:

```
[Security Adapters]
LDAP = LDAP

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

The following example is from the configuration file ldap_remote.cfg:

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

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

- The Siebel application's configuration file must contain a section that corresponds to a security adapter listed in its [SecurityAdapters] section. For example, the [LDAP] section may contain parameters for the LDAP line in the [SecurityAdapters] section, as shown.

    - It must, at least, include the `UseRemoteConfig` parameter, which provides the path to a remote configuration file in universal naming convention format, that is, \\server\vol\path\filename.cfg.
    - It may include any other parameters typical to this section, or none of them.

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

For information about the Authentication Manager, see "Siebel Authentication Manager" on page 92.

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

Remote configuration is discussed in a usage context in "Security Adapter Deployment Options" on page 107.

Secure Adapter Communications

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

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

To implement SSL for the Siebel LDAP security adapter

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

To implement SSL for the Siebel ADSI security adapter

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

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

Secure Adapter Communications is discussed in a usage context in "Security Adapter Deployment Options" on page 107.

Shared Database Account

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

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

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

To implement a shared database account

1. Create a database account to be shared by all users who log 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 Directory" on page 102.

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

   - In the [*adapter_name*] section, for example [LDAP]:

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

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

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

The shared database account is discussed in a usage context in "Deployment Options for Security Adapter Authentication" on page 113 and in "Setting Up Security Adapter Authentication: A Scenario" on page 114.

Adapter-Defined User Name

This option can be implemented in the following authentication strategies:

- Siebel security adapter authentication
- Web SSO

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

When a user logs in with an adapter-defined user name, the user's Siebel user ID must still be provided to the Application Object Manager.

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

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

Even if other requirements to administer user attributes in the directory through the Siebel client are met, you must also set the `UsernameAttributeType` and `OM - Username BC Field` parameters. Otherwise, changes through the Siebel client to the underlying field are not propagated to the directory.

For example, for users to log in with their work phone number, you must specify UsernameAttributeType to be the directory attribute in which the phone number is stored, for example telephonenumber, and you must define `OM - Username BC Field` to be Phone #, the field in the User business component for work phone number.

To implement an adapter-defined user name

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

   In the [*adapter_name*] section, for example [LDAP]:

   `UseAdapterUsername = TRUE`

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

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

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

   The Application Object Manager parameter to be populated is `UsernameBCField`.

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

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

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

For information about setting Siebel application configuration file parameters, see "Siebel Application Configuration File Parameters" on page 197.

For information about setting Name Server parameters, see "Name Server Parameters" on page 205.

The adapter-defined user name is discussed in a usage context in "Deployment Options for Security Adapter Authentication" on page 113.

User Specification Source

This option can be implemented in the following authentication strategy:

- Web SSO

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

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

To specify the source of the username

- In the eapps.cfg file, provide the following parameter values in either the [defaults] section or the section for each individual application, such as, 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 192.

The user specification source is discussed in a usage context in "Deployment Options for Web SSO" on page 137 and in "Setting Up Web SSO: A Scenario" on page 138.

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 external authentication, the anonymous user must have a corresponding record in the user directory.

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

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

The anonymous user is discussed in a usage context in "Setting Up Security Adapter Authentication: A Scenario" on page 114 and in "Setting Up Web SSO: A Scenario" on page 138.

Anonymous Browsing

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

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

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

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.

NOTE: 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 parameters in application configuration files, see "Siebel Application Configuration File Parameters" on page 197.

Anonymous browsing is discussed in a usage context in "Setting Up Security Adapter Authentication: A Scenario" on page 114.

Secure Views

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

- The value (`TRUE` or `FALSE`) of the view's Secure attribute. For information about the Secure attribute for a view, see *Siebel Tools Reference*.
- The value (`TRUE` or `FALSE`) of the `SecureBrowse` parameter in 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 non-secure 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 non-secure views in Siebel applications. If you are using the Sun ONE Web Server, set the value of `SecureBrowse` to `TRUE`.

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

Digital Certificate Authentication

For customers who have an existing PKI (Public Key Infrastructure) with client certificates, Siebel 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 136, 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.
`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 sections indicated:

```
[SWE]
SecureBrowse = FALSE

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

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

Configuration Parameters Related to Authentication

Configuration parameters specify the authentication strategies and options you implement to the Siebel Web Engine and to Application Object Managers.

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

You set configuration parameters in the following locations:

- The eapps.cfg file
- The configuration file for each Application Object Manager
- Name Server of the Siebel Gateway
- Siebel eBusiness Applications system preferences

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, for all Siebel applications.

The eapps.cfg file is located in the *SWEAPP_ROOT*\bin directory, where *SWEAPP_ROOT* is the directory in which you installed the Siebel Web Server Extension.

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

```
[swe]
Language = enu
Log = all
LogDirectory = D:\10638\SWEApp\log
```

```
ClientRootDir = D:\10638\SWEApp
WebPublicRootDir = D:\10638\SWEApp\public\enu
WebUpdatePassword = test

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

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

[/ebriefings]
ConnectString = siebel.TCPIP.none.NONE://ecollab_blitz:2320/siebel
/eBriefingsObjMgr/ecollab_blitz

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

[ConnMgmt]
CACertFileName = d:\siebel\admin\cacertfile.pem
CertFileName = d:\siebel\admin\certfile.pem
KeyFileName = d:\siebel\admin\kefile.txt
KeyFilePassword = mypassword
PeerAuth = FALSE
PeerCertValidation = FALSE
```

The eapps.cfg file includes sections such as [swe], [defaults], and [connmgmt] and sections for individual Siebel applications, for example [/echannel] and [/callcenter]. Each parameter value in the [defaults] section is used by individual applications, unless you override the parameter's value with an entry in an application's own section.

In the eapps.cfg sample above, the `AnonUserName` and `AnonPassword` values in the [/echannel] section are used by Siebel Partner Portal instead of the values provided in the [defaults] section.

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

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

Authentication-Related Parameters

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

- **AnonUserName.** This parameter is the user name for an anonymous user that is stored in the directory and also in the Siebel Database.

  The anonymous user provides binding between the directory and the Application Object Manager, to allow a Siebel application home page to display to a user who has not logged in. Similarly, this anonymous user supplies a login so the user can see other pages for which you allow anonymous browsing. The home page that is displayed likely provides an interface for the user to log in.

- **AnonPassword.** This parameter is the authenticated password that is paired with `AnonUserName`.

- **AnonUserPool.** This parameter sets the maximum number of anonymous user connections that can provide access to login pages. The anonymous user pool applies to the brief, initial actions taken by the user on the login pages before logging in. After users log in, they have a separate connection.

- **SingleSignOn.** The Siebel Web Server Extension operates in Web SSO mode when `TRUE`.

- **TrustToken.** This token string is a shared secret between the Siebel Web Server Extension and the security adapter. It is a measure to protect against spoofing attacks. This setting must be the same on both the Siebel Web Server Extension and the security adapter.

- **UserSpec.** In a Web SSO implementation, this variable name specifies where the Siebel Web Server Extension looks for a user's username within the source given by `UserSpecSource`. The value, `REMOTE_USER` by default, is populated by the authentication filter.

  If digital certificate authentication is implemented on Windows 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.

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

- **UserSpecSource.** In a Web SSO implementation, this parameter specifies the source from which the Siebel Web Server Extension derives the user credentials: Server, if from the usual Web server user name field; Header, if the variable is within the HTTP request header.

- **ClientCertificate.** When this parameter is set to `TRUE` in a Web SSO implementation, the user is authenticated through a digital certificate.

- **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, refer to *Siebel Web Client Administration Guide*.

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

- **ProtectedVirtualDirectory.** This parameter specifies the protected virtual directory for a Siebel application. This parameter specifies a Web server virtual directory that represents the protected location of the Siebel application. This parameter must have a value in a Web SSO implementation, and is optional in other implementations.

  The protected directory allows you to configure your Web server or third-party authentication software to require user authentication to access specific Siebel application views. Requests for any views that require explicit login are redirected to this virtual directory.

  For more information, see "Creating Protected Virtual Directories" on page 140.

  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 installation 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 will redirect the request in order to authenticate.

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 Siebel Web Server Extension for SSL Encryption" on page 70.

- **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 Application Configuration File Parameters

A configuration file exists for each Siebel eBusiness Application for each language. The parameters in the file determine how the user interacts with the Application Object Manager and with the security adapter.

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

- **Configuration file on the Siebel Server.** For users connecting with the standard Web Client, application configuration files are located in the *SIEBSRVR_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.
- **Configuration file on the Siebel Dedicated Web Client.** For users connecting through the Siebel Dedicated Web Client (or Mobile 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 Dedicated Web Client connects directly to the database; it bypasses the Siebel Server.

For a list of Siebel application configuration files, refer to *Siebel Server Administration Guide*.

For more information about working with configuration files, see *Siebel Web Client 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.

CAUTION: The parameter values that reference directory attributes that you provide for the Siebel LDAP and ADSI adapters are case-sensitive. The values must match the attribute names in the directory.

The following parameters are authentication-related parameters that are present by default or can be added to each application's configuration file. They are grouped by the labeled sections in which they occur. This listing does not include parameters in an application's configuration file that are not authentication-related.

[SWE] section:

- **AllowAnonUsers.** (TRUE or FALSE) Unregistered users are not allowed access to this Siebel application if this parameter value is FALSE.
- **SecureLogin.** (TRUE or FALSE) If TRUE, the login form completed by the user is transmitted over Secure 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 non-secure views, but employee applications (such as Siebel Call Center) do not. For more information, see "Secure Views" on page 190.

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

  For information about the Secure attribute for a view, see *Siebel Tools Reference*.

[SecurityAdapters] section:

- **Adapter Name, for example "LDAP".** Each line you enter here refers to a section in this application's configuration file that contains parameters for a particular security adapter. For example, the line `LDAP = LDAP` means this entry in the security adapters list, `LDAP`, points to an [LDAP] section that follows containing configuration parameters for a particular security adapter, such as the Siebel LDAP security adapter. The names you provide are arbitrary.

[*adapter_name*] section, for example [LDAP]:

Each security adapter's section, for example [LDAP] or [ADSI], corresponds to the right member of a line in the [SecurityAdapters] section. In each security adapter's section, the set of parameters configures how the security adapter is implemented.

Each authentication-related parameter in an application's configuration file is interpreted by either the Application Object Manager or the security adapter (for LDAP or ADSI), or both. If you implement a non-Siebel security adapter, you must configure your adapter to interpret the parameters used by the Siebel adapters if you want to use those parameters.

For information about configuring a non-Siebel security adapter, see "Security Adapters for External Authentication" on page 27.

Some parameters apply only in a Web SSO authentication environment.

- **DllName.** This parameter is interpreted by the Application Object Manager. It is the DLL that implements the security adapter API required for integration with Siebel eBusiness Applications. For example, sscfldap.dll implements the Siebel LDAP adapter in a Windows implementation, and libsscfldap.so does so in a UNIX implementation. If the DLL name for the Siebel LDAP adapter is used in a UNIX implementation, it is converted internally to the actual filename.
- **ServerName.** This parameter is interpreted by Siebel security adapters. It is the name of the machine on which the LDAP or ADS server runs, for example 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 Siebel ADSI security adapter.

- **Port.** This parameter is interpreted by the Siebel LDAP security adapter only. It is the port on the server machine that is used to access the LDAP server. Typically, use 389, the default value, for standard transmission or use 636 for secure transmission. You set the port at the ADS directory level, not as a configuration parameter.
- **BaseDN.** This parameter is interpreted by Siebel security adapters. The Base Distinguished Name is the root of the tree under which users of this Siebel application are stored in the directory. Users can be added directly or indirectly below this directory. A typical entry for an LDAP server might be `BaseDN = "ou=people, o=`*`domain_name`*`"`. "`o`" denotes "organization" and is typically your Web site's domain name. "`ou`" denotes "organization unit" and is the subdirectory in which users are stored.

  A typical entry for an ADS server might be `BaseDN = "CN=Users, DC=qatest, DC=siebel, DC=com"`. Domain Component (DC) entries are the nested domains that locate this server. Common Name (CN) entries are the specific paths for the user objects in the directory. Therefore, adjust the number of CN and DC entries to represent your architecture.

- **UsernameAttributeType.** This parameter is interpreted by Siebel security adapters. It is the attribute type under which the user's login name is stored in the directory. For example, if `UsernameAttributeType = uid`, then when a user attempts to log in with username HKIM, the security adapter searches for a record in which the uid attribute has the value HKIM. This attribute is the Siebel user ID, unless the `UseAdapterUsername` parameter is `TRUE`.

  NOTE: If you implement an adapter-defined user name (`UseAdapterUsername = TRUE`), then you must set the `OM - Username BC Field Name Server` parameter appropriately to allow the directory attribute defined by `UsernameAttributeType` to be updated from the Siebel client. For more information about implementing an adapter-defined user name, see "Adapter-Defined User Name" on page 184.

- **PasswordAttributeType.** This parameter is interpreted by the Siebel LDAP security adapter. It is the attribute type under which the user's login password is stored in the directory.

  `PasswordAttributeType = userPassword` is the only supported value for LDAP. When a user with username HKIM attempts to log in, the security adapter compares the value in the userPassword attribute for HKIM with the password the user enters.

  ADS does not store the password in an attribute, so this parameter is not used with the Siebel ADSI adapter.

- **CredentialsAttributeType.** This parameter is interpreted by Siebel security adapters. It is the attribute type that stores a database account. For example, if `CredentialsAttributeType = dbaccount`, then when a user with username HKIM is authenticated, the security adapter retrieves the database account from the dbaccount attribute for HKIM.

  This attribute value must be of the form `username=`*`U`* `password=`*`P`*, 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 "Shared Database Account" on page 183.

- **RolesAttributeType.** This parameter is interpreted by Siebel security adapters. It is the attribute type for roles stored in the directory. For example, if `RolesAttributeType = roles`, then when a user with username HKIM is authenticated, the security adapter retrieves the user's Siebel responsibilities from the roles attribute for HKIM.

  Responsibilities are typically associated with users in the Siebel Database, but they can be stored in the database, in the directory, or in both. The user gets access to all of the views in all of the responsibilities specified in both sources. However, it is recommended that you define responsibilities in the database or in the directory, but not in both places.

- **SslDatabase.** This parameter is interpreted by the Siebel LDAP security adapter only. It determines whether a Secure Sockets Layer (SSL) is used for communication between the LDAP adapter and the directory. If empty, SSL is not used. If not empty, its value must be the absolute path of a Sun ONE cert7.db file that contains a certificate for the certificate authority that is used by the LDAP server.

- **UseSSL.** (TRUE or FALSE) This parameter is interpreted by the Siebel ADSI security adapter only. If it is set to TRUE, a Secure Sockets Layer (SSL) is used for communication between the ADSI adapter and the ADS directory, otherwise SSL is not used.
- **EncryptCredentialsPassword.** (TRUE or FALSE) This parameter is interpreted by the Application Object Manager. If TRUE, the database password in the directory for an authenticated user is encrypted by a Siebel-provided utility before being sent to the Object Manager. The encrypted version is the valid database login password. This parameter's default value is FALSE.
- **ApplicationUser.** This parameter is interpreted by Siebel security adapters. It is the user name of a record in the directory with sufficient permissions to read any user's information and do any necessary administration.

  If this parameter value is not empty, this user provides the initial binding of the LDAP or Active Directory server with the Application Object Manager 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.

  It is strongly recommended that you implement an application user.
- **ApplicationPassword.** This parameter is interpreted by the Siebel LDAP and ADSI security adapters. It must match the password in the directory for the user defined by the `ApplicationUser` parameter.

  In an LDAP directory, the password is stored in an attribute. In ADS, the password is stored using ADS user management tools. It is not stored in an attribute.
- **EncryptApplicationPassword.** (TRUE or FALSE) This parameter is interpreted by Siebel security adapters. If TRUE, the password in the `ApplicationPassword` parameter is compared with an encrypted version of the password for the application user in the directory.

- **SingleSignOn.** (`TRUE` or `FALSE`) This parameter is interpreted by the Application Object Manager. If `TRUE`, the security adapter is used in Web SSO mode, instead of using security adapter authentication.

- **TrustToken.** This parameter is interpreted by Siebel security adapters. It applies only in a Web SSO environment. The adapter compares the `TrustToken` value provided in the request with the value stored in this application configuration file. If they match, the Application Object Manager accepts that the request has come from the Siebel Web Server Extension, that is, from a trusted Web server. This parameter's default value is an empty string.

- **SharedCredentialsDn.** This parameter is interpreted by Siebel security adapters. It is the absolute path (not relative to the `BaseDN`) of an object in the directory that has the shared database account for the application. If 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.

- **UseAdapterUsername.** (`TRUE` or `FALSE`) This parameter is interpreted by the Application Object Manager. If `TRUE`, this parameter indicates that when the user key passed to the security adapter is not the Siebel user ID, the security adapter retrieves the Siebel user ID for authenticated users from an attribute defined by the `SiebelUsernameAttributeType` parameter. The default value for the `UseAdapterUsername` is `FALSE`.

- **SiebelUsernameAttributeType.** This parameter is interpreted by the Siebel security adapters. If `UseAdapterUsername = TRUE`, this parameter is the attribute from which the security adapter retrieves an authenticated user's Siebel user ID. If this parameter is left empty, the username passed in is assumed to be the Siebel user ID.

- **UseRemoteConfig.** This parameter is interpreted by the Application Object Manager. It is the path to a configuration file that contains only parameters for a security adapter, that is, it contains parameters as they would be formatted if they were included in a section such as [LDAP] in an application's configuration file. The parameter values in the remote configuration file override those in the same section in the application's configuration file.

  You must provide the path in universal naming convention (UNC) format, that is, \\server\vol\path\filename.cfg.

Name Server Parameters

Parameters for the Name Server of the Siebel Gateway can be set at one or more of the enterprise, server, or component levels. They are set in the Server Administration screen of a Siebel employee application such as Siebel Call Center.

Parameters you set at the enterprise level configure all Application Object Managers throughout the enterprise. Parameters set at the server level configure all Application Object Managers on a specific Siebel Server. Parameters set at the component level configure all the tasks, or instances, of a specific component.

For purposes of authentication, all of the components of interest are Application Object Managers, such as the Call Center Object Manager or the eService Object Manager.

A particular parameter set at a lower level overrides the same parameter set at a higher level. For example, if `Security Adapter Name = LDAP` at the enterprise level, and `Security Adapter Name = ADSI` at the component level for the eService Object Manager component, then the ADSI security adapter is used for Siebel eService.

Table 16 lists the authentication-related parameters in the Name Server.

Table 16. Name Server Parameters

Subsystem	Parameter	Description	Set at Enterprise Level	Set at Server Level	Set at Component Level
Object Manager	`OM - Configuration File`	Name of an application's (Application Object Manager's) configuration file, such as eservice.cfg, from which other parameter values are applied, as described in "Siebel Application Configuration File Parameters" on page 197.	X	X	X
	`OM - Data Source`	The data source, such as ServerDataSrc, in the file specified by `OM - Configuration File`, to which these parameters apply.	X		X
	`OM - Proxy Employee`	User ID of the proxy employee. For information about the proxy employee, see "Seed Data" on page 399.	X	X	X

Table 16. Name Server Parameters

Subsystem	Parameter	Description	Set at Enterprise Level	Set at Server Level	Set at Component Level
	`Security Adapter Name`	The name of the security adapter you implement, as it appears as a section in the application configuration file defined by `OM - Configuration File`. For example, enter `LDAP` if the section of security adapter parameters is the [LDAP] section.	X	X	X
	`OM - Username BC Field`	This parameter is used only if you implement an adapter-defined username. It specifies the field of the User business component that populates the attribute in the directory defined by the `UsernameAttributeType` parameter in the application's configuration file. That is, when the user ID (LoginName field in the User business component) is not the identity key, this field is. If this parameter is not present in the parameters list, you must add it.	X	X	X

Table 16. Name Server Parameters

Subsystem	Parameter	Description	Set at Enterprise Level	Set at Server Level	Set at Component Level
Infrastructure Objmgr configu	`Application Encrypt Password`	This parameter is useful for preventing users from logging directly into the server database using a non-Siebel application such as SQL*Plus. ■ If `TRUE` in a database authentication environment, the password entered by the user at login is encrypted before being passed to the database. ■ If `TRUE` in an external authentication environment, the password entered by the user or passed to the SWSE by a third-party authentication client is encrypted before being compared with the password stored for the user in the directory. When enabled, a Siebel-supplied encryption algorithm is applied to the password before it is used to authenticate. ■ To function properly, the database account or directory password with which it is compared must also be set up with the encrypted version of the password. ■ This parameter is not supported for Mobile Web Client. ■ If you are using the Dedicated Web Client, include an `EncryptPassword` parameter in the [Siebel] section of the application .cfg file (for example, `EncryptPassword = "TRUE"`)		X	X

To set Name Server parameters

1. Log into a Siebel employee application, such as Siebel Call Center, and make one of the following choices from the application-level menu:
   - To set enterprise level parameters, choose View > Site Map > Server Administration > Enterprise Configuration.
   - To set server level parameters, choose View > Site Map > Server Administration > Servers.
   - To set component level parameters, View > Site Map > Server Administration > Components.
2. If you are setting parameters at the server or component level, select the applicable server or component.
3. Do one of the following:
   - To set enterprise-level parameters, click the Enterprise Parameters view tab.
   - To set server-level parameters, click the Server Parameters view tab.
   - To set component-level parameters, click the Component Parameters view tab.
4. Select a parameter record, edit the Current Value field, and then click Save.
5. Restart the Siebel Server before the changes take effect.

System Preferences

You can set various authentication-related system preferences for Siebel applications in the Application Administration screen. System preferences are enterprise-wide settings.

Following are authentication-related system preferences:

- **SecExternalUserAdministration.** (TRUE or FALSE) In a security adapter authentication architecture, you must set this preference to FALSE to allow administration of the directory through Siebel applications. When an administrator then adds a user or changes a password from within a Siebel application or a user self-registers, the change is propagated to the directory.

  NOTE: A non-Siebel security adapter must support the SetUserInfo and ChangePassword methods to allow dynamic directory administration. For information about implementing a non-Siebel security adapter, see "Security Adapters for External Authentication" on page 27.

- **SecThickClientExtAuthent.** (TRUE or FALSE) You must set the SecThickClientExtAuthent system preference to TRUE to allow security adapter authentication for users who log in through the Siebel Dedicated Web Client. This system preference has no effect on security adapter authentication for users who log in on a Web Client.

- **Security Adapter CRC.** You can implement checksum validation to verify that each user gains access to the database through the correct security adapter. This preference contains the value calculated by the checksum utility for the applicable security adapter DLL. If you leave this value empty, the system does not perform the check. If you upgrade your system, you must recalculate and replace the value in this system preference.

  For information about checksum validation, see "Checksum Validation" on page 179.

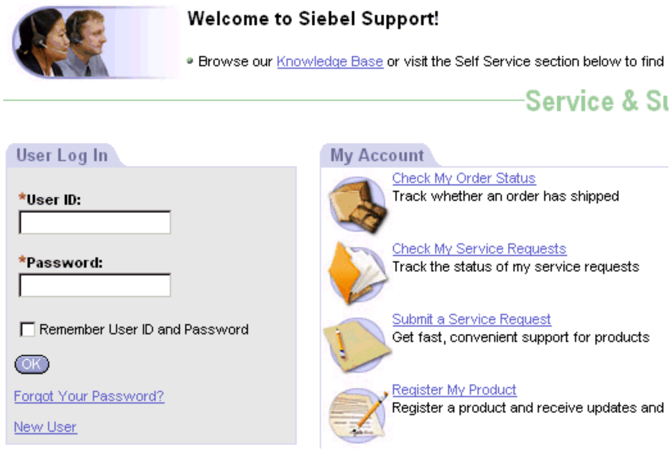
To edit a system preference

1. Log in as an administrator to a Siebel employee application.
2. Navigate to the Application Administration screen.
3. From the Show drop-down list, choose System Preferences.
4. In the System Preferences list, select a system preference to edit.
5. Edit the entry in the System Preference Value column, and then step off of the record to save it.
6. Restart the Siebel Server.

Login Features

This section describes features and considerations associated with user login to Siebel applications.

A login page or a login form embedded in a Siebel application page is the means by which user credentials are collected. Figure 12 shows a login form embedded in the Siebel eService home page.



Welcome to Siebel Support!

- Browse our Knowledge Base or visit the Self Service section below to find

Track whether an order has shipped

Track the status of my service requests

Get fast, convenient support for products

Register a product and receive updates and

Figure 12. Embedded Login Form

A user is required to login, thereby identifying himself or herself as a registered user, to be allowed access to protected views in Siebel applications. Protected views are designated for explicit login. Views that are not designated for explicit login are available for anonymous browsing, if the Siebel application allows anonymous browsing.

For information about setting view properties, see *Siebel Tools Reference*.

For information about anonymous browsing, see "Anonymous Browsing" on page 189.

Siebel applications also provide other features on a login form besides user credentials collection, such as remembering a user name and password and providing forgotten password support.

Alternatively, you can configure a Siebel application to bypass the login form by providing the required user ID and password in the URL that accesses the application.

Remember My User ID and Password

A user can check the Remember My User ID and Password check box when logging into a Siebel application. By doing so, the user can access the same Siebel application through other browser instances without having to log in again. The functionality is available only during the current Web session.

Remember My User ID and Password uses the auto-login cookie that the Siebel Web Engine provides when a session is started. This functionality requires that cookies are enabled.

For information about cookies and session management, see "Cookies and Session Management" on page 215.

Forgot Your Password?

Forgot Your Password? allows a user who has forgotten the login password to get a new password. A seed workflow process provides interactive questions by which the user identifies himself or herself.

For information about Forgot Your Password?, see "Forgot Your Password?" on page 250.

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. When a password is about to expire, the directory provides warning messages to the Siebel application to display when the user logs in. The warning indicates 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 will not be allowed to log into the application to change the password.

For example, to enable password expiration on a Sun ONE Directory Server, use the Directory Server's console or command line interface to set the passwordExp and passwordMaxAge attributes. For more information, see the documentation provided with your external LDAP directory.

To enable password expiration on ADSI, set the Maximum Password Age password policy (corresponding to the maxPwdAge domain attribute), and make sure that Password Never Expires is not set for each user. The Password Last Set (pwdLastSet) user attribute stores when the user's password was last changed. For more information, see the documentation provided with ADSI.

When you configure password expiration for LDAP or ADSI, you also add the `PasswordExpireWarnDays` parameter to the [LDAP] or [ADSI] section of the Siebel application configuration file, as appropriate. Set the value to the number of days you want to provide the warning message before the password expires.

Password expiration is supported for Security Adapter and Web Single Sign-On authentication, but not for database authentication.

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: By using URL login, user passwords are transmitted in clear text over the network.

The easiest, but least secure, option for a form of Web SSO to Siebel applications is to make explicit login requests to a Siebel customer or partner application from navigational entry points to the application. This option works best if the number of navigational entry points to the Siebel application is small, if you are not concerned about users knowing their Siebel username and password, and if you are not deploying a full Web SSO infrastructure.

Following is a sample showing the URL syntax:

```
http://yourhost/eservice/
start.swe?SWECmd=ExecuteLogin&SWEUserName=HKIM&SWEPassword=HKIM
```

NOTE: The parameter names in the URL are case-sensitive.

You can create a single URL that contains a path to a predefined view in addition to a user’s login credentials. You must use a SWEAC 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 GUEST are represented using escape characters: %48%4B%49%4D. (Note that such character strings are not secure.)

```
http://siebel.com/echannel/
start.swe?SWECmd=ExecuteLogin&SWEUserName=%47%55%45%53%54&SWEPas
sword=%47%55%45%53%54&SWEAC="SWECmd=InvokeMethod,SWEMethod=Drill
down,SWEView=Service+Request+List+View+(SCW),SWEApplet=Service+R
equest+List+Applet+(SCW),SWEField=SR+Number,SWERowIds=SWERowId0%
3d1-15P"
```

NOTE: You must use commas instead of ampersands (&) as delimiters between arguments in an SWEAC expression.

Cookies and Session Management

Four cookies are generated dynamically by the Siebel Web Engine when a Web session starts:

- Session cookie
- Auto-login cookie
- SSO for Siebel Reports cookie
- Mode cookie

The Siebel Web Engine generates cookies as a default feature. No configuration is required. You should not modify any of the cookies.

If a browser does not support cookies or a user disables cookies, Siebel Web Engine manages the session in cookieless mode. You can configure Siebel Web Engine to function in cookieless mode for all sessions.

For more information about cookies used by Siebel applications and about modifying how your Web browser supports cookies, refer to *Siebel Web Client Administration Guide*.

Session Cookie

The session cookie manages the Web session for a Siebel Web application.

- **Cookie name.** _sn
- **Applications.** Siebel employee, partner, and customer applications
- **Format.** `Session ID`
- **Consequence if cookies are disabled.** Siebel Web Engine supports cookieless sessions. The session ID becomes part of the URL.

  For information about cookieless sessions, see "Cookieless Sessions" on page 216.

Auto-Login Cookie

The auto-login cookie underlies the Remember My User ID and Password feature. Encrypted user information is collected to a desktop cookie. If the user subsequently accesses the application URL through another browser window, the user information is provided to the application so the user does not have to log in again.

- **Cookie name.** start.swe.
- **Applications.** Siebel employee, partner, and customer applications.
- **Format.** `start.swe=`*`encrypted_user_information`*.
- **Consequence if cookies are disabled.** Auto-login does not work in cookieless mode.

Cookieless Sessions

A Web session can be managed without cookies. In cookieless mode, the session management information for each page is included in its URL.

Functionality provided by the auto-login cookie is not available in cookieless mode.

A cookieless session is invoked when the browser does not send back a session cookie to the Siebel Web Engine. This event can be caused by cookies being disabled by the user or by a browser that does not support cookies.

You may want a Siebel application to function in cookieless mode for all sessions for reasons such as security requirements that do not permit cookies. You can set a Siebel application to function in cookieless mode by setting the `URLSession` parameter to `TRUE` for the application in the eapps.cfg file.

For information about additional eapps.cfg parameters that relate to cookies, such as `AutomaticSession` or `CookieSession`, refer to *Siebel Server Installation Guide*.

For information about setting parameter values in the eapps.cfg file, see "Editing Parameter Values in the eapps.cfg File" on page 148.

User Administration 9

This section provides information about registering and administering users of Siebel employee, partner, and customer applications.

Overview of User Registration

A user who is not a registered Siebel application user has no authenticated access to the database. Depending on the Siebel application, unregistered users have various levels of access. Minimally, the user can access a login page. By default or by your configuration, unregistered users may have access to some or all of the views of a particular Siebel application.

You typically grant registered users more access to data and features than you grant unregistered users. A user can be registered for some or for all of your Siebel applications. You can grant different registered users different levels of access to the database and features.

Typically, a user is registered when the following tasks are performed.

- Create a user record in the Siebel Database.
- Provide the means for the user to be authenticated at login.

Depending on the Siebel application, a user can be registered in one or more of the following ways:

- **Self-registration.** The user can self-register at the Web site.
- **Internal registration.** An administrator at your host company can register users.
- **External registration.** A delegated administrator (a user at a customer or partner company) can register users.

If you implement an external authentication system, then adding a user to the Siebel Database, whether by self-registration or by an administrator, may or may not propagate the user's login data to the external authentication system. If the login credentials do not propagate to the authentication system, then you must create the login credentials separately in the authentication system.

If you implement database authentication, then adding the user to the database with the user's user ID and password is enough to allow the user to be authenticated.

For more information about authentication and propagation of user data, see "User Authentication Overview" on page 89.

Requirements

You must complete the following implementations before you can register users:

- Install your Siebel applications.
- Setup and configure your user authentication architecture.
- Create database accounts for users as required by your authentication architecture.

For information about user authentication, see "User Authentication Overview" on page 89.

Seed Data

When you install your Siebel eBusiness Applications, you are provided seed data that is related to user registration, to authentication, and to user access to Siebel applications. The seed data includes users, responsibilities, positions, an organization, and a database login. References to the seed data appear throughout this section.

For detailed information on seed data and for procedures for viewing and editing seed data, see "Seed Data" on page 399.

Unregistered Users and Anonymous Browsing

Several Siebel applications allow anonymous browsing of views intended for public access as default functionality. Anonymous browsing typically applies to Siebel customer and partner applications, not employee applications. However, you can configure any Siebel application to either allow or disallow anonymous browsing.

Unregistered users gain access to application views and the database through the anonymous user. The anonymous user is a record in the Siebel Database that also performs functions during user authentication and user self-registration. If you implement an external authentication system, the anonymous user has a corresponding record in the user directory.

The anonymous user is required even if your applications do not allow access by unregistered users. When the Application Object Manager first starts up, it uses the anonymous user account to connect to the database and retrieve information (such as a license key) before presenting the login page. For information about the anonymous user's role in user authentication, see "User Authentication Overview" on page 89.

Implementing Anonymous Browsing

To make views accessible to unregistered users, you must perform the following tasks:

- Modify the anonymous user record.
- Set configuration parameters.
- Modify views.

For Siebel applications for which anonymous browsing is implemented by default, you should confirm that these tasks are done.

Modifying the Anonymous User Record

The anonymous user is a record in the Siebel Database and, if you implement external user authentication, a corresponding record in the external directory of users. The anonymous user is a component in user authentication, anonymous browsing, and self-registration. For applications that allow anonymous browsing, the anonymous user provides visibility of the pages for which you allow anonymous browsing.

You should set up your user authentication architecture before configuring an application for user access. Therefore, the anonymous user should already exist in your Siebel Database and in your directory.

The responsibility that is assigned to a user record in the database contains a list of views to which the user has access. You must confirm that the anonymous user that you use for your Siebel application includes an appropriate responsibility so that unregistered users can see the views you intend them to see.

If you choose to use a seed anonymous user in your authentication setup, then you should verify that its seed responsibility includes the views you want to provide for anonymous browsing. For example, if you use the GUESTCST seed user for a Siebel customer application, then you should verify that its responsibility, Web Anonymous User, includes the required views. If the responsibility does not include your required views, then you can do one of the following:

- Create one or more additional responsibilities that include missing views, and then add the responsibilities to the existing seed responsibility in the anonymous user's multi-value Responsibility field. The user has access to all the views in all the assigned responsibilities.
- Copy the seed responsibility record, add missing views to the copy, and replace the responsibility in the anonymous user record with the modified responsibility.

NOTE: You cannot directly modify a seed responsibility.

For information about creating a responsibility or adding views to a responsibility, see "Access Control" on page 287.

For information about assigning a responsibility to a user, see "Internal Administration of Users" on page 262.

For information about seed data, see "Seed Data" on page 399.

Setting Configuration Parameters

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 197.

- **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 Application Object Manager to allow a Siebel application home page to display to a user who has not logged in. Similarly, this anonymous user supplies a login so the user can see other pages for which you allow anonymous browsing.

- **AnonPassword.** This parameter from the eapps.cfg file is the authenticated password that is paired with `AnonUserName`.

  For information about setting parameter values in the eapps.cfg file, see "Parameters in the eapps.cfg File" on page 192.

Modifying Views to Allow or Disallow Anonymous Browsing

Even when a view is included in the responsibility for the anonymous user, the view is not accessible to unregistered users if the view is designated for "explicit login." A view that is designated for explicit login requires the viewer to be a registered user who has been authenticated.

The following procedure is intended to present the main steps in a Siebel Tools task. For detailed information about modifying view properties in Siebel Tools, see *Siebel Tools Reference*.

To set or remove the explicit login requirement for a view

1. Open Siebel Tools.

2. In Object Explorer, select the View object type.

   The Views list appears.

3. Select a view.
4. Choose Tools > Lock Project.
5. Check the Explicit Login field to set the view for explicit login or remove the check to allow anonymous browsing.
6. Recompile the Siebel repository file, and unlock the project.

Overview of Self-Registration

Several Siebel applications allow users to self-register as a default functionality.

This section observes the following principles about self-registration functionality that is provided by default with your Siebel applications:

- Self-registration applies to Siebel customer and partner applications.
- Self-registration can be implemented only in Siebel applications whose clients use standard interactively. It cannot be implemented for Siebel employee applications or for any other Siebel application that uses the high interactively client.
- You can configure any eligible Siebel application to either allow or disallow self-registration.
- You implement security adapter authentication with Siebel applications for which you allow self-registration.

To implement self-registration for applications that use Web SSO user authentication, you are responsible for configuring the self-registration functionality at the Web site level and for synchronizing the user data with the Siebel Database. Configuration guidelines are not provided in Siebel applications documentation. Self-registration is not feasible when you implement database authentication.

NOTE: If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel applications, including user self-registration. For information about user authentication, see "User Authentication Overview" on page 89.

Self-registration functionality for Siebel customer and partner applications is included in your Siebel eBusiness Applications installation.

End User Experience for Self-Registration

The self-registration experience for end users varies, depending on the application. Some application-specific capabilities are:

- **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.
- **Siebel eAuction.** A user self-registers to be an auction bidder or to be an auction lister.
- **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.

For more information on registering partners and partner users for Siebel Partner Portal, see *Siebel Partner Relationship Management Administration Guide*.

For more information on registering users for Siebel eAuction, see *Siebel eAuction Guide*.

To self-register

1 The user clicks New User on a Siebel application page.

The Personal Information form appears.

2 The user completes the form using the following guidelines, and then clicks Next.

Field	Entry
First Name	Required.
Last Name	Required.
User ID	Required. This contiguous character string is stored as the user ID in the User record. Depending on how you configure authentication, the user may or may not use this entry as a login name.
Password	Optional (required for some authentication implementations). Required. The user uses this password to log in. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. The user enters this password to log in. It must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form.
Verify Password	Required.
Challenge Question	Required. The user enters a phrase for which there is an "answer." If the user clicks Forgot Your Password?, this phrase is displayed, and the user must enter the correct answer to receive a new password.
Answer to Challenge Question	Required. The user provides a word or phrase that is considered the correct answer to the challenge question.

The Contact Information form appears. The fields on this form vary depending on the application.

3 The user completes the Contact Information form, and then clicks a button at the bottom of the form to continue. The names and number of buttons vary depending on the application.

4 If the application is Siebel Partner Portal, Siebel eAuction, 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 eAuction or eSales completes forms to provide some or all of the following: payment information, and address information, wireless access information, or a request to become a seller.

5 On the Usage Terms form, the user must agree to the terms of the license agreement to be registered.

The Registration Confirmation message appears.

Implementing Self-Registration

Several components comprise the self-registration feature:

- Siebel seed workflow processes provide a sequence of interactive forms to the user for collecting the new user's data. These processes also validate data and write much of the data to the new User record in the Siebel Database.
- Some fields in the new User record in the database are populated automatically from fields in the anonymous user record.
- A new record is created in the user directory. The security adapter authenticates the user against this record. Fields are populated automatically from the data the user enters to the forms.

You must perform one or more of the following tasks to implement self-registration:

- (Optional) Modify the anonymous user record.
- Set configuration parameters.
- Activate workflow processes for self-registration.

Modifying the Anonymous User Record

The anonymous user is a record in the Siebel Database and a corresponding record in the user directory. The anonymous user is a component in user authentication, anonymous browsing, and self-registration.

Your user authentication architecture should be set up before configuring an application for user access. Therefore, the anonymous user should already exist in your Siebel Database and in your user directory.

For information about user authentication, see "User Authentication Overview" on page 89.

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. "Seed Data" on page 399 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). When a user self-registers through Siebel eAuction, data is also written to eAuction-specific business components.

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 with a responsibility you create.
- Copy the seed responsibility record, add missing views to the copy, and replace the New Responsibility with the modified responsibility.

NOTE: You cannot directly modify a seed responsibility.

For information about creating a responsibility or adding views to a responsibility, see "Access Control" on page 287.

For information about seed data, see "Seed Data" on page 218.

Setting Configuration Parameters

The user directory can be administered through Siebel applications if you implement security adapter authentication. Changes such as adding a user or changing a password by an internal administrator, a delegated administrator, or when a user self-registers are propagated to the user directory.

You must set the following parameter for user data, including user name and password, to propagate to the user directory when users self-register:

- **SecExternalUserAdministration.** Set this Siebel system preference to FALSE to allow administration of the user directory through the Siebel Web Client.

For information about the functions of Siebel system preferences and the procedure for setting them, see "System Preferences" on page 209.

NOTE: If you do not configure your security adapter authentication architecture to allow administration through the Siebel Web Client as described here, then you must manually create a record in the user directory whenever a new user of this application is created in the Siebel Database.

Activating Workflow Processes

When you install your Siebel eBusiness Applications, you are provided the following workflow processes that control self-registration for several Siebel applications. These workflow processes together present a sequence of forms for the user to complete, perform data validation, and invoke database operations.

- **User Registration Initial Process.** For purposes of self-registration, this process is invoked when a user clicks New User on the login form or clicks Check Out during the buying process in Siebel eSales. This process is also invoked by clicking Forgot Your Password? on the login form. The process branches to one of the following subprocesses:
  - User Registration Process
  - User Registration Forgot Password Process
- **User Registration Process.** This is the main self-registration process. It updates the database, including:
  - Creating a new User record
  - Checking for a duplicate User record
  - Updating the existing User record with new information if a duplicate record is found
- **User Registration SubProcess.** This process is a subprocess to User Registration Process. It performs all of the information gathering and validation. The validated information includes:
  - A duplicate user ID does not exist in the database.

- The Password and Verify Password entries are identical.
- All required fields are completed.

To view workflow processes

1. From a Siebel employee application such as Siebel Call Center, navigate to the Business Process Administration screen.
2. From the Show drop-down menu, choose Workflow Processes.

   The Workflow Processes list appears.
3. In the Workflow Processes list, scroll or query to find and select a workflow process.
4. Do one of the following, depending on the information about the process you want to see:
   - Click the Process Designer view tab to see a flowchart of the process. You can double-click a step to see its properties.
   - Click the Process Properties view tab to see any property in this workflow process.

The registration workflow processes branch at various stages depending on these cases:

- The application is Siebel Partner Portal.
- The application is Siebel eAuction. One individual branch requires either eAuction or eSales.
- The application is neither of the above. This is the default case, and it includes Siebel eService, eCustomer, eTraining, eEvents, and eMarketing.

Table 17 lists the views specified in the workflow processes that provide interactive forms during self-registration.

Table 17. Self-Registration Workflow Views

View Name	Applications that Use this View	Description
User Registration Initial Form View User Registration Password Error Msg View User Registration Missing Info Msg View User Registration Login Error Msg View User Registration Legal Confirmation View User Registration Confirmation Msg View User Registration Declined View	All	These views, common to all applications that use the User Registration Process, comprise two groups: ■ Personal Information form and messages resulting from flawed entries or a duplicate user ID with an existing user record. ■ Usage Terms form and messages resulting from accepting or declining to agree.
User Registration Contact Information View	Default	This view is the Contact Information form used by default.
User Registration Contact Information View (SCW) User Registration Company Information - Company View (SCW) User Registration Company Information - Individual View (SCW)	PRM Partner Portal	These views collect contact information and information about the user's company.
User Registration Contact Information View (eSales)	eSales eAuction	This view is the Contact Information form used by eSales and eAuction.
eAuction User Registration - Address eAuction User Registration - Payment eAuction User Registration - Seller eAuction User Registration - Wireless Device eAuction User Registration - Wireless Preferences	eAuction	These views collect various specialized data for eAuction.

For the self-registration workflow processes to be invoked, they must have the Active status.

To activate a workflow process

1. From a Siebel employee application such as Siebel Call Center, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. In the Workflow Processes list, scroll or query to find and select a workflow process.

   If the process has status Active, then you do not have to activate it.

3. To activate a workflow process, it must have the In Progress status. If the status is not In Progress, click Revise.

   A workflow process of the same name, but with an incremental version number, is created and selected. The original workflow process is given an Outdated status.

4. Click Activate.

   The new process is given the Active status. It is the only version of this process that has the Active status, and it is the version that is invoked.

5. Click Save.

Modifying Self-Registration Views and 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. However, you should understand the way that data is collected by the User Registration business component and written to the database before you do any modifications.

The views used in the self-registration workflow processes are based on the User Registration business component. The User Registration 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 business component allows collecting data into virtual fields. For most applications that use the self-registration workflow processes, no data is written to the database until all stages of collecting user data are completed. This process provides the following benefits:

- If the self-registration process is terminated before completion, there is no need to perform the time-consuming process of undoing a new, partially written record in the database. This process requires searching several tables.
- User record duplication can be prevented before a record is written.

Siebel Partner Portal differs in how it commits data during the self-registration process. It collects data into virtual fields during the initial part of the process. No data is committed to the database during this part of the sequence. During the latter part of the sequence, in which partner-specific data is collected, the registration process makes use of multi-value groups (MVGs) to populate some fields, such as Industries.

User data is written to the database in this phase, prior to completion of the entire process, because MVGs must be associated with a user's actual record in the database. At this point the record cannot be undone.

Replacing the License Agreement Text

You can replace the default license agreement that appears to the self-registering user in the User Registration Legal Confirmation View.

The DotCom Applet License Base 1 Column Web template includes the Web template file with the name DotCom Applet Form Base 1 Column which is the file of name dCCAppletLicenseBase1Col.swt. The license agreement is contained in the dCCAppletLicenseBase1Col.swt file, following the phrasing <!--This is where we include the html license agreement-->. You can replace the license agreement text.

For information about working with Web templates, see *Siebel Tools Reference*.

Revising a Workflow Process

The self-registration workflow processes for your business scenario may require that you do revisions to the seed self-registration workflow processes, such as:

- Replace or insert a view
- Insert or delete a step
- Modify a step

You cannot directly modify a seed workflow process, such as any of the self-registration processes. Instead, you must create a copy of the process, and then revise the copy.

By convention, to avoid renaming processes, you can use the Revise button to make a copy of the same name, but with an incremented version number. All other processes of the same name are assigned Outdated status, so that the new version can be the only active version. This convention is recommended for revising any workflow process, not just seed processes.

To create a revised copy of a workflow process

1. In a Siebel employee application, such as Siebel Call Center, log in as an administrator, and then from the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. Select a workflow process.

   NOTE: You cannot revise a workflow process whose status is In Progress. This status indicates that the workflow process is being modified.

3. Click Revise.

   A new workflow process record appears with the same name as the original process and with a version number one greater than the highest existing version number for that process.

For information about working with 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 *Siebel Tools Reference*.

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.

You can change whether a field is required, for a view used in the self-registration workflow processes.

Use the Business Process Administration screen to determine the view that includes a self-registration field.

To determine the view in which a self-registration field appears

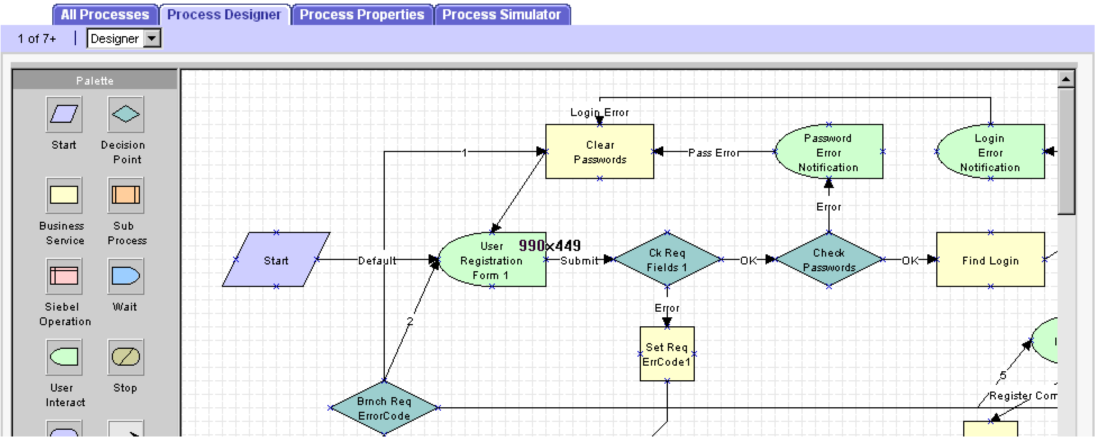
1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center, and then choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. Query or scroll to select User Registration SubProcess. All data collection from the self-registering user is performed in this workflow process.

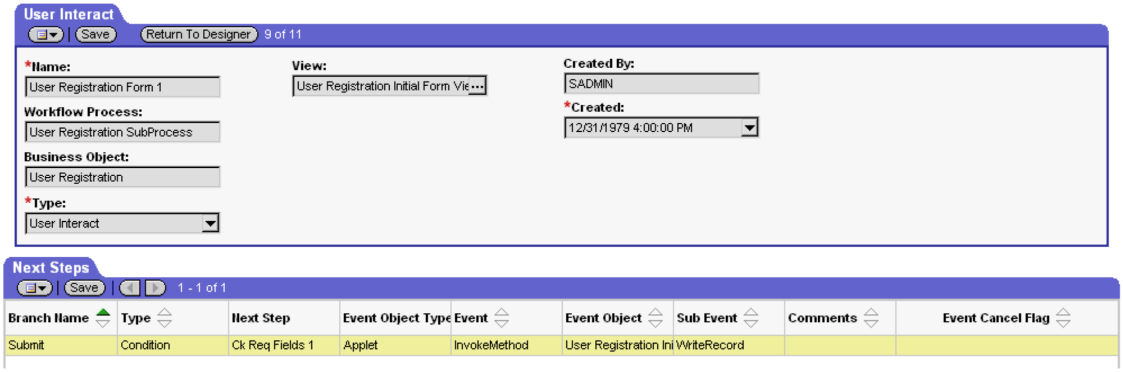
3. Click the Process Designer view tab.

   As shown below, the Process Designer appears, showing the current workflow process and the palette that you can use to add steps to your workflows.



4 Double-click the User Interact step, such as User Registration Form 1, which represents the stage of the self-registration process in which you want to require that a user complete a field.

As shown below, the User Interact form appears, listing properties of this step.



*Name: User Registration Form 1

Workflow Process: User Registration SubProcess

Business Object: User Registration

*Type: User Interact

View: User Registration Initial Form Vie

Created By: SADMIN

*Created: 12/31/1979 4:00:00 PM

Branch Name	Type	Next Step	Event Object Type	Event	Event Object	Sub Event	Comments	Event Cancel Flag
Submit	Condition	Ck Req Fields 1	Applet	InvokeMethod	User Registration Ini	WriteRecord		

5 Record the entry in the View field.

The CSSSWEFrameUserRegistration 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 *Siebel Tools Reference*.

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 the view you recorded in "To determine the view in which a self-registration field appears" on page 236.

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 new record using the following guidelines, and then save the record by stepping off of the record.

Field	**Entry**
Name	Required. Enter `Show Required` and a sequence number one greater than the 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, 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 238, or delete the record.

Adding or Deleting Fields in an Existing View

All the data collected in views used in the seed self-registration workflow processes are written to fields in the User Registration business component. The following process describes how data is collected in the user interface and written to a user's record in the database:

- The user enters data, such as the user's height, into a text box on a form.
- The form field is mapped to a virtual field, for example Vheight, in the User Registration business component, so the data is written directly to that field.

- Self-registration data collection is done in the User Registration SubProcess. A process property, for example Vheight, of the User Registration SubProcess maps to the Vheight virtual field. Therefore, the virtual field value populates the process property.

  The virtual field and the process property can have the same name, and this naming convention makes it easier to track the mapping.

- The Vheight process property serves as output from the User Registration SubProcess to its parent, the User Registration process. The posting happens only after the User Registration SubProcess is complete, that is, when the user has successfully completed the registration forms.

  The output is mapped to a process property in the User Registration Process, such as, again, Vheight by convention. Process properties from different workflow processes, even parent and child, can have the same name.

- The process property in User Registration Process, Vheight in this example, maps to a field in the database, such as Height. Because the User Registration business component writes to the same database tables as the User business component, each field is actually stored as part of a user record.

  Except for some Siebel partner-specific data, no data from the User Registration Process properties is written to the User Registration business component fields until the self-registration process is complete.

To add or delete fields in a view used in a self-registration workflow process, you must perform tasks in the following stages:

- Siebel Tools tasks

- Siebel Workflow (Business Process Designer) tasks

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 list the major tasks required. For detailed information about modifying views and applets, see *Siebel Tools Reference*.

To add a field to a view used in a self-registration workflow process

1. Open Siebel Tools.
2. Lock the User Registration project.
3. Determine the business component and the underlying database table on which the new field is based.
4. If the new field is not based on an existing database table column, define a column on an extension table of the appropriate table.
5. Create a new field, based on the new or existing table column, in the appropriate business component.
6. If the new field is based on the User Registration business component, create a new virtual field in the business component.

   a. Create the field in the business component as you would any field. The naming convention used for existing virtual fields is to prefix the name with a “V”, such as “Vheight.”

   b. Set the new field’s Calculated property to `TRUE`.

7. Configure the appropriate applet to expose the new virtual field.
8. If necessary, configure the new field so that a self-registering user is required to complete it.

   For information about configuring a required field, see “Redefining Required Fields” on page 235.

9. Recompile the Siebel repository file, and unlock the User Registration project.

To remove a field from the self-registration user interface, you do not have to delete the field from the applet in which it appears. Instead, configure the applet so that the field is not exposed. For detailed information about configuring applets, see *Siebel Tools Reference*.

Workflow Tasks for Adding or Deleting Fields

Adding a field to a view that is used in a self-registration workflow process requires that you associate process properties with the field so that information gathered through the workflow process is written to the appropriate field in the business component.

The following procedure is intended to list the major tasks you must perform in the Business Process Administration screen to allow an added field in the user interface to correctly populate a field in the User Registration business component. It applies the principle of writing user data to the database only after the registration process is complete. It assumes you have already completed the tasks described in "Siebel Tools Tasks for Adding or Deleting Fields" on page 240.

For detailed information about workflow administration, see *Siebel Business Process Designer Administration Guide*.

To modify self-registration workflow processes to handle an added field

1. In a Siebel employee application, such as Siebel Call Center, log in as an administrator, and then from the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. Query or scroll to select User Registration SubProcess.
3. Create a revised copy of User Registration SubProcess, as described in "To create a revised copy of a workflow process" on page 235. Edit this revised copy.
4. Click the Process Properties view tab.

   The Process Properties list appears.

5. In the Process Properties list, create a new record. Enter only the fields listed below by using the guidelines provided.

Field	Guideline
Name	Enter a process property name, such as `Vheight`. This can be a name of your choice.
Data Type	Pick the appropriate data type.
Business Component	Enter `User Registration`.
Virtual Field	Enter the name of the virtual field, such as `Vheight`, in the User Registration business component that corresponds to the new field.

6 Click the All Processes view tab, and then select User Registration Process.

7 Click the Process Designer view tab.

The Process Designer appears, showing the current workflow process. One of its subprocess steps is Registration SubProcess.

8 Double-click the Registration SubProcess step.

The Sub Process form appears.

9 In the Sub Process Output Arguments list, create a new record. Enter only the fields listed below by using the guidelines provided.

Field	**Guideline**
Property Name	Enter a process property name, such as `Vheight`, for the User Registration Process. This can be a name of your choice.
Type	Enter `Output Argument`.
Sub Process Output	Enter the process property, such as `Vheight`, of the User Registration SubProcess that you created in Step 5 on page 242.

10 Click the Process Designer view tab.

The Process Designer flowchart appears.

11 Perform the following steps for each Siebel Operation step that inserts a new user, for example Insert New User and Insert New eAuction User:

a Double-click the step’s flowchart icon.

The Siebel Operation form appears.

b In the Fields list, create a new record. Enter only the fields listed below by using the guidelines provided.

Field	Guideline
Field Name	Enter the new field name, such as `height`, that you created in the User Registration business component. This should be the field that writes to the database, not the corresponding virtual field.
Type	Enter `Process Property`.
Property Name	Enter the process property, such as `Vheight`, of the User Registration Process that you created in Step 9 on page 243. This process property is the end of the chain that passes the virtual field value collected by the user interface.

12 In the Siebel Operation form, click Return to Designer.

The Process Designer flowchart and palette appear.

13 Click the All Processes view tab.

The Workflow Processes list appears. The revised process is still selected.

14 On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

NOTE: If you remove a field from the self-registration user interface, you must also make sure that the User Registration SubProcess workflow process does not require the user to complete the field and that the field is not used to check for duplicate User records.

For information about removing the requirement that the user must complete a field, see "Workflow Tasks for Adding or Deleting Fields" on page 241.

For information about removing a field from the deduplication check, see "Modifying the Fields Used to Determine a Duplicate User" on page 247.

Changing the Physical Appearance of a View or Applet

For information about changing the physical appearance of a view or applet, such as moving fields or changing colors, see *Siebel Tools Reference*.

Creating a New View

You create a new view for insertion into one of the self-registration workflow processes in the same way you create a view for any other purpose.

You can include new applets in a view that you create that you include in a self-registration workflow process. You create the new applet and include it in the view in the same way as you would for any other purpose, with the following consideration:

- If you base the applet on the User Registration business component, apply the CSSSWEFrameUserRegistration class to the applet. This allows you to define fields for which an asterisk displays in the user interface. By convention, fields that you require users to complete during the self-registration process have an asterisk.

For information about working with views, see *Siebel Tools Reference*.

Modifying User Deduplication

When a user self-registers, the User Registration Process workflow process attempts to determine whether the user already exists in the database. User deduplication is a default feature, and it is configurable.

As default functionality, if all of the following non-null field values entered by the self-registering user match those for an existing user, the users are considered to be the same person.

- First name
- Last name
- Email address

If the self-registering user is a match of an existing user, the existing User record is updated instead of a new User record being written. If the value in a field of the existing User record differs from the self-registering user's non-null entry, the existing field is updated with the new data. All other existing field values are left unchanged.

In the User Registration SubProcess workflow process, the duplication comparison is done by the ValidateContact method in the User Registration business service. Depending on the application, the comparison is done in one of two business service steps.

- Check User Key
- Check User Key PRM

Modifying Updated Fields

You can specify that certain fields in the User Registration business component are not updated when a duplicate user is determined.

The following procedure is intended to list the major steps you must do. For detailed information about doing any step, see *Siebel Tools Reference*.

To exclude a field from being updated when a duplicate user is determined

1. Open Siebel Tools.
2. Lock the User Registration project.
3. Determine the field in the User Registration business component that you want to exclude from updating.
   a. In the Object Explorer, expand Business Component, and then expand its Field child.
   b. In the Business Component list, query or scroll to select the User Registration business component.
4. In the Object Explorer, expand Business Service, and then click on its Business Service User Properties child.

   The Business Services list applet and the Business Service User Properties child list applet appear.

5. In the Business Services list applet, select User Registration.
6. In the Business Service User Properties, create a new record.
7. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter `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 User Registration business component field name that you noted in Step 3 on page 246.

8. Commit the record.
9. Recompile the Siebel repository file and unlock the User Registration project.

Modifying the Fields Used to Determine a Duplicate User

You can change the fields that are used to determine whether a duplicate user exists.

The following procedure is intended to list the major steps you must perform to modify the fields used to determine a duplicate user. For detailed information about performing any step, see *Siebel Tools Reference*.

To modify the fields used to determine a duplicate user

1. Open Siebel Tools.
2. Lock the User Registration project.
3. Determine the fields in the User Registration business component that you want to add or delete from the duplication comparison.
   a. In the Object Explorer, expand Business Component, and then expand its Field child.
   b. In the Business Component list, query or scroll to select the User Registration business component.

4. In the Object Explorer, expand Business Service, and then click on its Business Service User Properties child.

   The Business Services list applet and the Business Service User Properties child list applet appear.

5. In the Business Services list applet, select User Registration.

6. Delete a field from the duplication comparison.

   a. In the Business Service User Properties list applet, select the record with name `App User Key: Default` *`number`* 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 by using the guidelines provided, and then commit the record.

Field	Guideline
Name	Enter `App User Key: Default` *`number`* or `App User Key:` *`number`*, where application is the name of the Siebel application, and *`number`* is the next number in the sequence for this particular user property. For example, enter `App User Key: Default 2` to add a field for Siebel eService or `App User Key: Siebel eChannel 4` to add a field for Siebel PRM Partner Portal. This entry is case-sensitive.
Value	Enter the name of the User Registration business component field that you want to add to the duplication check.

8. Recompile the Siebel repository file and unlock the User Registration project.

Deactivating the Duplication Check

You can deactivate the duplication check.

The following procedure is intended to show the main steps in deactivating the duplication check. For more detailed information on working with workflow processes, see *Siebel Business Process Designer Administration Guide*.

To deactivate the self-registration deduplication check

1. From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. Query or scroll to select User Registration SubProcess.

3. Create a revised copy of User Registration SubProcess as described in "To create a revised copy of a workflow process" on page 235. Edit this revised copy.

4. Click the Process Designer view tab.

   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.

   - **Check User Key eChannel**. This step applies if your application is Siebel Partner Portal or another Siebel partner application.

   - **Check User Key.** This step applies if your application is not a Siebel partner application.

6. Delete the bypassed process step, which should now not be the source or destination of any connector.

7. Click the All Processes view tab.

   The Workflow Processes list appears. The revised process is still selected.

8. On the Workflow Processes list, click Activate.

   The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

Forgot Your Password?

If a user who has previously self-registered on a Siebel customer 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 functionality of Siebel customer and partner applications, but it is available only if you implement ADSI or LDAP security adapter authentication or database authentication. If you want to implement a similar functionality in a Web SSO authentication environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, and in your security adapter. Configuration guidelines are not provided in Siebel applications documentation.

The User Experience

A user who has previously self-registered can retrieve a new password. The user can change the new password in the Profile view on a future login.

To retrieve a new password

1. In the login dialog box, the user clicks Forgot Your Password?.

   The User Information form appears.

2. The user completes all fields of the form, and then clicks Submit.

   - The database comparisons done with the Last Name field and First Name field entries are case-sensitive.
   - The Work Phone # entry numbers are compared with the database. The comparison disregards any separators.

   If a matching record is found, the Challenge Question form appears.

3 The user enters the answer to the challenge question.

If the challenge question is answered correctly, the New Password Confirmation dialog box appears with a new password for the user.

4 Click Continue.

Forgot Your Password? Architecture

Forgot Your Password? is implemented in the User Registration Forgot Password Process workflow process. This process is a subprocess in User Registration Initial Process.

As described in "To retrieve a new password" on page 250, to receive a new system-generated password, the user must provide identification data that is compared with database user records. If all four fields return a case-sensitive match with an existing record, the user must answer the challenge question associated with that record. The challenge answer must also return a case-sensitive match.

When a user enters values to the comparison fields in the user interface, the values are written to virtual fields in the User Registration business component. The User Registration business component is based on the same tables as the User business component. The virtual field values are not written to the database, but are compared with field values in those underlying tables. The user entries in the following fields in the user interface are compared with field values in the tables indicated:

- The Last Name, First Name, Email, and Work Phone # fields are compared with S_CONTACT field values.
- The Challenge Answer field is compared with an S_USER field value.

The User Registration Forgot Password Process workflow process uses the following views:

- User Registration Forget Pwd Info View
- User Registration Forget Pwd Challenge Ques View
- User Registration Forget Pwd Confirm View
- User Registration Forget Pwd Challenge Answer Error View

- User Registration Forget Pwd Decline View

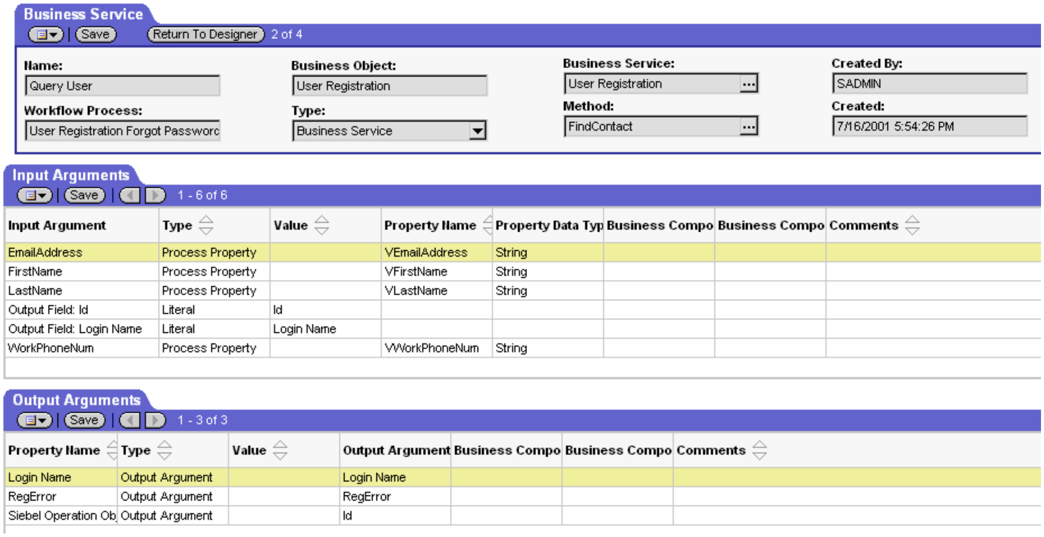
Modifying Forgot Your Password?

You can modify the User Registration Forgot Password Process workflow process in the following ways:

- Make a comparison of null fields as well as fields for which the user has provided a value.
- Request different identification data from the user.

In the User Registration Forgot Password Process workflow process, the Query User step invokes the FindContact method of the User Registration business service. This method queries the database for user records whose data matches the identification data provided by the user. If the query returns a unique record, the user can then prove he or she owns the record by answering the challenge question.

The parameters of the Query User step in User Registration Forgot Password Process are shown in Figure 13. These parameters include input arguments (such as EmailAddress, FirstName, and LastName) and output arguments (such as LoginName and RegError).



Name: Query User	Business Object: User Registration	Business Service: User Registration	Created By: SADMIN
Workflow Process: User Registration Forgot Passworc	Type: Business Service	Method: FindContact	Created: 7/16/2001 5:54:26 PM

Input Argument	Type	Value	Property Name	Property Data Typ	Business Compo	Business Compo	Comments
EmailAddress	Process Property		VEmailAddress	String			
FirstName	Process Property		VFirstName	String			
LastName	Process Property		VLastName	String			
Output Field: Id	Literal	Id					
Output Field: Login Name	Literal	Login Name					
WorkPhoneNum	Process Property		VWorkPhoneNum	String			

Property Name	Type	Value	Output Argument	Business Compo	Business Compo	Comments
Login Name	Output Argument		Login Name			
RegError	Output Argument		RegError			
Siebel Operation Ob	Output Argument		Id			

Figure 13. Query User Step Parameters

Table 18 describes the functions of parameters in the Query User step.

Table 18. Query User Step Parameters

List	Records	Comments About Values
Input Arguments	EmailAddress FirstName LastName WorkPhoneNum	The Input Argument field values are the field names in the User Registration business component that the FindContact business service queries for a match. The comparison is made with the process property values given in the Property Name field. These process properties collect the entries made by the user.
	Output Field: Id Output Field: Login Name	As given by the Input Argument field values, the FindContact method is requested to return the Id and Login Name field values for each user record whose field values match the entries by the user. A temporary table of values is defined in which the rows are the records returned and the columns are given by the Value field values. One row of the temporary table contains the ID for a returned record in the Id column and the record's Login Name in the Login Name column.
Output Arguments	Login Name Siebel Operation Object Id RegError	■ 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 Make a Comparison of Null Fields

By default, if a user completes fewer than all four fields on the User Information form, only the fields that a user completes are used in the query to find a unique matching record in the database. For example, if the user enters first and last name only, the query does not do any comparisons on the Email or Work Phone # fields.

You can specify that the FindContact method in the User Registration business service must also check that fields left empty by the user are confirmed to be NULL in the database record to conclude that a record is a match. To do so, you must add the QueryAllFields input argument with a value of Y to the Query User process step. By default, the value of this input argument is N, so it is not listed.

To specify that null fields be used in the query for a matching user record

1. From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. Query or scroll to select User Registration Forgot Password Process.

3. Create a revised copy of User Registration Forgot Password Process as described in "To create a revised copy of a workflow process" on page 235. Edit this revised copy.

4. Click the Process Designer view tab.

   The Process Designer appears, showing the current workflow process. One of its subprocess steps is Query User.

5. Drill down on the Query User step.

   A page that includes the Input Arguments list appears, as shown in Figure 13 on page 253.

6. In the Input Arguments list, click the menu button and choose New Record.

   A new input argument record appears.

7. Complete the new record, and then click Save. Enter only the following fields and values.

Field	Value
Input Argument	QueryAllFields
Type	Literal
Value	Y

8 In the Business Service form, click Return to Designer.

The Process Designer appears, showing the current workflow process.

9 Click the All Processes view tab.

The Workflow Processes list appears. The revised process is still selected.

10 On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

Modifying Workflow Process to Request Different Identification Data

The data requested from the user in the User Information form is compared with data in existing user records to locate a unique database record. If you want to compare different data than those compared in the seed User Registration Forgot Password Process workflow process, then you must do the following tasks:

- Modify the user interface.
- Modify User Registration Forgot Password Process.

Modifying the User Interface

To add or delete a field in the User Information form, you must use Siebel Tools to modify its underlying applet. The following procedure is intended to list the major steps you must perform to add or delete a field in the User Information form. For detailed information about performing any step, see *Siebel Tools Reference*.

To add or delete a field in the User Information form

1 Open Siebel Tools.

2 Lock the User Registration project.

3 If you are adding a field, determine both the virtual field in the User Registration business component that corresponds to the field you want to add and the actual field that is used to write to the underlying table. For example, if you want to add a comparison to City, note the VCity virtual field and the City field.

a In the Object Explorer, expand Business Component, and then expand its Field child.

b In the Business Component list, select the User Registration business component.

4 Configure the User Registration Forget Pwd Info Applet to expose or hide the field.

a In the Object Explorer, expand Applet, and then expand its Control child.

b In the Applets list, query or scroll to select User Registration Forget Pwd Info Applet.

c If you want to hide a field, select its record in the Controls list and check its Inactive field.

d If you want to add a field, add a new record in the Controls list, and then click Save. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter a name for this field, such as City
Caption	Enter the caption you want for this field in the user interface, such as City
Field	Enter the virtual field for this field that you determined in Step 3 on page 256, such as VCity
HTML Display Mode	Delete the default value, so the field is empty
HTML Row Sensitive	Check
HTML Type	Pick Text
Sort	Check
Text Alignment	Pick an alignment
Visible	Check
Visible - Language Override	Enter Y

5. Configure the appropriate applet Web template for the User Registration Forget Pwd Info Applet to display or hide the field.

   For information about adding or deleting a control in an applet Web template, see *Siebel Tools Reference*.

6. Recompile the Siebel repository file and unlock the User Registration project.

To remove a field from the self-registration user interface, you do not have to delete the field from the applet in which it appears. Instead, configure the applet so that the field is not exposed.

For detailed information about configuring applets, see *Siebel Tools Reference*.

If you are adding a field to the comparison, there must be a process property present to collect that field entry from the user and write it to a virtual field of the User Registration business component. If a process property is not present for collecting the entry, you must create a new process property.

To create a process property to collect and write data to a virtual field

1. From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

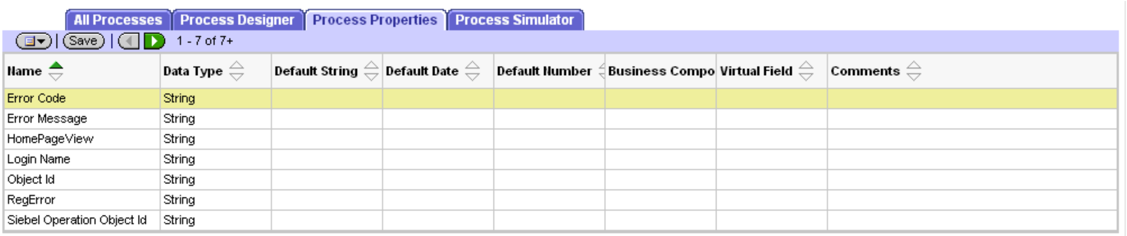
2. Query or scroll to select User Registration Forgot Password Process.

3. Create a revised copy of User Registration Forgot Password Process as described in "To create a revised copy of a workflow process" on page 235. Edit this revised copy.

   A copy of the record appears with an incremented version number and a status of In Progress.

4 Click the Process Properties view tab.

The following figure shows a list of process properties for a workflow process.



Name	Data Type	Default String	Default Date	Default Number	Business Compo	Virtual Field	Comments
Error Code	String						
Error Message	String						
HomePageView	String						
Login Name	String						
Object Id	String						
RegError	String						
Siebel Operation Object Id	String						

5 In the Process Properties list, click the menu button and choose New Record.

A new record appears.

6 Complete the new record, and then click Save. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	By convention, provide the same name as the virtual field in the User Registration business component to which this process property writes. This is the virtual field that you noted in Step 3 of “To add or delete a field in the User Information form” on page 256, such as `VCity`.
Data Type	Enter `String`.
Business Component	Pick `User Registration`.
Virtual Field	Enter the virtual field name that you noted in Step 3 of “To add or delete a field in the User Information form” on page 256, such as `VCity`.

7 Click the All Processes view tab.

The Workflow Processes list appears. User Registration Forgot Password Process is still selected.

8 Do one of the following:

- If you are pausing the process of adding a field to the FindContact method input arguments, click Activate on the Workflow Processes list.

  The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

- If you are continuing the process of adding a field to the FindContact method input arguments, leave the status as In Progress and exit this procedure.

In the Query User step of User Registration Forgot Password Process, you specify the input fields to the FindContact method in the User Registration business service that are used to find a matching user record. You must modify this step to add or delete an input field.

To add or delete input fields provided to the FindContact method

1. From the application-level menu, choose View > Site Map > Business Process Administration > Workflow Processes.

   The Workflow Processes list appears.

2. Query or scroll to select User Registration Forgot Password Process.

3. If you are not already working on a version of the process with an In Progress status, create a revised copy of User Registration Forgot Password Process as described in "To create a revised copy of a workflow process" on page 235. Edit this revised copy.

   A copy of the record appears with an incremented version number and a status of In Progress.

4. Click the Process Designer view tab.

   The Process Designer appears, showing the current workflow process. One of its subprocess steps is Query User.

5. Drill down on the Query User step.

   A page that includes the Input Arguments list appears, as shown in Figure 13 on page 253.

6 If you are deleting an input field, select the appropriate record in the Input Arguments, and then click the menu button and choose Delete Record.

The record is deleted.

7 If you are adding an input field, click the menu button in the Input Arguments list and choose New Record.

A new input argument record appears.

8 Complete the new record, and then click Save. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Input Argument	Enter the name of the field in the User Registration business component that you noted in Step 3 of "To add or delete a field in the User Information form" on page 256, 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 virtual field in the User Registration business component that you noted in Step 3 of "To add or delete a field in the User Information form" on page 256, such as `VCity`. The process property has the same name as the virtual field, by convention.
Property Data Type	This field automatically populates with the data type of the process property.

9 In the Business Service form, click Return to Designer.

The Process Designer flowchart and palette appear.

10 Click the All Processes view tab.

The Workflow Processes list appears. User Registration Forgot Password Process is still selected.

11 On the Workflow Processes list, click Activate.

The status of the revised workflow process changes to Activated, and the status of other versions by the same name change to Outdated.

Internal Administration of Users

You can provide an employee, a customer, or a partner user with access to one or more Siebel applications by performing the following tasks:

- Provide the user with a method to be authenticated and thus to connect to a database account.
- An internal administrator uses a Siebel employee application, such as Siebel Call Center, to add the user to the Siebel Database.

User Authentication Requirements

Your authentication architecture should be implemented before adding new users. As an ongoing task, you must arrange that each new user can be authenticated at login. The setup and administration that you must perform for each new user depends on the authentication architecture you implement.

For information about user authentication concepts mentioned in the following descriptions, see "User Authentication Overview" on page 89.

- **Database authentication.** You must enter the user name for a valid database account in the user's user ID field. You must provide the user ID and the password to the database account to the new user.

- **Security adapter authentication.** You can configure your application so that when you create or modify user records in the Siebel Database, the security adapter propagates those changes to the user directory. Therefore, no separate administration of the user directory is required.

  NOTE: For a Siebel security adapter to propagate new or modified user data from the Siebel Database to the user directory, the administrator who modifies the database records must log in through the same security adapter.

  If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel applications. This includes internal administration of users that provides propagation of a user's Siebel user ID to the directory.

  For information about user authentication, see "User Authentication Overview" on page 89.

  CAUTION: Make sure the application user has write privileges to the user directory. If you do not implement an application user, make sure all users who create or modify users have write privileges to the directory.

- **Web SSO authentication.** You must maintain corresponding records in the external authentication system, the user directory, and the Siebel Database for each user. If you want to implement a mechanism for synchronizing these records, you must develop the utility independently, and implement it at the Web site level. Configuration guidelines are not provided in Siebel applications documentation. You must provide authentication credentials to the new user.

Adding a User to the Siebel Database

A user of a Siebel application is a record in the User business component. The S_PARTY, S_CONTACT, and S_USER tables in the Siebel Database underlie the User business component. Each user is assigned a responsibility, a user ID, and, depending on the authentication architecture being used, a password.

An employee or a partner user is a user who has a position within a division, either internal or external, in the Siebel Database. Other users, such as those who use customer applications such as Siebel eSales, do not have a position or a division. The S_EMP_PER table underlies the Employee business component, to which employees and partner users belong, in addition to the tables that underlie the User business component.

For more information about the functions of responsibilities, positions, divisions, and organizations, see "Access Control" on page 287.

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.

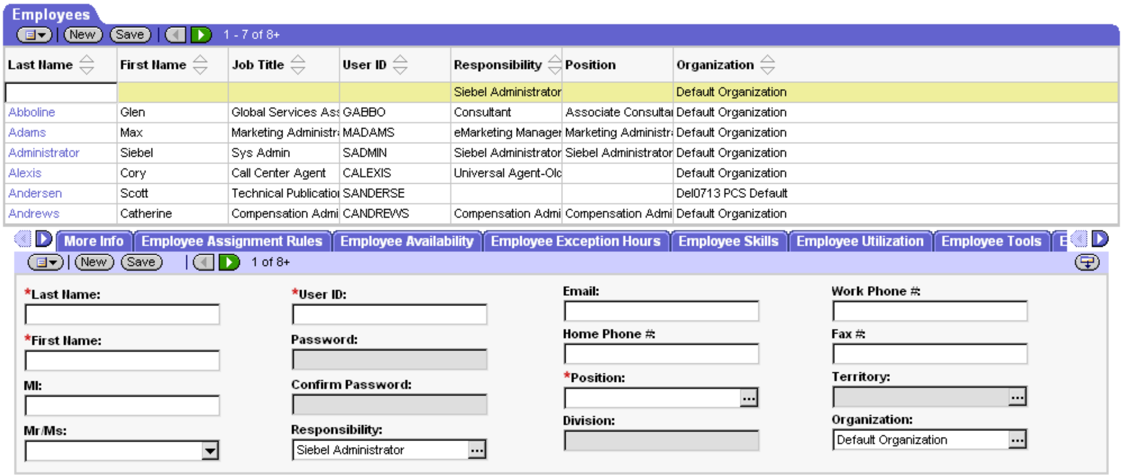
To add a new employee

1. Log in as an administrator to a employee application, such as Siebel Call Center, and then choose View > Site Map > User Administration > Employees.

   The Employees list appears.

2 Click the menu button, and then choose New Record.

As shown below, a new record appears in the Employees list and a corresponding form appears under the More Info view tab.



Last Name	First Name	Job Title	User ID	Responsibility	Position	Organization
				Siebel Administrator		Default Organization
Abboline	Glen	Global Services As:	GABBO	Consultant	Associate Consultai	Default Organization
Adams	Max	Marketing Administr:	MADAMS	eMarketing Manager	Marketing Administr:	Default Organization
Administrator	Siebel	Sys Admin	SADMIN	Siebel Administrator	Siebel Administrator	Default Organization
Alexis	Cory	Call Center Agent	CALEXIS	Universal Agent-Olc		Default Organization
Andersen	Scott	Technical Publicatioi	SANDERSE			Del0713 PCS Default
Andrews	Catherine	Compensation Admi	CANDREWS	Compensation Admi	Compensation Admi	Default Organization

*Last Name:

*First Name:

MI:

Mr/Ms:

*User ID:

Password:

Confirm Password:

Responsibility: Siebel Administrator

Email:

Home Phone #:

*Position:

Division:

Work Phone #:

Fax #:

Territory:

Organization: Default Organization

3 In the More Info form, click the show more button.

Additional fields appear in the More Info form, including the New Responsibility field.

4 Complete the form. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.
User ID	Required. This field must be unique for each user. Depending on your authentication architecture, the user may or may not log in with this identifier. If you implement database authentication, this field must be the login name for a database account.

Field	Guideline
Password	Optional (required for some authentication implementations). ■ This field is editable only if you implement database or security adapter authentication. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. The password is propagated to the user directory. The user uses this password to log in. ■ This field is not editable if you implement Web SSO authentication. For Web SSO, you maintain the user's login password independently in the external authentication system. For information about user authentication architectures, see "User Authentication Overview" on page 89.
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" on page 272.
New Responsibility	If the administrator who creates this user has a value in his or her New Responsibility field, then that responsibility is assigned to this field by default. For information about the New Responsibility field, see "New Responsibility Field" on page 272.
Position	Required. To be an employee, a user must have a position. If you assign multiple positions, the position you specify as Primary is the position the user assumes when he or she logs in.
Division	This field is populated automatically with the division to which the Primary position belongs.

Field	Guideline
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.
Organization	This field value is inherited from the user who creates this user, but the field is editable. Users whose positions are in this organization have access to this employee record. For information about organization access control, see "About Access Control Mechanisms" on page 309.

5. Click Save.

Completing Employee Setup

You can set up employees either before or after you assign them a responsibility. For more information about completing employee setup, refer to the initial setup section of *Applications Administration Guide*.

Also refer to *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 View > Site Map > User Administration > Employees.

   The Employees view appears.

2. In the Employees list, select the employee you want to deactivate.
3. In the More Info view tab, delete all records from the Responsibility field.

4. Change the user ID slightly, to indicate that the employee is no longer current.

   You may want to establish a convention for renaming user IDs when you deactivate employees. One possible convention is to append some text such as “expired” to the user ID. For example, you might change CARD to CARD-expired. That way you can continue to see the person’s name associated with previous activity in history records.

5. Remove the employee’s access to the database.

   If you implemented database user authentication, you should remove the user’s database account. If you implemented external authentication, then delete the user from the directory from which the user’s database credentials are retrieved.

   NOTE: In the case of external authentication, if the external user repository is shared by many applications—as in the case of an LDAP directory or Microsoft Active Directory—do not delete the user from the directory. In such a case, make sure that the user's database access user name and password are different from that user’s directory user name and password. Otherwise the user would be able to access the database directly using some database connection tools.

Adding a New Partner User

A partner user is typically an employee in a partner company or a consultant to your company.

A partner user must have a position in a partner organization to be associated with that organization or to belong to position-based teams, such as opportunity or account teams.

You can assign a position to a new partner user from the following sources:

- Positions that you create internally and associate with the delegated administrator’s partner organization
- Positions created by delegated administrators in the partner organization

You can register and administer partner users in the Partner Administration screen in Siebel Partner Manager or another Siebel employee application for which you have licensed this screen.

For information about using the Partner Administration screen, see *Siebel Partner Relationship Management Administration Guide*.

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 eTraining. They are called customer or contact users to distinguish them from employee and partner users.

Contacts, such as contacts at a customer account, can exist in the database without having login capability. You create such contacts as Persons in the User Administration screen. The procedure in this section applies to contact users to whom you are providing a login to the Siebel Database.

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.

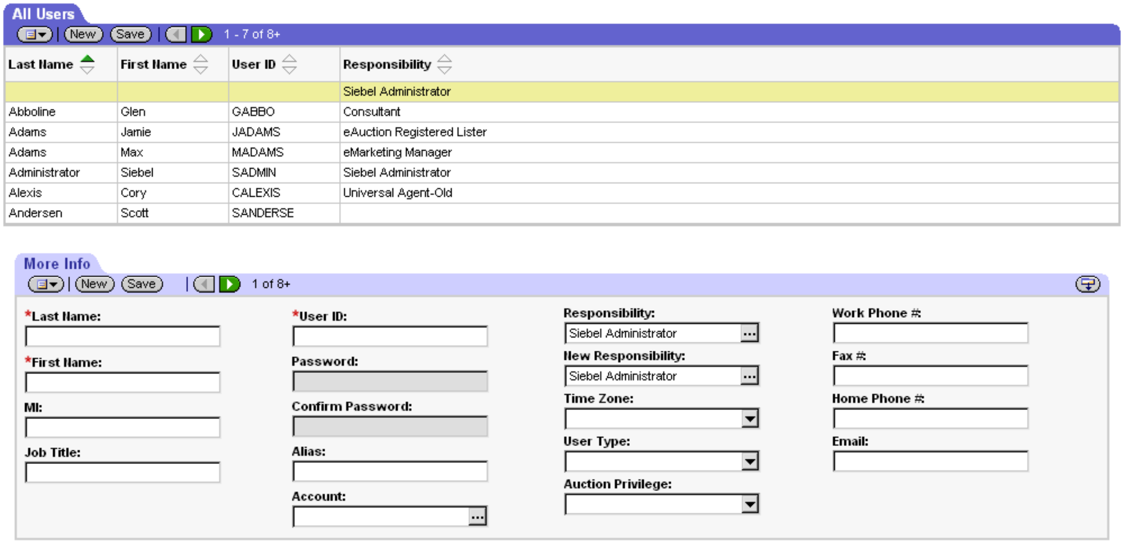
To add a new contact user

1. Log in as an administrator to a Siebel employee application, and then choose View > Site Map > User Administration > Users.

   The All Users list appears.

2 Click the menu button, and then choose New Record.

As shown below, a new record appears in the All Users list and a corresponding form appears under the More Info view tab.



Last Name	First Name	User ID	Responsibility
			Siebel Administrator
Abboline	Glen	GABBO	Consultant
Adams	Jamie	JADAMS	eAuction Registered Lister
Adams	Max	MADAMS	eMarketing Manager
Administrator	Siebel	SADMIN	Siebel Administrator
Alexis	Cory	CALEXIS	Universal Agent-Old
Andersen	Scott	SANDERSE	

*Last Name:

*First Name:

MI:

Job Title:

*User ID:

Password:

Confirm Password:

Alias:

Account:

Responsibility: Siebel Administrator

New Responsibility: Siebel Administrator

Time Zone:

User Type:

Auction Privilege:

Work Phone #:

Fax #:

Home Phone #:

Email:

3 Complete the fields in the More Info form, and then click Save. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.
User ID	Required. The user logs in with this ID.
Password	Optional (required for some authentication implementations). ■ For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database. The user uses this password to log in. ■ This field is not editable if you implement Web SSO authentication. For Web SSO, you maintain the user's login password independently in the external authentication system. For information about user authentication architectures, see "User Authentication Overview" on page 89.
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 (External) Administration of Users" on page 274.
Responsibility	Pick one or more responsibilities which include appropriate views in the customer application, such as Siebel eService, for this user. If the administrator who creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "New Responsibility Field" on page 272.
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" on page 272.
Time Zone	Choose a time zone so that times for events can be expressed in terms of this zone.

Field	Guideline
User Type	This field serves as a filter so that different applications can query for contact users only applicable to each particular application.
Auction Privilege	This field applies to users of Siebel eAuction only. For information about auction privileges, see *Siebel eAuction Guide*.
Work Phone # Fax # Home Phone #	The application interprets only the digits the user provides. Any separators are disregarded.

The new user appears in the All Users list.

You can promote an existing contact to a contact user by assigning user credentials and a responsibility to a Person record.

To promote an existing contact to a contact user

1. Log in as an administrator to a Siebel employee application, and then choose View > Site Map > User Administration > Persons.

   The All Persons list appears.

2. Select the record of the contact to promote.
3. Enter the user ID, Password, Responsibility, and New Responsibility fields as described in "To add a new contact user" on page 269.

New Responsibility Field

A user record may or may not have a value in the New Responsibility field. If a value does exist, then whenever the user creates a new user, the new user's Responsibility field is assigned the value in the creating user's New Responsibility field by default. This principle applies for any type of user (employee, partner user, contact user) creating any type of user that their application allows them to create.

A user's own New Responsibility field is populated in one of the following ways:

- The New Responsibility field value is inherited from the New Responsibility field of the user who creates this new user.
- The New Responsibility field value is manually assigned to the user.

A user's New Responsibility field can only be modified by an internal administrator.

Delegated administrators of Siebel customer and partner applications can upgrade a user's Responsibility, but they cannot edit the New Responsibility field. Therefore, your internal administrators control the default responsibility that any customer or partner user inherits from a delegated administrator. It is important to make sure delegated administrators have New Responsibility values that you intend your new customer and partner users to have, such as the seed responsibilities provided for such users.

You may or may not want to use the New Responsibility field functionality when administrators create new employee records. If there are a variety of responsibilities assigned new employees, then it may make sense to leave employee's New Responsibility field empty. If most of your new employees are assigned the same responsibility or you want to create a batch of new employee records that all have the same responsibility, then it is probably more efficient to assign a New Responsibility value to the administrator who adds the employees.

An internal administrator can modify New Responsibility values for employees, partner users, and contact users in the same administration screen.

To modify a user's New Responsibility field value

1. Log in as an administrator to a Siebel employee application, and then choose View > Site Map > User Administration > Users.

   The All Users list appears, containing all the employees, partner users, and contact users in the database.

2. In the All Users list, select the user record to modify.
3. In the More Info form, pick a new value in the New Responsibility field, and then click Save.

   The user must log out and log in for the New Responsibility value to become active.

Delegated (External) Administration of Users

A delegated administrator is a user of a Siebel customer or partner application whose responsibility provides views that allow the delegated administrator to register and administer other users of that application. Delegated administration is typically implemented in business-to-business relationships.

Delegated administration of users minimizes your internal administrative overhead by moving some of the administrative load to administrators in your customer or partner companies.

User Authentication Requirements

Delegated administration is a default functionality of most Siebel customer and partner applications, but it is available only if you implement ADSI or LDAP security adapter authentication.

Delegated administration cannot be implemented if you use database authentication. If you want to implement delegated administration in a Web SSO authentication environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, and in your security adapter. Such configuration guidelines are not provided in Siebel applications documentation.

Delegated administration requires you configure the ADSI or LDAP security adapter to propagate new and modified user data from the Siebel Database to the user directory.

If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow Siebel user IDs stored in the directory to be managed from within Siebel applications, including delegated administration of users. For information about user authentication, see "User Authentication Overview" on page 89.

CAUTION: Make sure the application user for your Siebel customer or partner application has write privileges to the user directory. If you do not implement an application user, make sure delegated administrator users of the application have write privileges to the directory. Typically, you do this by assigning write privileges to all users to avoid administering privileges for individual users.

For information about setting up ADSI and LDAP security adapter authentication, see "LDAP and ADSI Security Adapter Authentication" on page 108.

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 "Seed Data" on page 399.

Registering Users—Delegated Administration

Delegated user administration screens, navigation, and procedures vary somewhat among Siebel applications. This section describes delegated administration that is representative of customer and partner applications.

Registering Contact Users

A delegated administrator who uses a Siebel customer application must belong to at least one account. The delegated administrator registers a user in the currently active account. The new user inherits membership in that account.

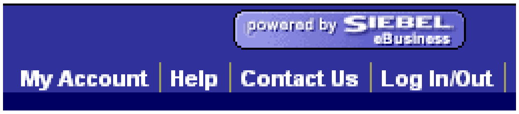
A delegated administrator must assign at least one responsibility to a new user. A delegated administrator only has responsibilities, including seed responsibilities, available for assigning to users that your host company associates with the organization with which the delegated administrator is associated. The delegated administrator is associated with the organization to which the proxy employee for the application belongs. A responsibility is associated with an organization by an administrator at your company using an employee application such as Siebel Call Center.

To register a new customer user (by a delegated administrator)

1. Log into a Siebel customer application that implements delegated administration and do one of the following to navigate to the Administration screen.

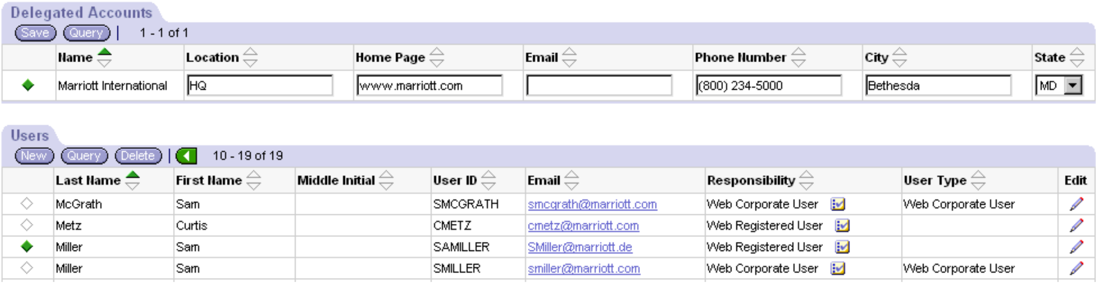
   a Click My Account, and then click User Administration under the My Company tab.

   The following figure shows the location of My Account on the Administration screen.



b Choose View > Site Map > Administration.

Lists of delegated accounts and associated users appears, as shown below. The list appearances may vary somewhat by application.



Delegated Accounts

Save Query | 1 - 1 of 1

	Name	Location	Home Page	Email	Phone Number	City	State
◆	Marriott International	HQ	www.marriott.com		(800) 234-5000	Bethesda	MD

Users

New Query Delete | 10 - 19 of 19

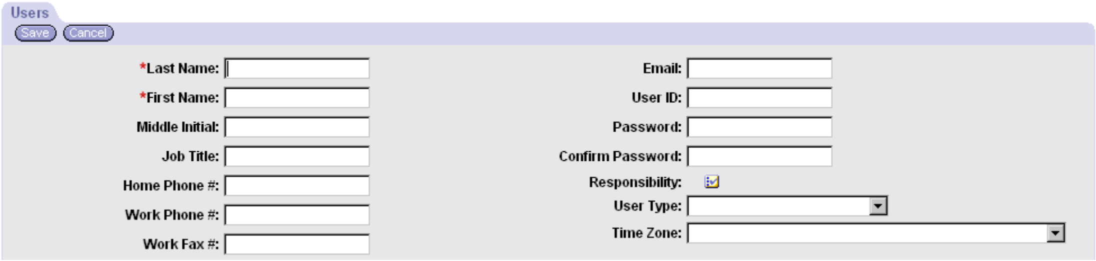
	Last Name	First Name	Middle Initial	User ID	Email	Responsibility	User Type	Edit
◇	McGrath	Sam		SMCGRATH	smcgrath@marriott.com	Web Corporate User	Web Corporate User	✎
◇	Metz	Curtis		CMETZ	cmetz@marriott.com	Web Registered User		✎
◆	Miller	Sam		SAMILLER	SMiller@marriott.de	Web Registered User		✎
◇	Miller	Sam		SMILLER	smiller@marriott.com	Web Corporate User	Web Corporate User	✎

2 In the Delegated Accounts list, select the account with which you want to associate the new user.

The users in this account appear in the Users list.

3 In the Users list, click New.

A Users form appears, similar to the one shown below for Siebel eService.



Users

Save Cancel

*Last Name:		Email:	
*First Name:		User ID:	
Middle Initial:		Password:	
Job Title:		Confirm Password:	
Home Phone #:		Responsibility:	
Work Phone #:		User Type:	
Work Fax #:		Time Zone:	

4 Complete the fields in the Users form, and then click Save. Use the following guidelines.

Field	Guideline
Last Name	Required.
First Name	Required.
User ID	Required to allow the user to log in. The security adapter identifies the user in the database with this field value. Depending on how you configure your security adapter, the user may log in with this ID.
Password	Optional (required for some authentication implementations). Required to allow the user to log in. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Responsibility	Pick one or more responsibilities, such as a seed responsibility provided for contact users. If the delegated administrator who creates this user has a value in the New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "New Responsibility Field" on page 272.
Home Phone # Work Phone # Work Fax #	The application interprets digits only in these telephone number entries. Any separators are disregarded.

The new user record appears in the Users list.

Registering Partner Users

A delegated administrator using a partner application, such as Siebel PRM 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.

A delegated administrator must do two tasks to provide a new partner user with access to the database:

- Register the partner user
- Assign a responsibility to the partner user

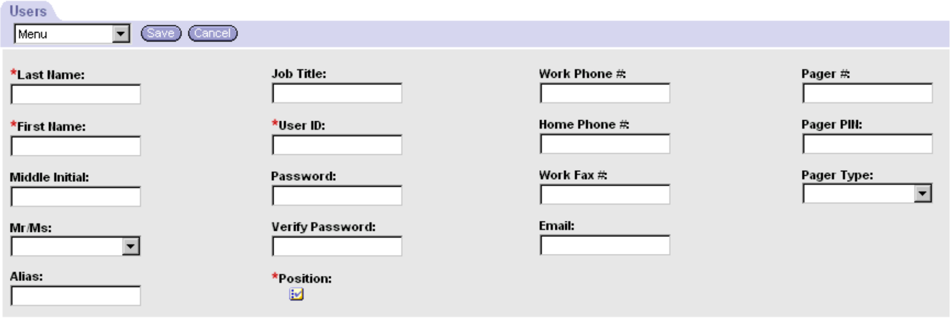
To register a new partner user (by a delegated administrator)

1. Log into a partner application, such as Siebel PRM Partner Portal, that implements delegated administration, and then choose Site Map > Administration > User Administration.

   The Users list appears, displaying partner users in the delegated administrator's organization.

2 In the Users list, click New.

A More Info form appears, similar to the one shown below.



3 Complete the fields in the Users form, and then click Save. Use the following guidelines.

Field	**Guideline**
Last Name	Required.
First Name	Required.
User ID	Required to allow the user to log in. The security adapter identifies the user in the database with this field value. Depending on how you configure your security adapter, the user may log in with this ID.
Password	Optional (required for some authentication implementations). Required to allow the user to log in. For security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.

Field	Guideline
Position	If you assign multiple positions, the position you specify as Primary is the position the partner user assumes when he or she logs in.
Work Phone # Home Phone # Fax # Pager #	The application interprets digits only in these telephone number entries. The user can enter any separators.

4 Click Save.

The new partner user record appears in the Users list.

The delegated administrator separately assigns a responsibility to a new registered partner user.

To assign a responsibility to a partner user (by a delegated administrator)

1 Log into a Siebel partner application that implements delegated administration, and then choose Site Map > Administration > User Administration.

2 Click the Responsibility view tab.

The Responsibility list appears. If the delegated administrator who creates this user has a value in their New Responsibility field, then that responsibility is assigned to this user by default.

3 On the Responsibility list, click the menu button, and then choose New Record.

The Add Responsibilities list appears.

4 Pick one or more responsibilities, and then click OK. For information about seed responsibilities provided for assigning to partner users, see “Seed Data” on page 399.

The new responsibility appears in the Responsibility list.

5 In the Users list, click Save.

For information about the New Responsibility field, see "New Responsibility Field" on page 272.

Maintaining a User Profile

Each employee, partner user, and customer user is provided a profile screen in which to update identification and authentication data. Depending on the application and on the authentication architecture you implement, a user can perform tasks such as:

- Edit personal information, such as the address or time zone.
- Edit company information in a partner application.
- Change the login password.
- Change the active position in an employee application.
- Change the primary position in a partner application.

Profile forms, names, and navigation paths differ somewhat across Siebel applications. The procedures in this section are representative of those in Siebel employee, partner, and customer applications. Procedures in individual applications may differ.

Editing Personal Information

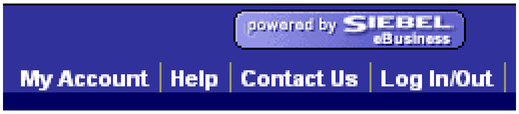
Users can change a variety of personal information in their profile form. In this context, authentication and access control data, such as passwords and positions, are not included.

To edit personal information

1 Depending on the application, the user does one of the following:

- In a Siebel customer application, the user clicks My Account, and then clicks User Profile under the My Settings tab.

  The following figure shows the location of My Account in a Siebel customer application.

  The User Profile form appears.

- In a Siebel partner application, the user clicks Profile. The Personal Profile form appears.
- In a Siebel employee application, the user chooses View > Site Map > User Profile Preferences > Profile. The Contact Information form appears.

2 The user clicks Edit to make the form fields editable, if necessary.

3 The user enters or changes data in editable fields, and then clicks Save.

Changing a Password

If you implement database or security adapter authentication, then a user can change the login password.

NOTE: If you want to implement a similar functionality in a Web SSO authentication environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, in your security adapter, and in the Siebel application views. Configuration guidelines are not provided in Siebel applications documentation.

To change a password, a user accesses the profile form as described in "Editing Personal Information" on page 282, and then completes the appropriate fields. The password-related fields are not editable if the password cannot be changed in the current authentication architecture.

Changing the Active Position

An employee or partner user of a Siebel application can have one or more positions, of which one is the primary position. When the user logs in, the user assumes the primary position only and the data access that the position determines.

An employee can assume a position other than the primary position, which immediately makes it the active position. The employee then accesses only the data determined by the new active position.

Changing the active position does not change the employee's primary position. When the employee subsequently logs in, the primary position becomes active.

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. Choose View > 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.

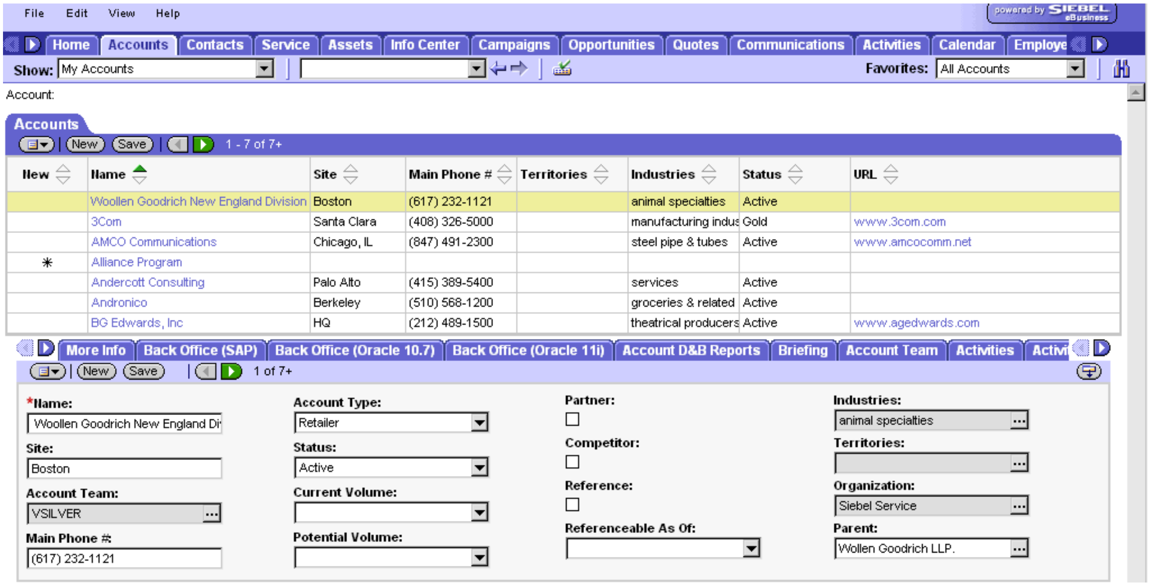
Access Control 10

Access control is the means to control visibility of data records to each individual user. This section discusses fundamental access control mechanisms you can use to control access to data and Siebel application functionality.

Access Control Overview

In Siebel application terms, a screen is a collection of views. The screen represents a broad area of functionality, such as working with accounts. To the user, a view is simply one Web page. Within a view, the user may see lists of data records or forms presenting individual records. These lists and forms are also referred to as applets in a configuration context.

In Figure 14, the My Accounts view of the Accounts screen is shown, as indicated by the selected Accounts screen tab and the display of My Accounts in the Show drop-down list. This view includes an Accounts list and an accompanying form with detail for the selected account.



Show: My Accounts

Favorites: All Accounts

New	Name	Site	Main Phone #	Territories	Industries	Status	URL
	Woollen Goodrich New England Division	Boston	(617) 232-1121		animal specialties	Active	
	3Com	Santa Clara	(408) 326-5000		manufacturing indus	Gold	www.3com.com
	AMCO Communications	Chicago, IL	(847) 491-2300		steel pipe & tubes	Active	www.amcocomm.net
✳	Alliance Program						
	Andercott Consulting	Palo Alto	(415) 389-5400		services	Active	
	Andronico	Berkeley	(510) 568-1200		groceries & related	Active	
	BG Edwards, Inc	HQ	(212) 489-1500		theatrical producers	Active	www.agedwards.com

*Name: Woollen Goodrich New England Di

Site: Boston

Account Team: VSILVER

Main Phone #: (617) 232-1121

Account Type: Retailer

Status: Active

Current Volume:

Potential Volume:

Partner: □

Competitor: □

Reference: □

Referenceable As Of:

Industries: animal specialties

Territories:

Organization: Siebel Service

Parent: Wollen Goodrich LLP.

Figure 14. My Accounts View

Basic access control consists of the following:

- **View-level access control.** You allow a user to see only the views that you want the user to see.
- **Record-level access control.** You allow a user to see only the data records that you want the user to see.

View-level access control mechanisms include filtering of available views at the application level, and through a user's responsibilities, or sets of views, assigned to the user.

For more information about implementing view-level access control, see "Implementing Basic Access Control" on page 333.

You can use several different access control mechanisms to associate data with users or groups of users. You can also create hierarchical organizations of users, and of data, to facilitate the implementation of access control.

The sections that follow examine access control further:

- **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 289.

- **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 292, "Party Data Model" on page 295, and "How Parties Relate to Each Other" on page 307.

- **Access control mechanisms.** Access control mechanisms you apply to parties and data determines what data a user sees. For details, see "About Access Control Mechanisms" on page 309.

Access Control for Data

The following groupings of data are necessary for purposes of discussing access control:

- **Master data**

    - Master data includes the following referential data: products, literature, solutions, resolution items, decision issues, auctions, events, training courses, and competitors.

    - Master data can be organized into catalogs, which are hierarchies of categories. By categorizing master data, access can be controlled at the catalog and category levels through access groups. This is the recommended strategy for controlling access to master data.

  - Master data can be associated with organizations. By associating master data with organizations, access can be controlled at the data item level. This strategy requires more administration than the access group strategy.

  NOTE: Although you can add divisions to access groups, doing so has no effect on visibility. Use organizations instead.

- **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.
- **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.
- **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 15.

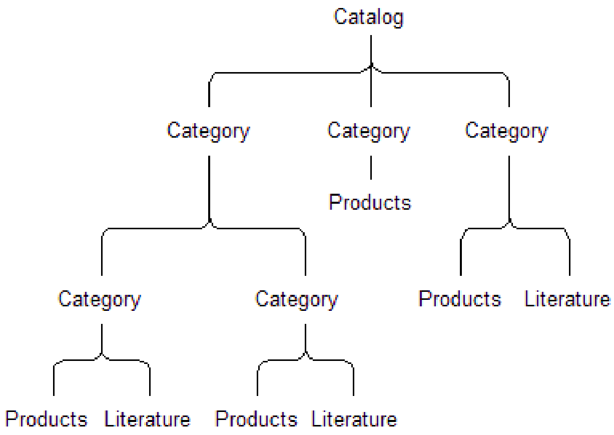


Figure 15. Catalogs and Categories

The following properties apply to catalogs and categories:

- A catalog can be thought of as the name for an entire hierarchy of categories.
- Individual data items are contained in categories.
- A category can contain one or more types of master data.
- A category can be a node in only one catalog.
- A data item can exist in one or more categories, in one or more catalogs.
- A catalog can be public or private. If it is private, some access control is applied at the catalog level. If it is public, then all users can see this catalog, but not necessarily categories within this catalog, depending on whether the categories are private or public.

Access Control for Parties

Individual people, groupings of people, and entities that represent people or groups are unified in the common notion of *parties*.

Parties are categorized into the following party types: Person, Position, Organization, Household, User List, and Access Group. Table 19 describes the qualitative differences among different parties.

Table 19. Party Types and Parties

Party Type	Party	Examples	Distinguishing Features
Person	Person (or Contact)	■ 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.
Person	User	■ 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.
Person	Employee	■ An employee at your company.	■ An Employee is a User who is associated with a position in a division within your company.
Person	Partner User	■ 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.

Table 19. Party Types and Parties

Party Type	Party	Examples	Distinguishing Features
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.
Organization	Account	■ 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.

Table 19. Party Types and Parties

Party Type	Party	Examples	Distinguishing Features
Organization	Division	■ An organizational unit within your company such as Manufacturing or Corporate.	■ A division exists for the purposes of mapping a company's physical structure into the Siebel Database and for providing a container for position hierarchies. ■ A division may have a parent division. It may also have child divisions. ■ Data cannot be associated directly with a division.
Organization	Organization	■ An organizational unit within your company, such as your European organization. ■ A partner company.	■ An organization exists for the purpose of providing a container in which positions can be associated with data. ■ An organization can be internal or it can be a partner organization. ■ A division can also be designated as an organization. ■ A division is associated with one organization: itself or an ancestor division that is also an organization.
Household	Household	■ A group of family members who reside at the same address. ■ 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.

Table 19. Party Types and Parties

Party Type	Party	Examples	Distinguishing Features
User List	User List	■ A support team made up of some internal employees and some partner users. ■ Some bidders on your online auction site who are granted access to private auctions.	■ 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.

Party Data Model

The S_PARTY table is the base table for all of the parties listed in Table 19 on page 292: 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, refer to *Siebel Tools Reference*.

In Figure 16, 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.

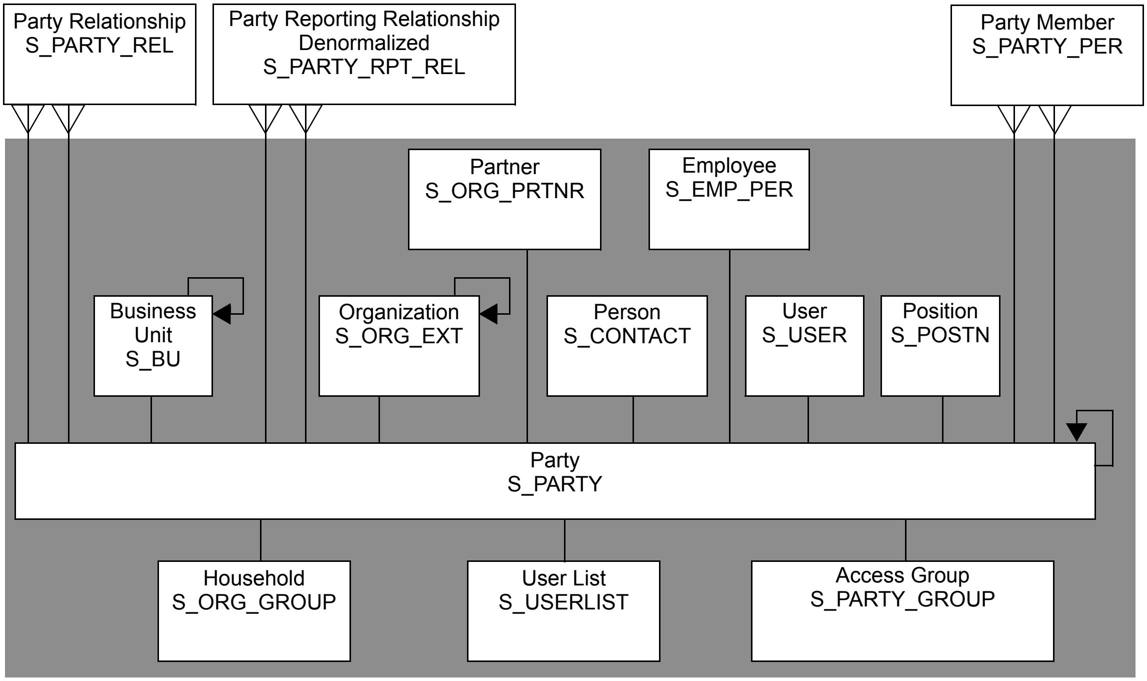


Figure 16. Party Data Model

Person (Contact) Data Model

In Figure 17, the base table and extension table (S_CONTACT) that define a Person, or Contact, are shaded in the figure. A Person is the simplest representation of an individual in the database.

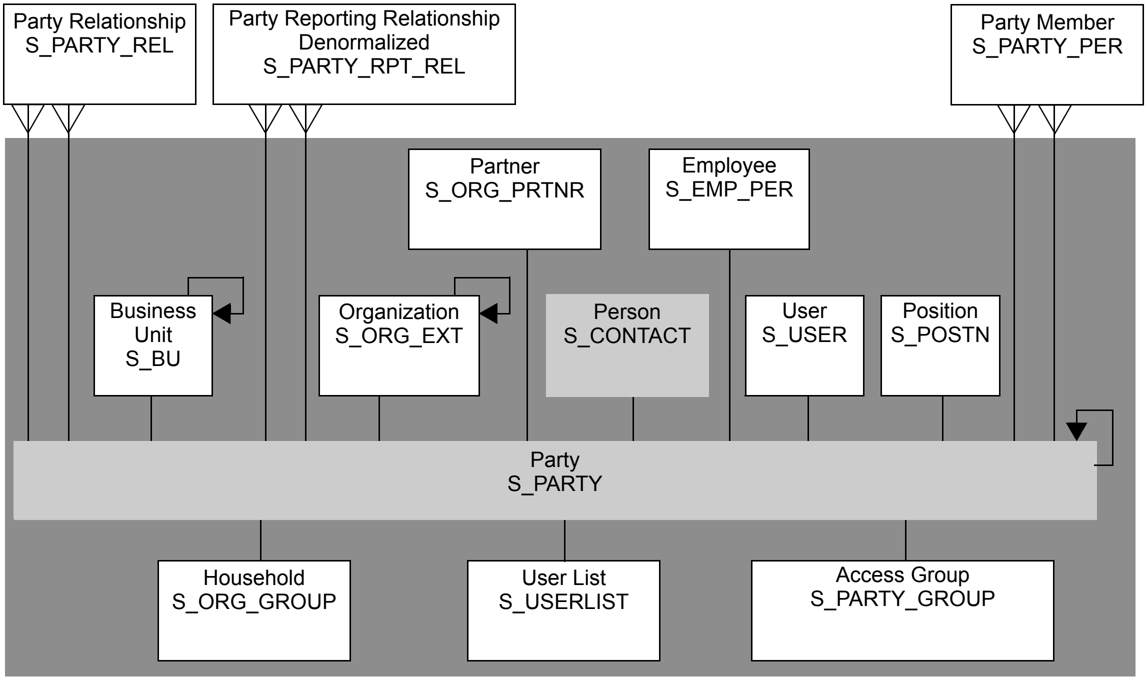


Figure 17. Person (Contact) Data Model

User Data Model

In Figure 18, the base table and extension tables (S_CONTACT and S_USER) that define a User are shaded in the figure. A User is a Person with the following added qualities:

- S_USER contains a login for this user.
- The S_PER_RESP intersection table (not shown) specifies a responsibility for this user.

- 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 User Administration screen causes the person to appear as a user in the All Users view.

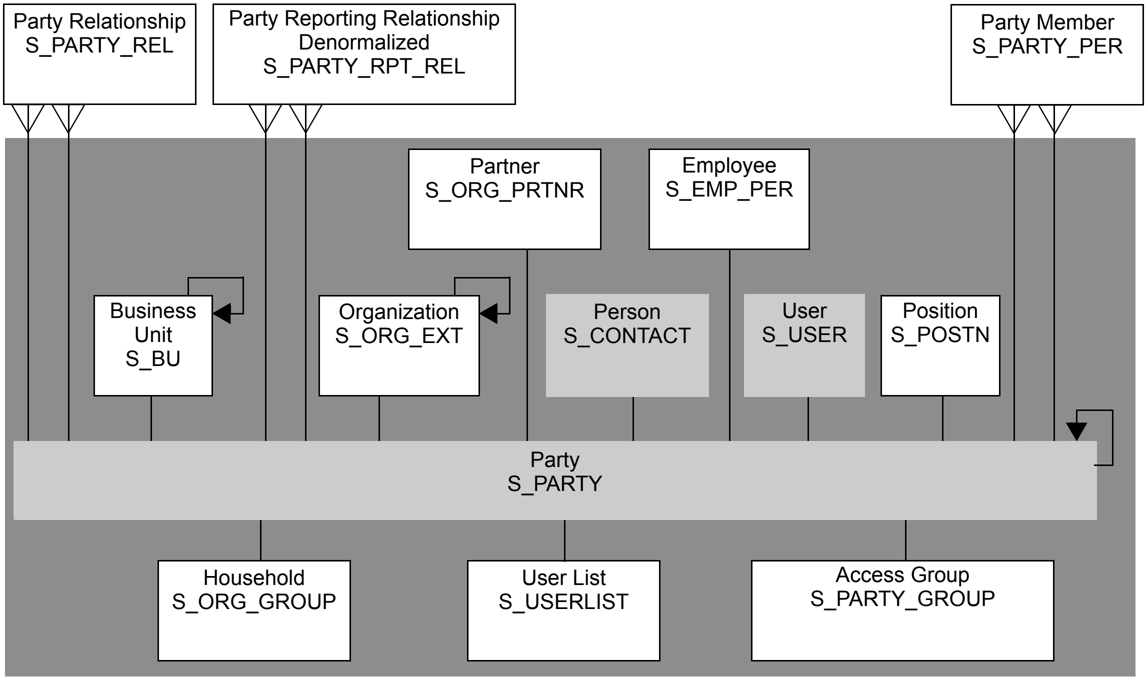


Figure 18. User Data Model

Employee Data Model

In Figure 19, the base table and extension tables (S_CONTACT, S_USER, and S_EMP_PER) that define an Employee are shaded in the figure. 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.

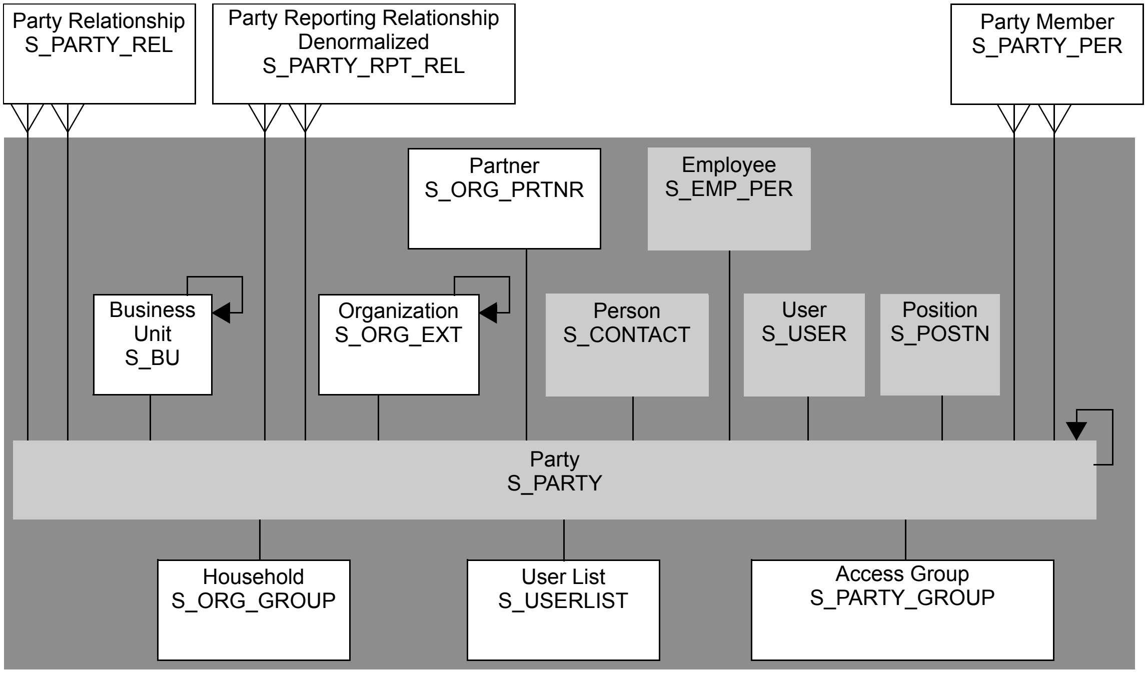


Figure 19. Employee Data Model

Position Data Model

In Figure 20, the base table and extension table (S_POSTN) that define a Position are shaded in the figure.

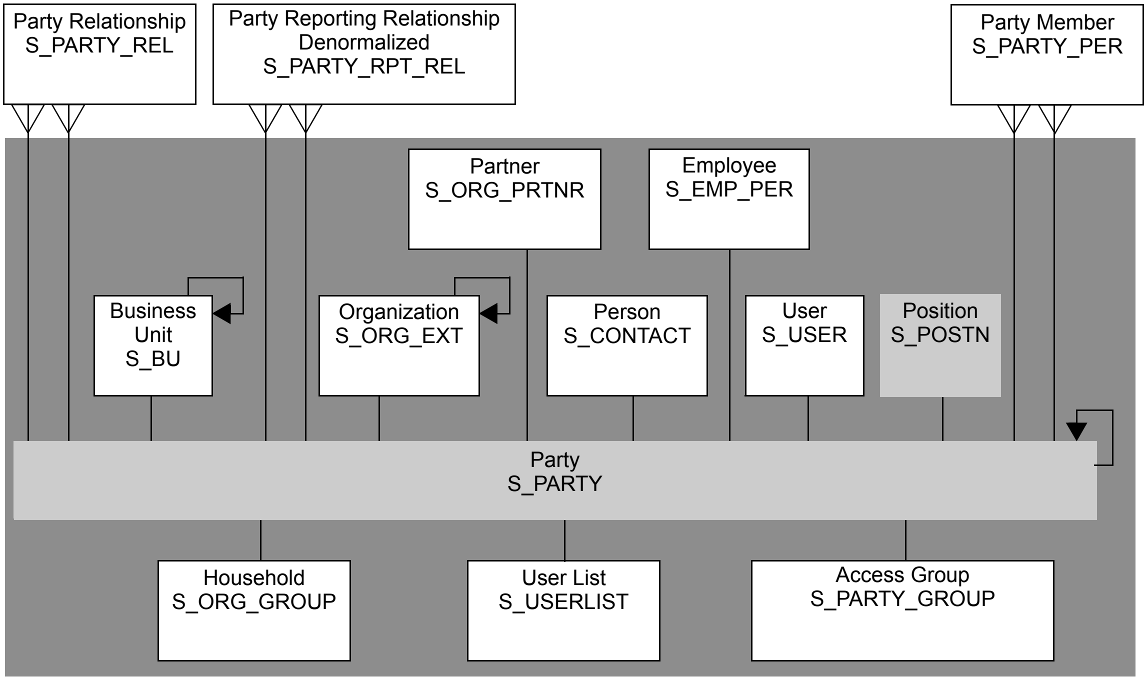


Figure 20. Position Data Model

Account Data Model

In Figure 21, the base table and extension table (S_ORG_EXT) that define an Account are shaded in the figure.

(Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.)

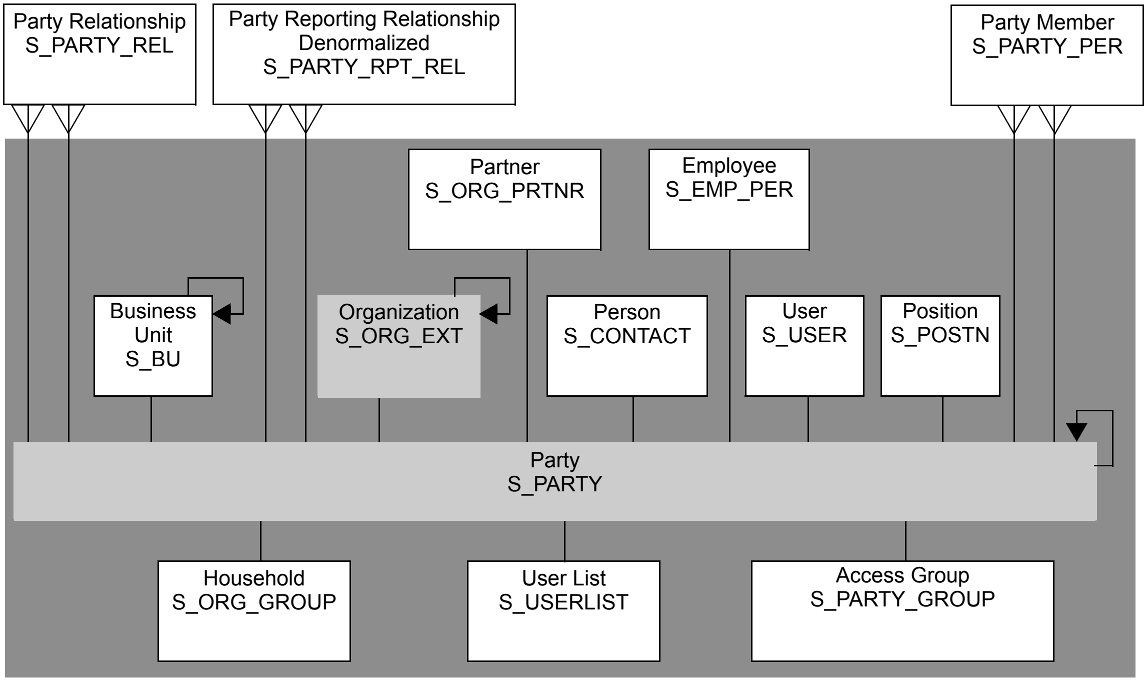


Figure 21. Account Data Model

Division Data Model

In Figure 22, the base table and extension table (S_ORG_EXT) that define a Division are shaded in the figure.

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.)

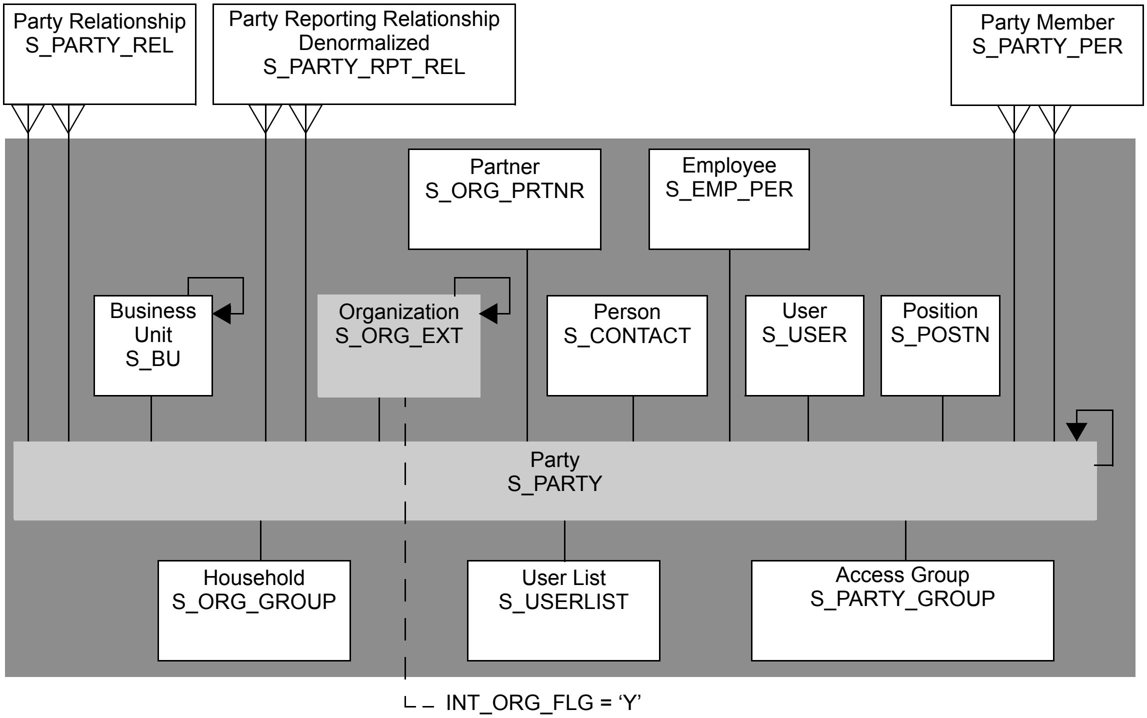


Figure 22. Division Data Model

Organization Data Model

In Figure 23, the base table and extension tables (S_ORG_EXT and S_BU) that define an Organization are shaded in the figure.

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.)

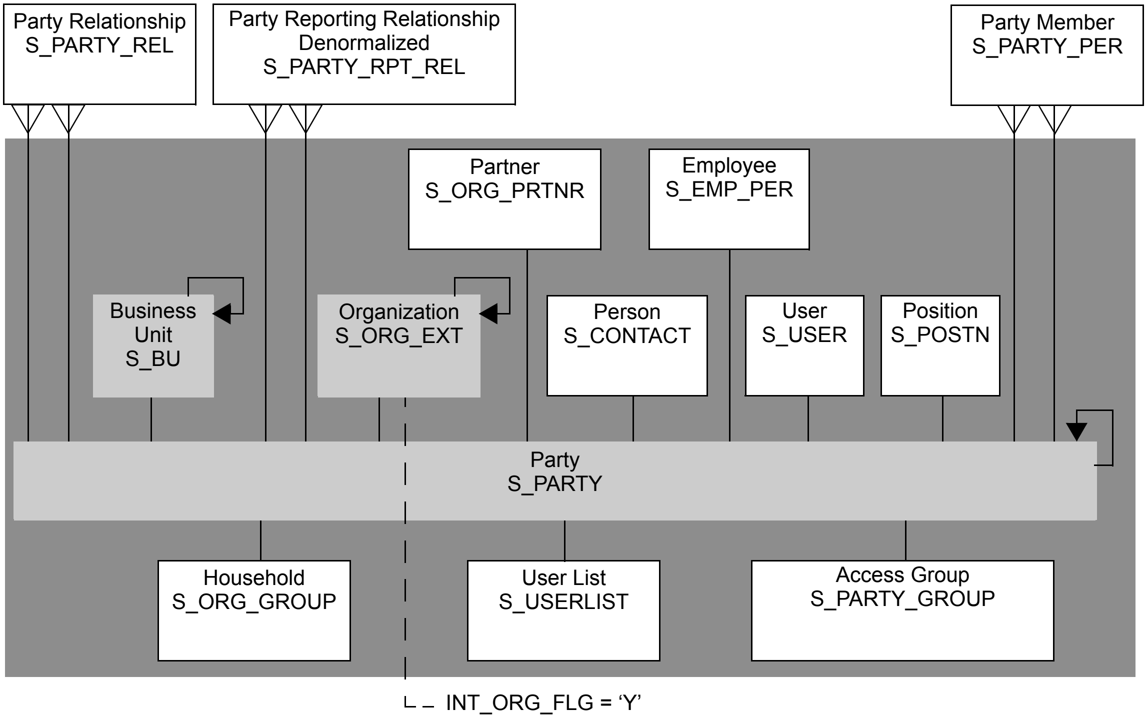


Figure 23. Organization Data Model

Partner Organization Data Model

In Figure 24, the base table and extension tables (S_ORG_EXT, S_BU, and S_ORG_PRTNR) that define a Partner Organization are shaded in the figure.

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.)

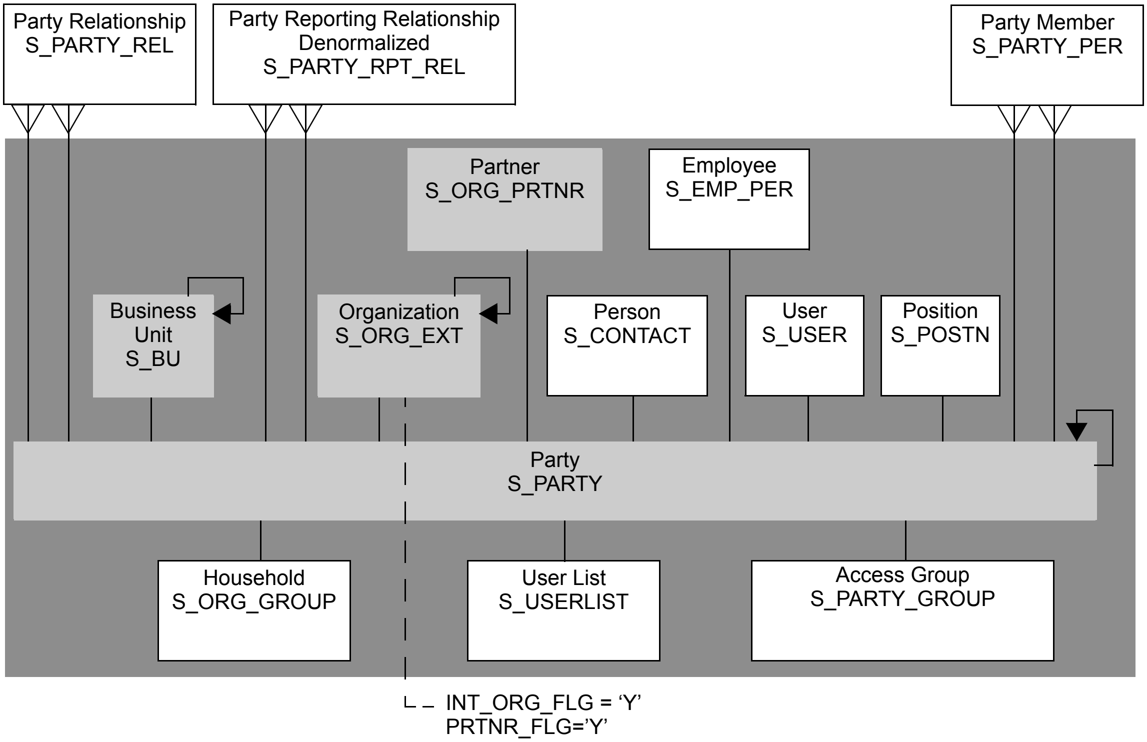


Figure 24. Partner Organization Data Model

Household Data Model

In Figure 25, the base table and extension table (S_ORG_GROUP) that define a Household are shaded in the figure.

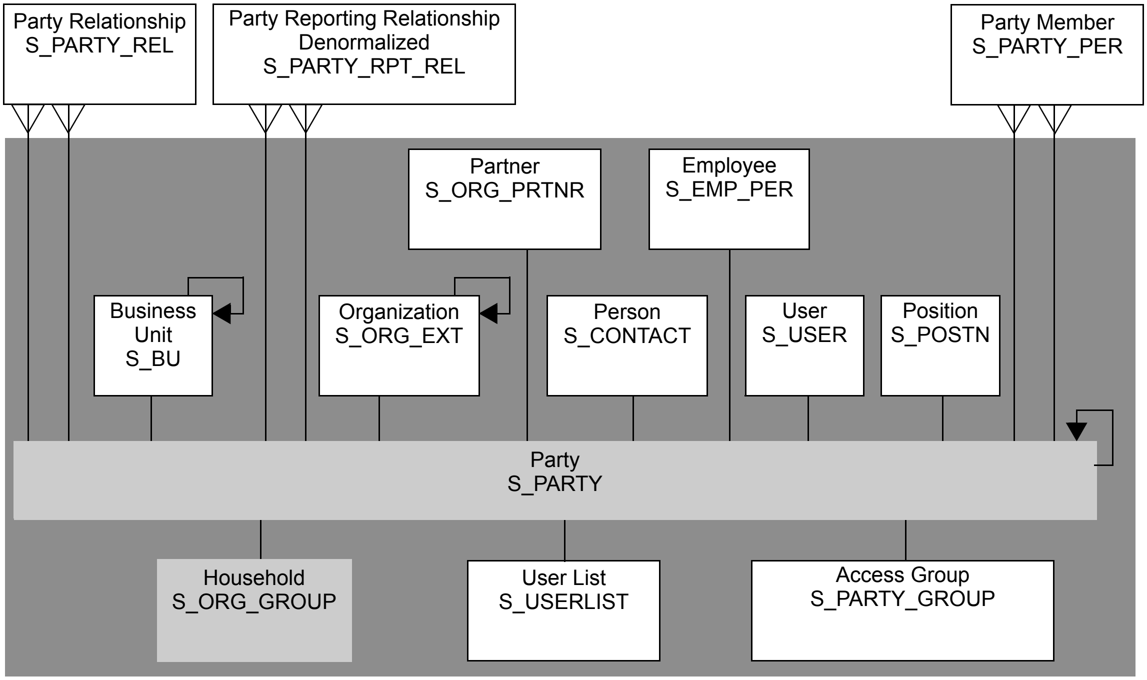


Figure 25. Household Data Model

User List Data Model

In Figure 25, the base table and extension table (S_USERLIST) that define a User List are shaded in the figure.

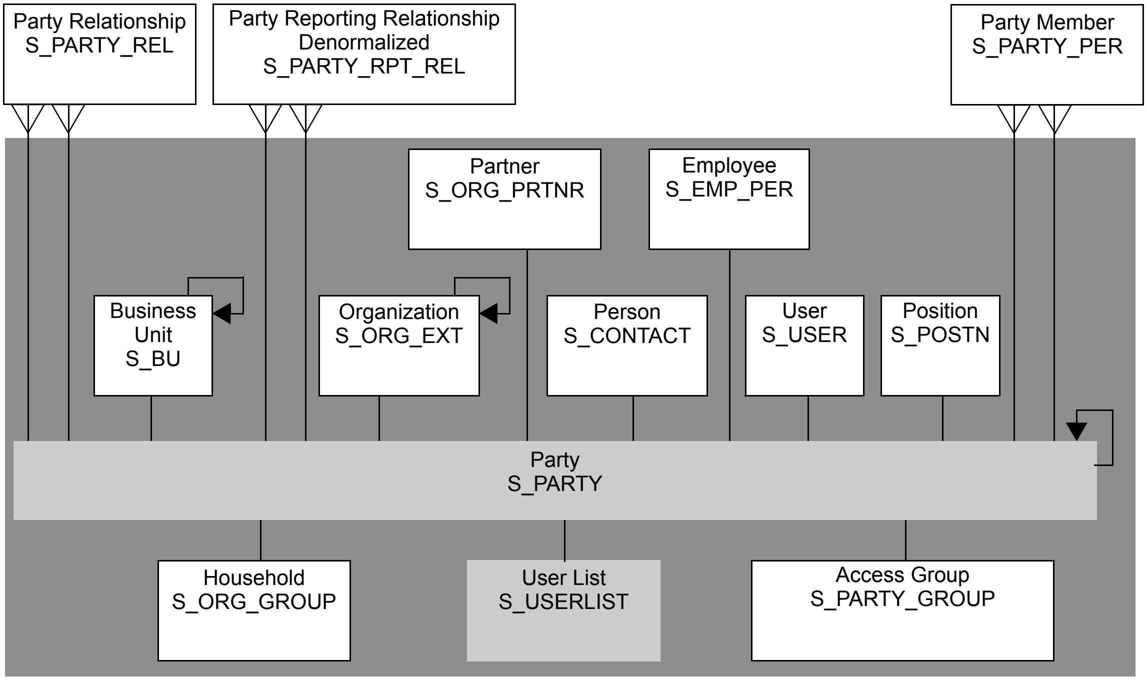


Figure 26. User List Data Model

Access Group Data Model

In Figure 25, the base table and extension table (S_PARTY_GROUP) that define an Access Group are shaded in the figure.

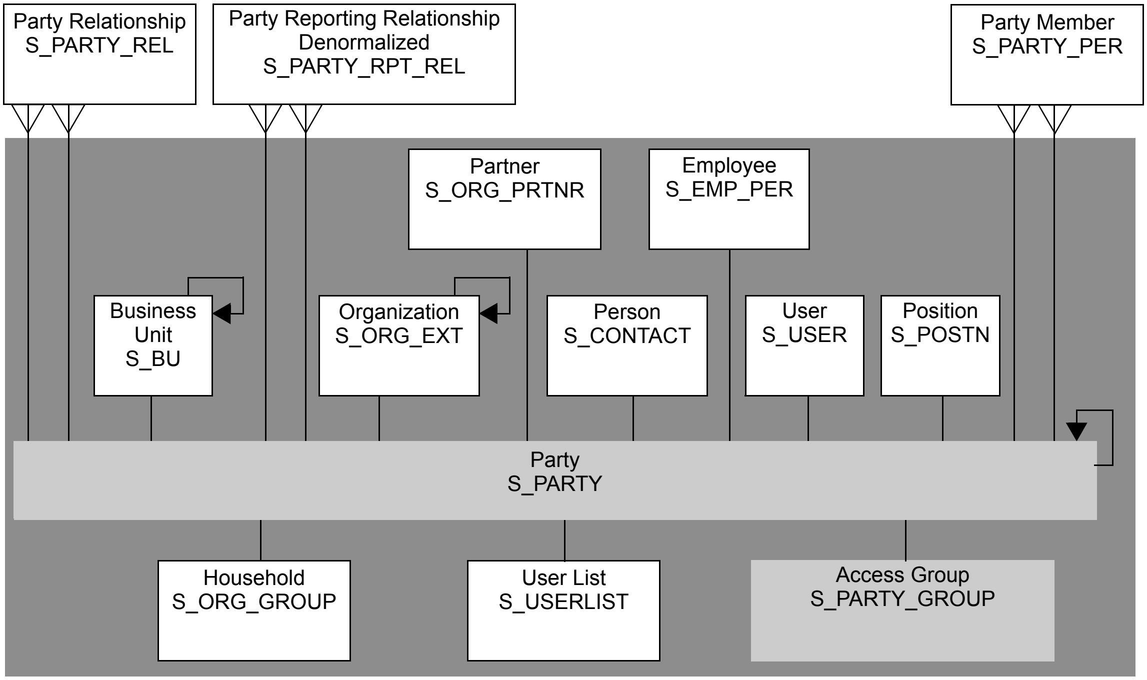


Figure 27. Access Group Data Model

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 table S_PARTY_PER. 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 table S_PARTY_REL. 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.

About Access Control Mechanisms

The basic access control mechanisms include the following, which are described in subsequent sections:

- **Personal access control.** For details, see "Personal Access Control" on page 309.
- **Position-based access control.** This includes single-position, team-based, and manager access control). For details, see "Position-Based Access Control" on page 310.
- **Organization-based access control.** This includes single-organization, multiple-organization, and suborganization access control. For details, see "Organization-Based Access Control" on page 315.
- **All access control.** For details, see "All Access Control" on page 319.
- **Access-group access control.** For details, see "Access-Group Access Control" on page 320.

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-based access control. For example, the My Opportunities view applies position-based access control.

Frequently different views have the same name because they are used in similar, but different, contexts. Some views under a given name may apply personal access control, while others with the same name may apply position- or organization-based access control.

For information about business component view modes, see "Business Component View Modes" on page 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

Position-Based Access Control

A position is a job title in a division of an internal or partner organization. A position hierarchy represents reporting relationships among positions. Positions provide an appropriate basis for access control in many scenarios, because a position in an organization is typically more stable than the individual's assignment to the position.

Customer data and some types of referential data can be associated with one or more positions. If individual data can be associated with a position, then you can apply position-based access control to the data by one or more of the following means:

- **Single-position access control.** You can associate a single position to individual data records.
- **Team-based access control.** You can associate multiple positions, in the form of a team, to individual data.
- **Manager access control.** You can grant access concurrently to data associated with a position and data associated with subordinate positions in a reporting hierarchy.

An employee or partner user can be associated with one or more positions, of which one can be the active position at a given time. All position-based access control for an employee or partner user is determined by the active position.

One of the user's positions is designated as the primary position. When a user logs in, the primary position is the active position. To make a different position the active position, one of the following must happen:

- An employee must designate another position as the active position, 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, refer to *Siebel Communications Server Administration Guide*.

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 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-based, or team-based 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 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

Team-Based 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-based 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-based access control, for example My Projects, the name of the active login is displayed. Other views, such as those using organization-based 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-based access control. However, *My* does not always imply team-based access control. Some *My* views apply personal, organization-based, or single-position access control. For example, the My Activities view applies personal access control.

A business component's view modes determine whether team-based access control can be applied in a view that is based on the business component. To have team-based 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-based access control.

If a business component is configured for team-based 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 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

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, the employee or partner has access to the following data:

- If the business component on which the view is based uses single-position access control, the user sees data associated directly with the user's active position or with subordinate positions.

- If the business component on which the view is based uses team-based 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-based 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 non-primary manager visibility.

  To configure non-primary 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, refer to *Siebel Developer's Reference*.

  CAUTION: Configuring non-primary 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 user sees only data associated with the user's primary position.

Views that apply manager access control generally contain the phrase *My Team's* in the title, such as My Team's Accounts. The word *My* is sometimes omitted, as in Team's Activities.

There are no business component view modes specific to manager access control. Manager access control is set at the view level. It requires that the business component on which the view is based has a view mode with owner type Position.

For information about business component view modes, see "Business Component View Modes" on page 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

Organization-Based Access Control

When individual data can be associated with an organization, you can apply organization-based access control to the data by one or more of the following means:

- **Single-organization access control.** You can associate a single organization with individual data.
- **Multiple-organization access control.** You can associate multiple organizations with individual data.
- **Suborganization access control.** You can grant access concurrently to data associated with an organization and data associated with subordinate organizations in the organizational hierarchy.

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 "Position-Based Access Control" on page 310.

A contact user is indirectly associated with an organization through the proxy employee specified for a Siebel customer application.

For information about proxy employees, see "User Authentication Overview" on page 89 and "Seed Data" on page 399.

Single-Organization and Multiple-Organization Access Control

Depending on the type of data, you can associate one or more organizations to individual data. The user can see data that is associated with the user's active organization. For example, in the All Service Requests view, a user can see all the service requests associated with the user's active organization.

For data that can be associated with multiple organizations, one of the organizations is designated as the primary organization.

The primary organization is a factor in suborganization access control, but not in multiple-organization access control.

Table 20 lists data on which you can apply organization-based access control and whether a single organization or multiple organizations can be associated with the data.

Table 20. Organization-Enabled Data

Object Type	Object	Relationship
Customer data	Account	Multiple
	Competitor	Multiple
	Contact	Multiple
	Opportunity	Multiple
	Order	Multiple
	Partner	Multiple
	Quote	Multiple
	Service Request	Multiple
Referential data	SmartScript	Multiple
	Literature	Multiple
	Price List	Multiple
	Product	Multiple
	Catalog	Multiple
Administrative data	Employee	Single
	Division	Single
	Position	Single
	Responsibility	Multiple
Other	Cost list/Rate list	Multiple
Assignment Manager	Assignment Manager	Enabled

NOTE: Customizable products that you create with Siebel eConfigurator 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 titles of views applying single or multiple-organization access control. For example, the All Contacts view applies single-organization access control, and the All Product Defects view applies multiple-organization access control. However, *All* does not always imply single- or multiple-organization access control. Some *All* views apply *All* access control. For example, the All Service Requests view applies *All* access control.

A business component's view modes determine whether single-organization or multiple-organization access control can be applied in a view that is based on the business component.

- To have single-organization access control available, a business component must have a view mode (typically Organization) of owner type Organization with an entry in the Visibility Field column (instead of the Visibility MVField column).
- To have multiple-organization access control available, a business component must have a view mode (typically Organization) of owner type Organization with entries in the Visibility MVField and Visibility MVLink columns (instead of the Visibility Field column).

For information about *All* access control, see "All Access Control" on page 319.

For information about business component view modes, see "Business Component View Modes" on page 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

Suborganization Access Control

Suborganization access control, based on hierarchical organizations, is analogous to manager access control, based on hierarchical positions.

For any organization in the organizational hierarchy, you can grant access to data associated with subordinate organizations. This access control mechanism is designed to provide 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 View > Site Map > Group Administration > Organizations.

The organizational hierarchy is included as seed data when you install your Siebel application. Within the organizational hierarchy, you can create branches for both internal and partner organizational structures.

You can specify one parent organization for an organization.

In a view using 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 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

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-based 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 340.

For information about implementing access control in a view, see "View Access Control Properties" on page 348.

For information about Admin mode, see "View Access Control Properties" on page 348.

Access-Group Access Control

Access-group access control is a means to control access by groups of diverse party types to categorized master data.

An access group is a collection of any combination of positions, organizations, accounts, 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, auctions, 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.

A category of master data can contain any combination of master data items. You can only control access to catalogs and categories of master data. You cannot control access to individual master data using access-group access control.

When access groups are associated with a catalog or with categories in the catalog, you can apply access-group access control. You can control access to the data in one of the following ways:

- **Group.** While in a given category, the user sees either a list of the category's first-level subcategories (child categories) to which he or she has access or all the data records in the current category, depending on the applet being used. If the user is at the catalog level, the user sees the first-level categories.
- **Catalog.** The user sees a flat list of all the data in categories across all catalogs to which the user has access. This 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 289.

For more information about parties, see "Access Control for Parties" on page 292.

For information about administering access-group access control, see "Administering Access-Group Access Control" on page 356.

Planning for Access Control

Two main strategies are available for controlling access to data in Siebel applications:

- **Access-group access to catalogued data.** This strategy can be implemented with all party types. It is designed to reduce access control administration by associating hierarchical groups of users with similarly organized data. This strategy can be applied to master data only.

  For more information, see "Access-Group Access Control" on page 320 and "Administering Access-Group Access Control" on page 356.

- **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 the sections following this one, and see "Organization-Based Access Control" on page 315.

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.

Business Environment Structure

As part of implementing an access control strategy for your application, you must define your company's structure, outside partner relationships, and so on. How you define the structure of your business environment will impact the records and views users will be able to access.

This section provides some background information about business environment structure. If your business enterprise is large and complex, you can accurately reflect its structure in setting 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 21.

Table 21. Elements of Business Environment Structure

Element	Parent-Child	Description
Organizations	Y	The major parts or entities that make up your company (or your partner companies). Used to control visibility of data.
Divisions	Y	Subunits of your company's (or partner company's) organizations. Used to set default currencies. Can be used in Actuate reports.
Positions	Y	Control the data set (records) to which a user has access.
Responsibilities	N	Control the views to which a user has access.
Employees	N	Individual users in your company and in partner companies who have access to your company's data.

For information about how Siebel Assignment Manager uses these elements, see *Siebel Assignment Manager Administration Guide*.

You can set up organizations, divisions, positions, responsibilities, and employees in any order. You can also associate these types of records with one another in a variety of ways. For example, to link a responsibility and an employee, you can associate the employee with the responsibility from the responsibility record, or you can associate the responsibility with the employee from the employee record.

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 Assignment Manager or Business Process Designer 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 must set up channel partner organizations to control their access.

  For more information on using organizations with Siebel customer and partner applications, see *Siebel Partner Relationship Management Administration Guide*.

Setting Up Organizations

This section and those that follow explain the common tasks for defining a company structure in your Siebel application. These include tasks for defining organizations, divisions, responsibilities, and positions.

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 *Siebel Tools Reference*.

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.
- Changing the name of the default organization, which is Default Organization, is not recommended. 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 *Siebel Tools Reference*.

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.

To set up an organization

1. From the application-level menu, choose View > Site Map > Group Administration > Organizations.

   The Organizations view appears.

2. In the More Info form, add a new record and complete the necessary fields.

   Some fields are described in the following table.

Field	Guideline
Parent Organization	If this organization is a suborganization, select the parent organization. This allows an organization to be associated with another organization.
Partner Manager Position	Used for Siebel PRM. Person in the organization who manages the relationship of that particular channel partner. Used in fund requests as the default value in the “Assign to” column.
Partner Flag	Used for Siebel PRM. When selected, indicates that the organization represents an external enterprise that is a partner of your company.

Setting Up Divisions

Divisions belong to organizations and have no direct effect on visibility. Divisions help you to group positions, to record addresses, and to maintain default currencies. User reporting structures are defined by their parent positions, but their country of operation and currency are defined by their division.

To implement Siebel eBusiness Applications, you must set up at least one division.

You can assign divisions to organizations. You can also promote a division to an organization. Multiple divisions can be arranged in a multilevel hierarchy by assigning some divisions as the parents of others.

You can assign positions to a division. When you associate employees with those positions, the employees become associated with the division.

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.

To set up a division

1. From the application-level menu, choose View > Site Map > Group Administration > Divisions.

   The Divisions view appears.

2. In the More Info form, add a new record and complete the necessary fields.

   Some fields are described in the following table.

Field	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.
Partner Manager Position	Used for Siebel PRM. Person in the organization who manages the relationship of that particular channel partner. Used in fund requests as the default value in the “Assign to” column.

Setting Up Positions

A position represents a specific job slot within your company. As you define your company structure, define specific positions with each level in the hierarchy of divisions. Positions determine which records users have access to. You must be logged on to a server database to add positions.

NOTE: An employee should have a position in order to create and use accounts, opportunities, contacts, and other customer data objects in your Siebel application.

Each position typically has only one associated employee. In some circumstances such as job-sharing situations, a position may have multiple associated employees. One employee can be associated with multiple positions. There can be only one primary employee for a position, but an employee can be primary for more than one position.

There is a drawback to having multiple employees associated with a position. Because a position can have only one primary employee, only the primary employee is visible in the Employee field. If you search for an employee in a positions list, you may not find relevant position records in which the employee is not primary for the position.

Only the primary employee for a position appears in the Account Team, Opportunity Sales Team, and Contact Access lists. However, all the employees in that position can access the My Accounts, My Opportunities, and My Contacts views.

A position can be associated with only one organization. If you want an employee to have visibility to multiple organizations, you must create a position for each organization and assign that employee to each position. The employee can then see one organization’s data at a time by changing positions.

Positions can be set up in a multilevel hierarchy. In this case, the parent position gains visibility to all the sets of data visible to the child positions individually.

Your Siebel application allows users to change their position to any other position in the organization. A user can change positions while logged in by choosing View > Site Map > User Preferences > Change Position, 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.

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).

A special consideration for mobile users is as follows: If you change a mobile user's position, that user's visibility rules change. In this case, it is recommended that the user reextract his or her local database. However, if you change only the position name (for example, from Sales Representative to Sales Associate), then the reextraction is not required. This is because position names are stored in the S_POSTN table, and this column has enterprise-wide visibility. In other words, changes to this column will be distributed to all users.

To set up a position

1. From the application-level menu, choose View > Site Map > Group Administration > Positions.

   The Positions view appears.

2. In the More Info form, add a new record and complete the necessary fields.

   Some fields are described in the following table.

   NOTE: Most fields in the More Info form are filled in automatically from the Employee record of the active employee. If you have not set up employees, you can associate them with positions later.

Field	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.

Field	Guideline
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.

Defining Responsibilities and Adding Views and Users

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.

Use responsibilities provided as seed data where applicable. Define any additional responsibilities you require that correspond to the major job functions in your organization.

For example, you might create responsibilities for the marketing administrator, the sales manager, and sales representatives. The sales representative responsibility might have access to all views except those reserved for sales management, marketing administration, and applications administration. The sales manager responsibility might have access to the same views as the sales representative, plus the sales manager views, and so on.

To define a responsibility, you must specify which views are available to that responsibility. You can use the seed responsibilities that come with your Siebel application. These can be copied and then customized.

NOTE: You cannot modify or delete the seed responsibilities. For instance, you cannot change the SADMIN responsibility. You can copy the seed responsibilities and modify the copies.

When you are defining responsibilities, consider the following issues:

- You should grant access to the System Preferences view to only a selected group of administrators. End users should not be given access to the System Preferences view. System preferences control many things throughout the system, for example server logic and processing for Siebel Remote and Territory Assignment.

- You should not add Administration views to responsibilities associated with end users. Likewise, you should limit access to the Master Forecasts, Mobile Web Clients, Responsibilities, Views, and Territories views. The work performed with these views has far-reaching implications for the entire application.

- You may want to hide access to license keys by deleting the license key-related views from a user's responsibility. For more information, see *Applications Administration Guide*.

- If you add the Internal Division View to a user's responsibility, all organizations in the Organizational picklist are displayed. By default, only the organization the user belongs to appears in this list.

- If you log into the application through the normal Siebel Web Client, you can add new views to responsibilities in the Application Administration > Responsibilities view.

  However, if you log into the application through the Siebel Dedicated Web Client or the Siebel Mobile 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, start the Dedicated or Mobile Web Client with the command-line option `/editseeddata`.

  For example, instead of starting the application with the following command:

  ```
  siebel.exe /c c:\sea752\client\bin\ENU\siebel.cfg
  ```

  an administrator can start the application with this command:

  ```
  siebel.exe /c c:\sea752\client\bin\ENU\siebel.cfg /editseeddata
  ```

  CAUTION: Before using the `/editseeddata` command-line option, you must fully understand the impact this feature may have upon your data.

To define a responsibility and add views and users

1. From the application-level menu, choose View > Site Map > Application Administration > Responsibilities.

   The Responsibilities view appears.

   NOTE: By default, the Responsibilities view shows all responsibilities, regardless of organization. However, you may want to configure new views in Siebel Tools that restrict the visibility to responsibilities. For more information on configuring views, see *Siebel Tools Reference*.

2. In the Responsibility list, add a new record and enter a name and description for the responsibility.
3. In the Organization field, select an organization for the responsibility.
4. To add views, do the following:

   a In the Views list, add a new record.

   b Select the appropriate views in the Add Views dialog box and click OK.

   NOTE: You can also delete views from the Views list.

5. To add users, do the following:

   a In the Users list, add a new record.

   b Select the appropriate users in the Add Users dialog box and click OK.

   NOTE: You can also delete employees from the Users list.

Implementing Basic Access Control

The particular data exposed in a view and whether a view is exposed at all are determined by settings made for related components.

You configure most of these settings in Siebel Tools. This section specifies where to find these settings within 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 *Siebel Tools Reference*.

The following components determine what views a user sees:

- **Application.** Each Siebel application includes a licensed set of views. When a user is in an application, the user has no access to views that are not included in the application.
- **Responsibilities.** Every user has one or more responsibilities, which define the collection of views to which the user has access. If a particular view is not in a user's responsibilities, then the user does not see that view. A wide-ranging view such as All Opportunities Across Organizations is not typically included in the responsibility for an employee such as a district sales rep.

The following components determine the data within a view to which a user has access.

- **Business component view mode.** A view can have several applets—lists, forms, or trees. Each applet is based on a business component. The business component's view mode determines the allowable parties on which access control can be based for that business component. The business component's view modes also determine how the association with the party will be determined, for example "owned by" or "created by."
- **Applet visibility properties.** A view can specify one of its applets as the visibility applet. The visibility applet connects the business component to the view. The visibility applet specifies which business component to use and the display names for the business component's fields.
- **View visibility properties.** A view's visibility properties determines the access control mechanism that is applied to the business component on which the view is based. For example, the business component may have personal or position-based access control available. The view specifies which of these to use, and in which form to use it.

In short, the application and a user's responsibility restrict the views presented to the user. Within a view, view visibility properties determine the applet that drives visibility in the view and specifies the access control mechanism to apply to the business component. The view's visibility applet specifies the business component used in the view. The business component specifies how a user can be associated with data to provide access.

Application-Level Access Control

Each Siebel application is associated with a set of screens. Each screen is in turn made up of a set of views.

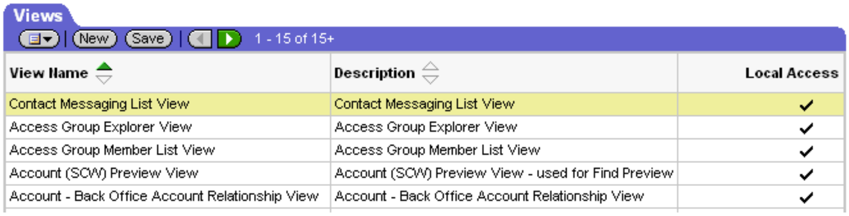
In a particular application, all users are limited to the views that are licensed to your company and that are defined for the application. The licensed views are specified in the license key, which is determined by the features you purchase for your Siebel eBusiness Applications.

To see an application's views

1. Log in as an administrator, and then click the Application Administration screen tab.

2. In the Show drop-down list, select Views.

   This figure shows a sample list of views defined for an application.



View Name	Description	Local Access
Contact Messaging List View	Contact Messaging List View	✓
Access Group Explorer View	Access Group Explorer View	✓
Access Group Member List View	Access Group Member List View	✓
Account (SCW) Preview View	Account (SCW) Preview View - used for Find Preview	✓
Account - Back Office Account Relationship View	Account - Back Office Account Relationship View	✓

For information about adding screens and views, see *Siebel Tools Reference*.

Responsibilities

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 Show drop-down list, 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 Server Administration screen. The administrator sees the Server Administration screen listed in the Site Map and the appropriate views in the Show drop-down list. A customer care agent typically does not have administrative views in a responsibility, so the agent would not see the Server Administration screen or its views listed in any context.

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 372.

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 requires that the associated Application Object Manager be restarted in order for these new settings to take effect for users of the Siebel Web Client.

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 PRM Partner Portal.

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 position- or organization-based views in the responsibility.

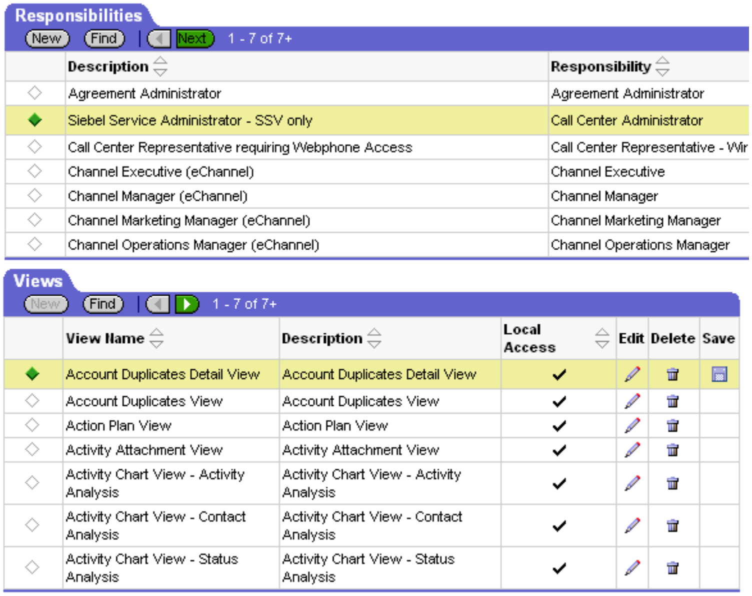
Local Access for Views

Each view has a Local Access flag. If it is set to `TRUE` (checked), all users with the view in their responsibilities can access the view from either the local database or the server database. When it is set to `FALSE` (unchecked), users can access the view only when they are connected to the server database.

The Local Access field can be set for a view through either of the following paths:

- View > Site Map > Application Administration > Views
- View > Site Map > Application Administration > Responsibilities

Figure 28 shows the Local Access field for views associated with a responsibility.



	Description	Responsibility
◇	Agreement Administrator	Agreement Administrator
◆	Siebel Service Administrator - SSV only	Call Center Administrator
◇	Call Center Representative requiring Webphone Access	Call Center Representative - Wir
◇	Channel Executive (eChannel)	Channel Executive
◇	Channel Manager (eChannel)	Channel Manager
◇	Channel Marketing Manager (eChannel)	Channel Marketing Manager
◇	Channel Operations Manager (eChannel)	Channel Operations Manager

	View Name	Description	Local Access	Edit	Delete	Save
◆	Account Duplicates Detail View	Account Duplicates Detail View	✓	✎	🗑	💾
◇	Account Duplicates View	Account Duplicates View	✓	✎	🗑	
◇	Action Plan View	Action Plan View	✓	✎	🗑	
◇	Activity Attachment View	Activity Attachment View	✓	✎	🗑	
◇	Activity Chart View - Activity Analysis	Activity Chart View - Activity Analysis	✓	✎	🗑	
◇	Activity Chart View - Contact Analysis	Activity Chart View - Contact Analysis	✓	✎	🗑	
◇	Activity Chart View - Status Analysis	Activity Chart View - Status Analysis	✓	✎	🗑	

Figure 28. Responsibility Views List

NOTE: In the Responsibility Views list shown in Figure 28, you cannot edit the Local Access field for a view in a seed responsibility. Use the Views Administration view instead.

The Local Access field is primarily a mechanism for controlling which views mobile users can work in offline. In addition to enabling or disabling local access to views based on responsibility, administrators can turn off one set of views for one mobile user and a different set for another mobile user. For more information, see *Siebel Remote and Replication Manager Administration Guide*.

NOTE: You should disable access to views applying *All* access control by setting the Local Access field to FALSE. A view with *All* access control will have unpredictable and possibly undesirable results for a mobile user.

For information about *All* access control, see "All Access Control" on page 319.

Assigning a Responsibility to an Individual

You can add a responsibility to a Person, to a User, to an Employee, or to a Partner record. The following procedure describes how to add a responsibility to a Person record. Alternatively, you can assign a responsibility in the All Users list, in the All Employees list, or in the All Partners list of the User Administration screen.

If the individual does not have a current responsibility, this procedure upgrades the Person to a User. If the individual already has at least one responsibility, then the individual is already a User, an Employee, or a Partner. As such, the individual's record appears in the Persons list also, so this procedure works for any scenario.

To assign a responsibility to a Person

1. Log into a Siebel employee application as an administrator and choose View > Site Map > User Administration > Persons.

   The All Persons list appears.

2. Select a Person record.

3. In the More Info form, click the browse button on the Responsibility field.

   A list of the responsibilities assigned to this Person appears.

4. In the Responsibilities list, click New.

   A list of responsibilities available for assigning appears.

5. Select one or more responsibilities, and then click OK.

   The selected responsibilities appear in the list of responsibilities for this Person.

6. Click OK.
7. In the More Info form, click Save.

If you want to assign the same responsibility to multiple users, you can alternatively add the users to the responsibility through the Application Administration screen.

Business Component View Modes

A business component's view modes determine the allowable access control mechanisms that can be applied to the business component in any view. When a view is based on a particular business component, the view must use one of the view modes specified for the business component. For example, the Account business component can only be used in Organization view mode or Sales Rep view mode.

Each view mode also determines how data is associated with a user to determine whether the user gets access. For example, a business component that allows personal access control may connect the data to the person by comparing the data's Owner Id field to the person's Login ID. Another business component may apply personal access control through the data's Created by field.

You use Siebel Tools to work with properties of business components.

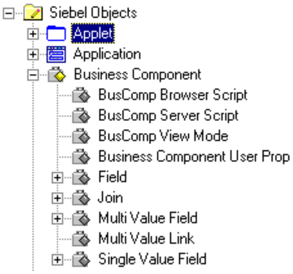
NOTE: If a business component has no listed view modes, then there is no access control based on the business component in views that are based on that business component.

To view a business component's view mode and visibility fields

1. Launch Siebel Tools.

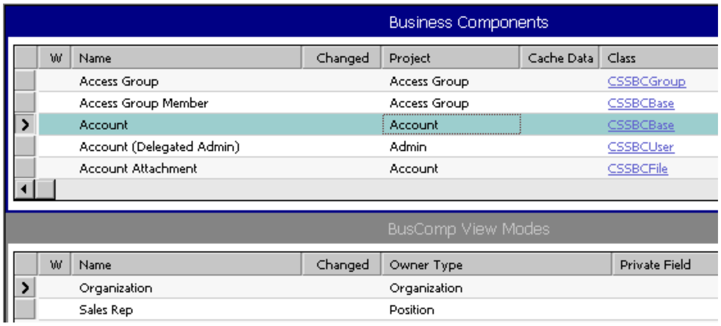
2 In the Object Explorer, click + (the plus sign) to expand the Business Component object type.

The Business Component sub-tree 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 in the following figure.



Business Components

	W	Name	Changed	Project	Cache Data	Class
		Access Group		Access Group		CSSBCGroup
		Access Group Member		Access Group		CSSBCBase
>		Account		Account		CSSBCBase
		Account (Delegated Admin)		Admin		CSSBCUser
		Account Attachment		Account		CSSBCFile

BusComp View Modes

	W	Name	Changed	Owner Type	Private Field
>		Organization		Organization	
		Sales Rep		Position	

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 multi-value field).** This field has the same purpose as Visibility Field, except a value in this field indicates that there can be more than one party associated with this business component when using this view mode.

  For example, the Account business component's Sales Rep view mode determines whether the user is associated with the record by comparing the user's position with the value in the Sales Rep field.

  When this view mode is used, more than one position can be associated with a record. In some applets, the Sales Rep field has a display name like "Account Team," indicating that more than one position is associated with the record.

- **Visibility MVLink (or multi-value link).** An entry in this field is required if there is a value in Visibility MVField.

  This field specifies which of the business component's multi-value links should be used to determine the value in the MVField for this record.

  Links establish a parent/child relationship between business components, often by specifying an intersection table (in the case of a many-to-many relationship). This multi-value link's Destination Link property indicates which link ultimately defines this relationship.

  To see a business component's multi-value links and their properties in Siebel Tools, expand the Business Component object in the Object Explorer, and then click Multi Value Link. The Destination Link property is a field in each record.

  For example, the Account business component's Sales Rep view mode has Position as its MVLink. The Destination Link property for this multi-value link specifies that this relationship uses the Account/Position link. As seen in 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.

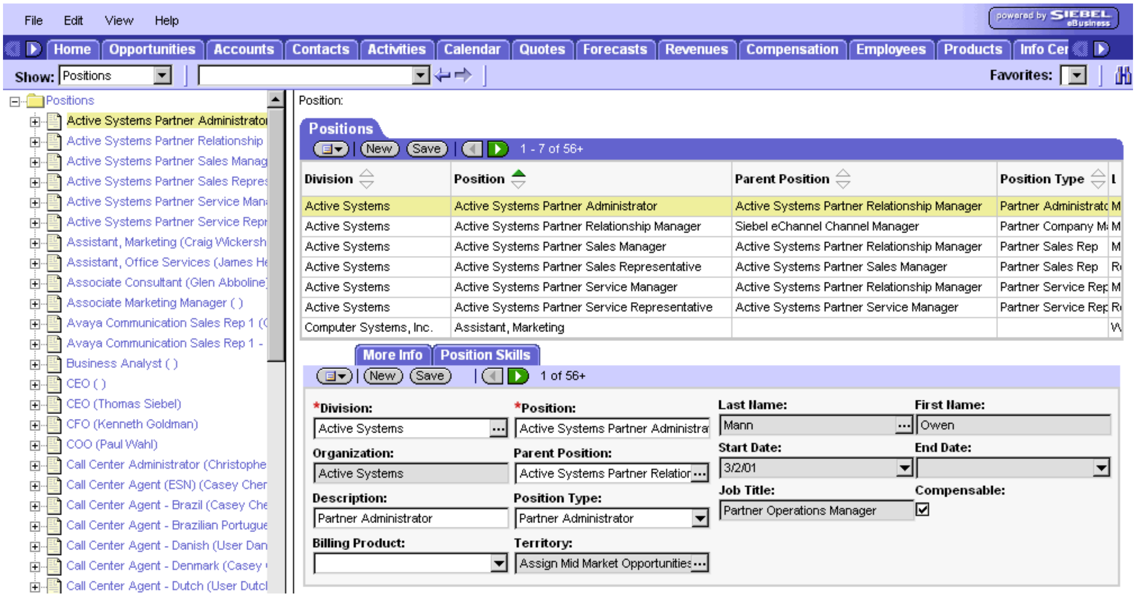
  An example of an exception to the typical naming convention is the Service Request business component.

  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. These two Person-based view modes are needed because the creator and the customer care agent both need access to the data based on their person.

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

Applet Access Control Properties

A view presents a collection of lists, forms, and trees at once, as shown in Figure 29. These lists and forms are referred to as applets in a configuration context.



Positions
- Active Systems Partner Administrator
- Active Systems Partner Relationship
- Active Systems Partner Sales Manag
- Active Systems Partner Sales Repres
- Active Systems Partner Service Man
- Active Systems Partner Service Repr
- Assistant, Marketing (Craig Wickersh
- Assistant, Office Services (James He
- Associate Consultant (Glen Abboline)
- Associate Marketing Manager ( )
- Avaya Communication Sales Rep 1 ((
- Avaya Communication Sales Rep 1 -
- Business Analyst ( )
- CEO ( )
- CEO (Thomas Siebel)
- CFO (Kenneth Goldman)
- COO (Paul Wahl)
- Call Center Administrator (Christophe
- Call Center Agent (ESN) (Casey Cher
- Call Center Agent - Brazil (Casey Che
- Call Center Agent - Brazilian Portugue
- Call Center Agent - Danish (User Dan
- Call Center Agent - Denmark (Casey
- Call Center Agent - Dutch (User Dutcl

Division	Position	Parent Position	Position Type	L
Active Systems	Active Systems Partner Administrator	Active Systems Partner Relationship Manager	Partner Administratc	M
Active Systems	Active Systems Partner Relationship Manager	Siebel eChannel Channel Manager	Partner Company M	M
Active Systems	Active Systems Partner Sales Manager	Active Systems Partner Relationship Manager	Partner Sales Rep	M
Active Systems	Active Systems Partner Sales Representative	Active Systems Partner Sales Manager	Partner Sales Rep	R
Active Systems	Active Systems Partner Service Manager	Active Systems Partner Relationship Manager	Partner Service Rep	M
Active Systems	Active Systems Partner Service Representative	Active Systems Partner Service Manager	Partner Service Rep	R
Computer Systems, Inc.	Assistant, Marketing			W

*Division: Active Systems	*Position: Active Systems Partner Administra	Last Name: Mann	First Name: Owen
Organization: Active Systems	Parent Position: Active Systems Partner Relatior	Start Date: 3/2/01	End Date:
Description: Partner Administrator	Position Type: Partner Administrator	Job Title: Partner Operations Manager	Compensable: ☑
Billing Product:	Territory: Assign Mid Market Opportunities		

Figure 29. 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.

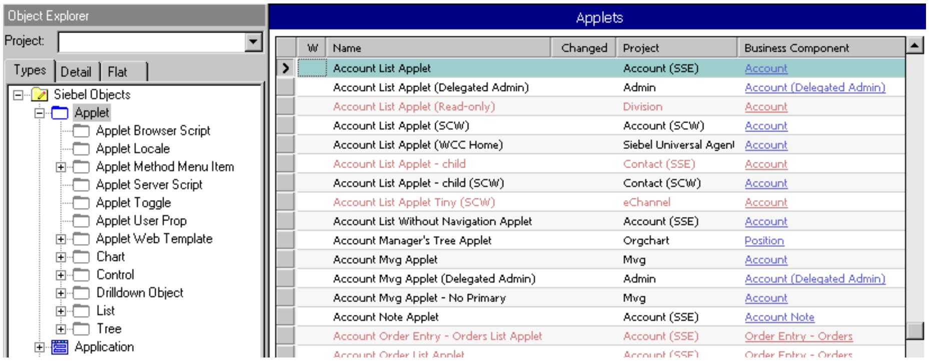
You use Siebel Tools to work with properties of applets.

To view an applet's properties

1 Launch Siebel Tools.

2 In the Object Explorer, click + to expand the Applet object type.

The Applet subtree appears. The Applets list also appears as shown in the following figure.



- Siebel Objects
  - Applet
    - Applet Browser Script
    - Applet Locale
    - Applet Method Menu Item
    - Applet Server Script
    - Applet Toggle
    - Applet User Prop
    - Applet Web Template
    - Chart
    - Control
    - Drilldown Object
    - List
    - Tree
  - Application

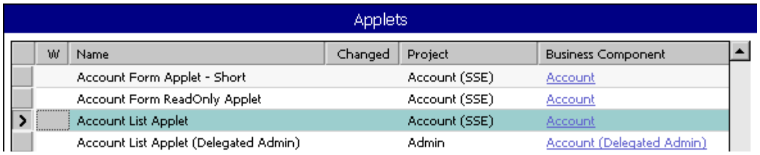
W	Name	Changed	Project	Business Component
	Account List Applet		Account (SSE)	Account
	Account List Applet (Delegated Admin)		Admin	Account (Delegated Admin)
	Account List Applet (Read-only)		Division	Account
	Account List Applet (SCW)		Account (SCW)	Account
	Account List Applet (WCC Home)		Siebel Universal Agent	Account
	Account List Applet - child		Contact (SSE)	Account
	Account List Applet - child (SCW)		Contact (SCW)	Account
	Account List Applet Tiny (SCW)		eChannel	Account
	Account List Without Navigation Applet		Account (SSE)	Account
	Account Manager's Tree Applet		Orgchart	Position
	Account Mvg Applet		Mvg	Account
	Account Mvg Applet (Delegated Admin)		Admin	Account (Delegated Admin)
	Account Mvg Applet - No Primary		Mvg	Account
	Account Note Applet		Account (SSE)	Account Note
	Account Order Entry - Orders List Applet		Account (SSE)	Order Entry - Orders
	Account Order List Applet		Account (SSE)	Order Entry - Orders

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.** As shown in Figure 30, this field in the Applets list applet specifies the business component on which the applet is based. For example, Account List Applet uses the Account business component.

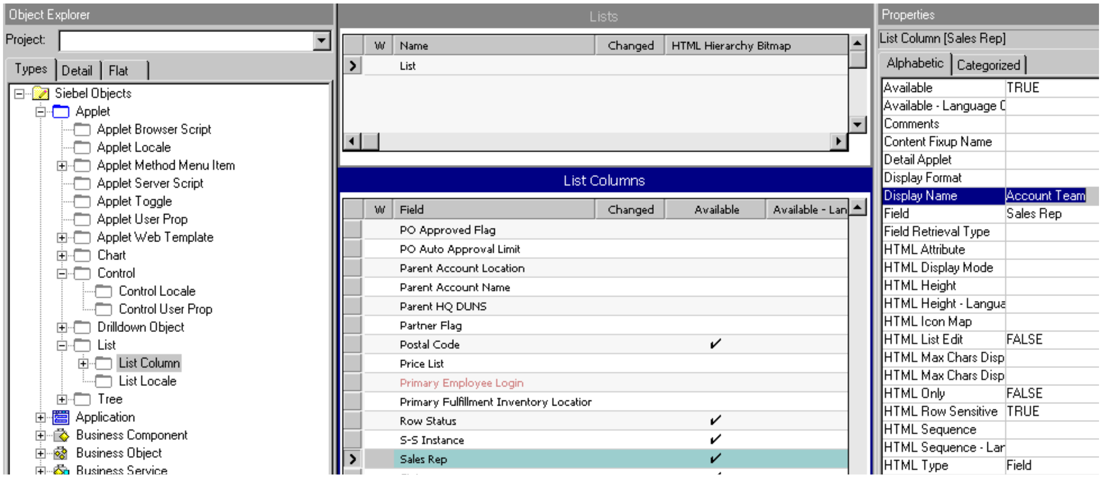


W	Name	Changed	Project	Business Component
	Account Form Applet - Short		Account (SSE)	Account
	Account Form ReadOnly Applet		Account (SSE)	Account
	Account List Applet		Account (SSE)	Account
	Account List Applet (Delegated Admin)		Admin	Account (Delegated Admin)

Figure 30. Business Component Field for an Applet

- **Display Name.** In the Tools Object Explorer, choose Applets > List > List Columns. As shown in Figure 31, the List Columns list applet shows the fields of the business component that this applet will display. For each business component field, the Display Name entry in the accompanying Properties 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.



Lists

W	Name	Changed	HTML Hierarchy Bitmap
	List		

List Columns

W	Field	Changed	Available	Available - Lan
	PO Approved Flag			
	PO Auto Approval Limit			
	Parent Account Location			
	Parent Account Name			
	Parent HQ DUNS			
	Partner Flag			
	Postal Code		✓	
	Price List			
	Primary Employee Login			
	Primary Fulfillment Inventory Locatior			
	Row Status		✓	
	S-S Instance		✓	
	Sales Rep		✓	

List Column [Sales Rep]

Available	TRUE
Available - Language C	
Comments	
Content Fixup Name	
Detail Applet	
Display Format	
Display Name	Account Team
Field	Sales Rep
Field Retrieval Type	
HTML Attribute	
HTML Display Mode	
HTML Height	
HTML Height - Langua	
HTML Icon Map	
HTML List Edit	FALSE
HTML Max Chars Disp	
HTML Max Chars Disp	
HTML Only	FALSE
HTML Row Sensitive	TRUE
HTML Sequence	
HTML Sequence - Lar	
HTML Type	Field

Figure 31. List Columns List Applet

For information about working with applets, see *Siebel Tools Reference*.

View Access Control Properties

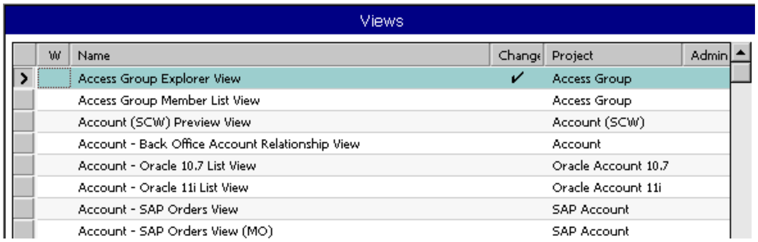
A view's access control properties determine what applet is used to drive visibility and what access control mechanism is applied to the business component on which the view is based.

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.



Views

W	Name	Change	Project	Admin
	Access Group Explorer View	✓	Access Group	
	Access Group Member List View		Access Group	
	Account (SCW) Preview View		Account (SCW)	
	Account - Back Office Account Relationship View		Account	
	Account - Oracle 10.7 List View		Oracle Account 10.7	
	Account - Oracle 11i List View		Oracle Account 11i	
	Account - SAP Orders View		SAP Account	
	Account - SAP Orders View (MO)		SAP Account	

The following fields in the Views list 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 Show drop-down list for any screen has a visibility applet, but a view that results from drilling down from another view does not. A view with no visibility applet typically inherits access control properties from the view from which it is derived.

  - Multiple views can have the same visibility applet. For example, both All Account List View and Manager's Account List View have Account List Applet as their visibility applet.

- **Visibility Applet Type.** This field determines the access control mechanism that is applied to that view. It specifies which of the business component's view modes are applied and how they are applied. Following are the choices available in the 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-based 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-based access control, then the user sees data for which the user's active position is the primary position on the team or a subordinate position is the primary member on the team.

  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 inset, delete, merge, and update restrictions for the business component used by applets of the view are ignored (including those restrictions specified by business component user properties).

  Examples of Admin mode views include Account Administration view, Opportunity Administration view, and Product Administration view.

  Admin mode does not override pop-up visibility. It does not override Read Only restrictions on fields in a business component.

  In Admin mode, every record in a view that uses team-based access control is visible, even those with no primary position designated. (This mode is distinct from *All* visibility, which shows all records that have a primary team member designated.)

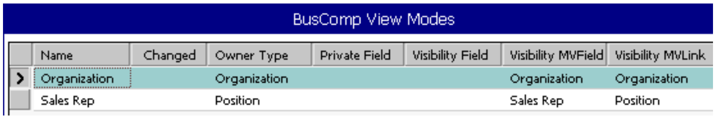
CAUTION: Views using Admin mode are intended for access by administrators and are typically included in a grouping of like views in an administration screen, such as Application Administration. Do not include views in Admin mode in a screen with views not set for Admin mode. When a user transitions from a view that is in Admin mode to one that is not, the target view remains in Admin view, thereby exposing data that is not intended to be seen.

An Example of Flexible View Construction

The following example shows how several existing views were constructed, based on the same visibility applet and business component. It suggests how similar view “families” can be constructed in Siebel Tools, but does not give procedures for constructing views. Changing any settings in Siebel Tools requires recompiling the Siebel repository file (SRF).

For more information about required practices when using Siebel Tools, see *Siebel Tools Reference*.

Figure 32 shows the BusComp View Modes list in Siebel Tools, for the Account business component.



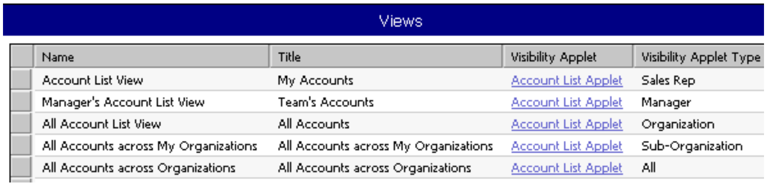
BusComp View Modes

Name	Changed	Owner Type	Private Field	Visibility Field	Visibility MVField	Visibility MVLink
Organization		Organization			Organization	Organization
Sales Rep		Position			Sales Rep	Position

Figure 32. Account Business Component View Modes

As indicated by the Owner Type field, organization-based and position-based view modes are allowed. As indicated in Visibility MVField, accounts can be associated with multiple organizations and multiple positions (for example, sales teams).

Figure 33 shows five views in the Views list in Siebel Tools.



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 33. Some Views Based on the Account Business Component

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.

These five views provide different lists of data by specifying different visibility applet types, as shown below in Table 22.

Table 22. Views and Visibility Applet Types

View	Visibility Applet Type	Data Access
Account List View (displayed as My Accounts)	Sales Rep	Sales Rep is a position-based access control mechanism. It is applied to a business component for which multiple positions can be associated. Access is granted to a user whose position is on the account team.
Manager's Account List View (displayed as Team's Accounts)	Manager	Manager is a position-based access control mechanism. Here it is applied to a business component for which multiple positions can be associated. Access is granted to data for which the user's active position or a subordinate position is the primary position on the account team.
All Account List View (displayed as All Accounts)	Organization	Organization is an organization-based access control mechanism. It is applied to a business component for which multiple organizations can be associated. Access is granted to a user whose primary organization is one of the organizations with which the account is associated.
All Accounts across My Organizations	Sub-Organization	Sub-Organization is an organization-based access control mechanism. In this view it is applied to a business component for which multiple organizations can be associated. Access is granted to data for which the user's active organization or a descendant organization is the primary organization.
All Accounts across Organizations	All	The Account business component has only position-based and organization-based view modes. Any user with this view in the user's responsibilities sees every account for which there is a primary position on the account team or an organization associated with the account.

Administering Access-Group Access Control

You associate an access group to a catalog or category of master data. When an access group is associated with a catalog or a category, the users associated with the access group have visibility of the data in the catalog or the category.

The following principles apply to access-group access control. An access group in the following context is an individual node in an access group hierarchy:

- **Private catalogs and categories.** A catalog is a hierarchy of categories. A catalog cannot itself contain data. To apply access-group access control on all of a catalog's categories, you must designate the catalog as private, and then associate access groups to the catalog. If a catalog is not private, then any user can see data in its categories. You can designate individual categories private within a public catalog.
- **Access group access is inherited.** If an access group is associated with a category, then the group's 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 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 34 on page 359 illustrates one access control structure that solves this business problem.

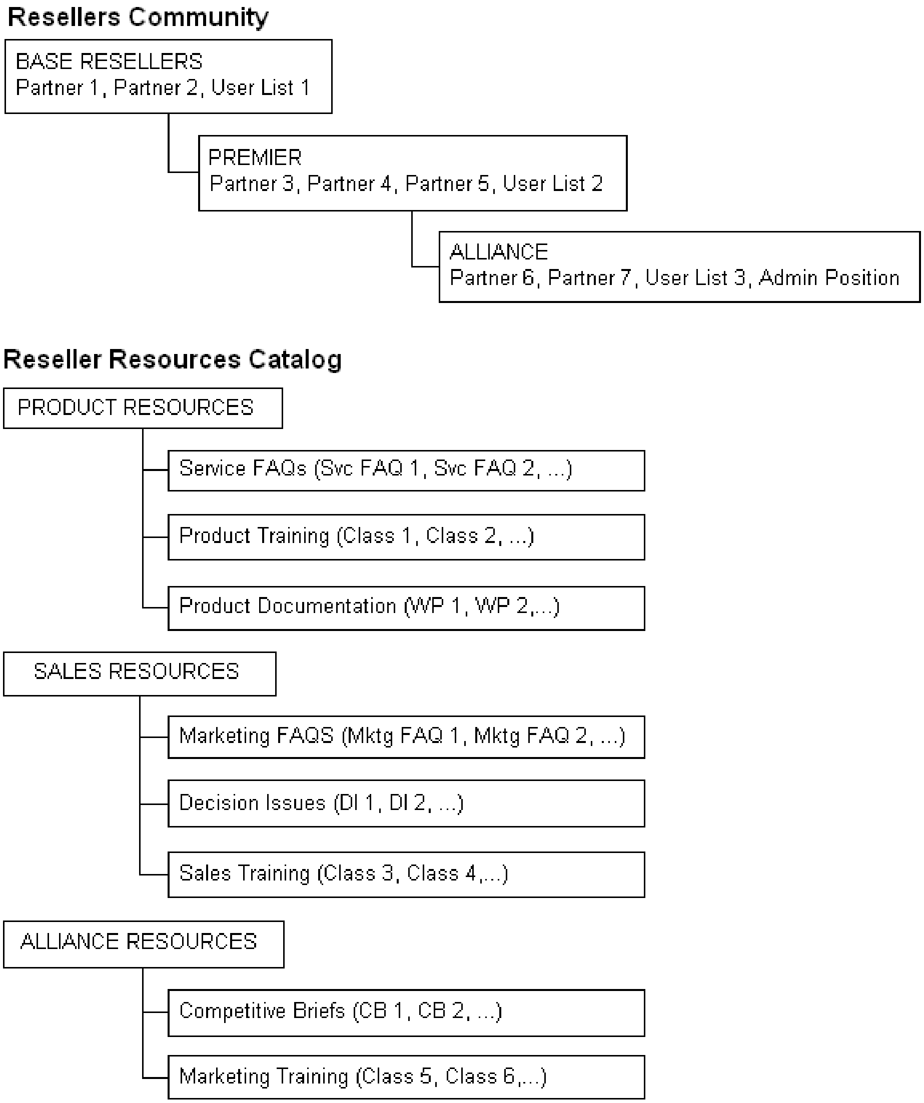

Resellers Community
BASE RESELLERS
Partner 1, Partner 2, User List 1
PREMIER
Partner 3, Partner 4, Partner 5, User List 2
ALLIANCE
Partner 6, Partner 7, User List 3, Admin Position
Reseller Resources Catalog
PRODUCT RESOURCES
Service FAQs (Svc FAQ 1, Svc FAQ 2, ...)
Product Training (Class 1, Class 2, ...)
Product Documentation (WP 1, WP 2,...)
SALES RESOURCES
Marketing FAQS (Mktg FAQ 1, Mktg FAQ 2, ...)
Decision Issues (DI 1, DI 2, ...)
Sales Training (Class 3, Class 4,...)
ALLIANCE RESOURCES
Competitive Briefs (CB 1, CB 2, ...)
Marketing Training (Class 5, Class 6,...)

Figure 34. Reseller Resources Access Control

This solution assumes that your partners are stored as organizations, in which partner users are associated with positions. The consultants exist as users; they have responsibilities, but not positions, and are not associated with an organization.

The Resellers Community is an access group hierarchy. Each node is an access group whose members are partner organizations and a single user list. The user list in each node contains all consultants of the appropriate status. For internal administrators to have visibility of the catalog, include their positions in the ALLIANCE access group.

The Reseller Resources catalog is constructed of categories containing data and nodes that are empty categories to define access levels.

Apply the following principles to construct this structure:

- Construct the Resellers Community such that the upper levels have the narrowest access to resources. Therefore, the BASE RESELLER access group is the parent of the PREMIER access group, which is in turn the parent of the ALLIANCE access group.
- Construct the Reseller Resources Catalog such that the PRODUCT RESOURCES, SALES 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 PRM 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*.

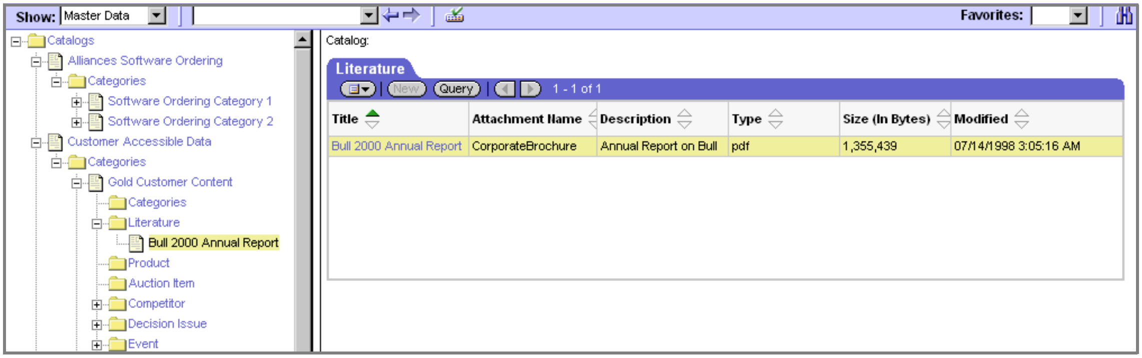
- Creating and administering user lists and access groups, see "Administering Access-Group Access Control" on page 356.

The User's Experience

You can configure a catalog to display in Siebel employee applications and in selected customer and partner applications, such as Siebel eSales and Siebel PRM Partner Portal, as a default functionality.

In an employee application, such as Siebel Call Center, a user can see categorized data controlled by access group membership in the Info Center and Info Center Explorer screens.

As shown in Figure 35, Info Center Explorer provides a tree interface for navigating all the catalogs to which the user has access, down to the data item level.



Show: Master Data

Favorites:

Catalog:

Literature

1 - 1 of 1

Title	Attachment Name	Description	Type	Size (In Bytes)	Modified
Bull 2000 Annual Report	CorporateBrochure	Annual Report on Bull	pdf	1,355,439	07/14/1998 3:05:16 AM

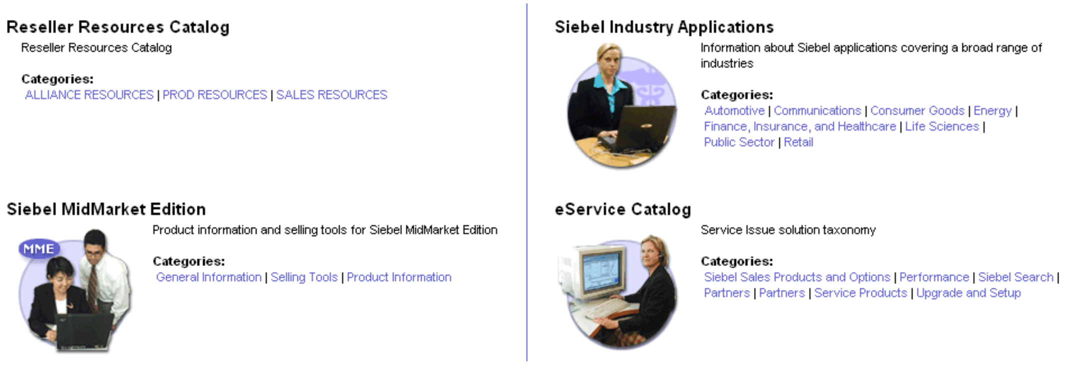
Figure 35. Info Center Explorer

Info Center is typical of the way categorized data can be presented in Siebel applications using a more open interface.

To see categorized data in Info Center

1 Choose View > Site Map > Info Center, and then click the Info Center link.

The Info Center screen appears as shown in the following figure. It shows accessible catalogs and their first-level categories.



Reseller Resources Catalog
Reseller Resources Catalog

Categories:
ALLIANCE RESOURCES | PROD RESOURCES | SALES RESOURCES

Siebel Industry Applications
Information about Siebel applications covering a broad range of industries

Categories:
Automotive | Communications | Consumer Goods | Energy | Finance, Insurance, and Healthcare | Life Sciences | Public Sector | Retail

Siebel MidMarket Edition
Product information and selling tools for Siebel MidMarket Edition

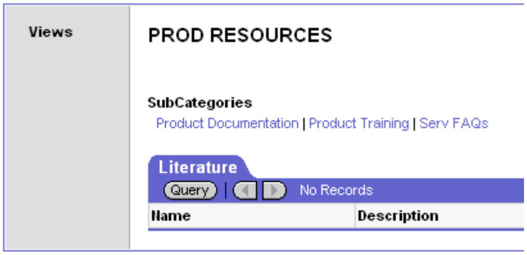
Categories:
General Information | Selling Tools | Product Information

eService Catalog
Service Issue solution taxonomy

Categories:
Siebel Sales Products and Options | Performance | Siebel Search | Partners | Partners | Service Products | Upgrade and Setup

2 Click a category link.

As shown below, the category appears, showing its data items and its first-level subcategories.



Views

PROD RESOURCES

SubCategories
Product Documentation | Product Training | Serv FAQs

Literature
Query | ◀ ▶ | No Records

Name	Description

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 Catalog Administration screen:

- Create and delete catalogs and categories of master data.
- Associate data with categories.
- Modify the hierarchical position of a category within a catalog.

Key principles for setting up a catalog include, but are not limited to:

- Set the Catalog Type field to allow display of the catalog in certain Siebel customer or partner applications, in addition to Info Center and Info Center Explorer in Siebel employee applications. For example, set the Catalog Type to Partner to display the catalog in Siebel PRM 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*, *Siebel eAuction 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 *Siebel Call Center User 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 292.

Creating a User List

You can create a user list in the Group Administration screen.

To create a user list

1. Choose View > Site Map > Group Administration > User Lists.

   The User Lists list appears.

2. In the User Lists list, add a new record.

   A new user list record appears.

3. Enter a name for the user list. Optionally, change the default entry for Group Type.
4. Click Save.

Modifying a User List

You can modify a user list by adding or deleting users.

To add users to a user list

1. Choose View > Site Map > Group Administration > User Lists.

   The User Lists list appears.

2. In the User Lists list, select a user list.
3. In the Users list at the bottom of the view, add a new record.
4. Select one or more users, and then click OK.

   The selected users appear in the Users list. If a user, such as a customer user, belongs to an account, the Account field populates automatically.

You can delete users from a user list similarly.

Administering Access Groups

You can group parties of types Position, Organization, Household, and User List into access groups for the purpose of controlling their individual members' access to data.

You administer access groups in the Group Administration screen by choosing View > Site Map > Group Administration > Access Groups. This screen contains the Access Groups tree and the Access Groups list.

The Access Groups tree lists all access groups on the second level of the tree. Each access group can be expanded to show its 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 292 and "Access-Group Access Control" on page 320.

Creating an Access Group

You can create an access group in the Group Administration screen.

To create an access group

1. Choose View > Site Map > Group Administration > Access Groups.

   The Access Groups tree and the Access Groups list appear.

2. In the Access Groups list, add a new record.

   A new access group record.

3. Complete the following fields, using the guidelines provided in the following table, and then click Save.

Field	Guideline
Name	Required. Provide a name for the access group.
Group Type	Pick Access Group or Partner Community. These labels denote conceptual differences. Functionally, they are the same.
Parent Access Group	Specify a parent access group from which this new group inherits access to data that the parent group has access to.

The new access group also appears in the Access Groups tree.

Modifying an Access Group

You can modify an access group by adding or deleting members.

To add members to an access group

1. Choose View > Site Map > Group Administration > Access Groups.

   The Access Groups list appears.

2. In the Access Groups list, select an access group.
3. In the Members list, add a new record.

   A pop-up list appears that contains positions, organizations, accounts, 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, click Save.

You can delete members from an access group similarly.

Modifying an Access Group Hierarchy

You can modify the hierarchy of an access group by changing an access group's parent.

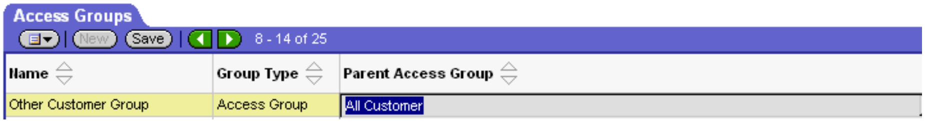
To modify a hierarchy of access groups

1. Choose View > Site Map > Group Administration > Access Groups.

   The Access Groups list appears.

2. In the Access Groups list, select an access group.
3. Click on the Parent Access Group field.

   The text box becomes editable and its entry is highlighted, as shown below.



Name	Group Type	Parent Access Group
Other Customer Group	Access Group	All Customer

4. Do one of the following to modify the hierarchy:

- To make the access group the top node of its own hierarchy, delete the entry in the Parent Access Group field, and then click Save.
- 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. Choose View > Site Map > Catalog Administration > Access Groups.

   The Catalogs list appears.

2. Select a catalog.
3. In the Access Groups list, add a new record.

   A pop-up list appears that contains access groups.

4. Select an access group, and then click Add.

   The access group appears in the Access Groups list.

5. In the Access Groups list, click Save.
6. Select an access group, and then click Add.

   The access group appears under the Access Group tab.

7. Complete the following fields, using the guidelines provided in the following table, and then click Save.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer the catalog.
Cascade	Set this flag to automatically associate this access group with the catalog's 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. Choose View > Site Map > Catalog Administration > Access Groups.

   The Catalogs list appears.

2. Drill down on a catalog name.

   The Categories list for the catalog appears.

3. Click the Access Groups view tab.
4. In the Access Groups list, add a new record.

   A multi-value group appears that lists access groups.

5. Select an access group, and then click Add.

   The access group appears in the Access Groups list.

6. In the Access Groups list, click Save.
7. Select an access group, and then click Add.

   The access group appears under the Access Group tab.

8 Complete the following fields, using the guidelines provided in the following table, and then click Save.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer this category.
Cascade	Set this flag to automatically associate this access group with this category's 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.

CAUTION: Procedures in this section must be performed after installing all applicable maintenance releases, and then patching the repository and importing additional seed data. For more information, refer to the relevant content in the *Maintenance Release Guide* for your Siebel products.

Administrators can use the Responsibilities view (Responsibility Detail - Tab Layout View) in the Application Administration 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 (View > 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, refer to *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.

NOTE: Tab layouts can be managed through roles instead of responsibilities. For more information, see "Creating and Administering Roles" on page 377.

Administering Tab Layout

To manage tab layouts, navigate to Application Administration > 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 375.

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 and choose View > Site Map > Application Administration > Responsibilities.
2. In the Responsibilities list, select the responsibility you want to associate tab layouts with.
3. Click the Tab Layout view tab.
4. In the Tab Layout list, select an application associated with the responsibility.
5. The Screen Tab Layout list displays all the screens used by the selected application:
   - **a** Select the Hide check box for any screens whose screen tabs will not be displayed.
   - **b** Change the numbers in the Order field to change the sequence in which the screen tabs are displayed.
6. Select each record in the Screen Tab Layout list, and the View Tab Layout list displays all the views for that screen:
   - **a** Select the Hide check box for any views whose view tabs will not be displayed.
   - **b** Change the numbers in the Order field to change the sequence in which the screen tabs are displayed.

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 User Administration 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. To make sure that tab layout defaults are available to your users, it is recommended that Siebel Dedicated Web Client deployments be configured to access the Siebel File System on the server rather than to use a local Siebel File System. For more information, refer to the `FileSystem` configuration parameter described in *Siebel Web Client Administration Guide*.

Exporting Tab Layouts

This section provides the procedure for exporting tab layouts to an XML file.

To export tab layouts

1. Navigate to Application Administration > 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. Navigate to Application Administration > 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 view in Application Administration, or you can modify the XML file and reimport it.

Creating and Administering Roles

Siebel applications administrators can create roles to enhance the usability of Siebel applications by tailoring the product to groups of users. Administrators use views in the Group Administration screen to create and administer roles.

NOTE: Do not confuse roles defined in the Siebel application interface with roles defined by an LDAP or ADS directory attribute. Roles in LDAP or ADS directories are collections of responsibilities that strictly enforce access to views and data records within Siebel applications. For information about roles defined in LDAP or ADS directories, see "Roles" on page 167.

When you create roles and assign users to these roles:

- Users have a task list for their role on their home page, with hyperlinks that take them directly to the views they use most frequently.
- Administrators can base personalization on role. For example, they can hide applets or display messages in salutation applet based on role.

- Roles can be used instead of responsibilities defining default tab layouts, and users only see the screen tabs and view tabs for their primary role.

NOTE: Tab layouts are primarily managed through responsibilities, as described in "Managing Tab Layouts Through Responsibilities" on page 372. To manage them through roles instead, set the parameter `EnableRoleTabLayout` to `TRUE` in the [SWE] section of your application configuration file, such as siebel.cfg. Setting the parameter as described renders the view Responsibility Detail - Tab Layout View ineffective. Customers can optionally disable this view.

To define a role in the application interface, you might create a role named Sales Representative. You would associate it with a list of tasks that sales representatives commonly perform, such as a task named View and Update Opportunities. Then you can associate users with the role of Sales Representative.

The home page for these users would include an applet with the title Tasks, which would have hyperlinks that take them directly to the views they use to perform these tasks. For example, in the Sales Representatives Tasks list of the home page, they could click View and Update Opportunities to go directly to the view they use to add an opportunity.

The home page can also be configured to display a salutation with an operational message based on the role, an analytics report specified for the role, and alerts targeted to specific roles. Use the Personalization Administration screen to personalize the home page based on the user's primary or non-primary roles.

To use roles, you must:

- Create roles
- Associate tasks with each role
- Assign users to roles in one of two ways:
  - Associate employees with roles in the User Administration, Employee Administration, or Partner Administration view.
  - Make roles available to partner companies, so delegated administrators can associate partner employees with roles. For more information, see *Siebel Partner Relationship Management Administration Guide*.

Creating Roles

You should create roles that represent the functional positions of a Siebel user in your business model, such as Sales Representative, Sales Manager, and Compensation Specialist. You can create roles that are appropriate for both employees and partner employees.

To create a role

1. Log in as an administrator and choose View > Site Map > Group Administration > Roles.
2. In the Roles list, click the New button, and enter information about the role in the new record.

Field	Guideline
Name	Enter the name of the role.
Description	Optionally, enter a description of the task for your own use.
Organization	Click the select button and choose all of the organizations where this role will be available. Add partner organizations here only if you want delegated administrators to be able to assign the role to new partner users.
Activation	Optionally, enter the date when this role will become available for use.
Expiration	Optionally, enter the last date when this role will be available for use.

Associating Tasks with a Role

After creating a role, enter the tasks commonly performed by employees who have that role, which you want to appear in the task list on the home page for these employees.

For each task, enter a caption and select an image file. These will be displayed as a hyperlink in the task list. Enter a description, which will also be displayed in the task list, underneath the caption.

In addition, for each task, specify the view where the task is performed. When the user clicks on the hyperlink for this task on the home page, this view will appear.

To associate tasks with a role

1. Log in as an administrator and choose View > Site Map > Group Administration > Roles.
2. In the Roles list, select the role you want to associate tasks with.
3. Click the Tasks view tab.
4. In the Tasks list, add a new record for each task associated with this role, and enter information about each task in the new records.

Field	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 role on the home page. If this field is left blank, tasks will be displayed in the order that you list them here.
Image	Select the graphic image that will be displayed as a hyperlink to the left of this task in the task list.
Group	This field is be used if search specifications are applied to filter the tasks that will be displayed in the task applet, if multiple task applets are associated with the role.

Associating Users with Roles

After a user is associated with a role, that user will see the tasks of that role in the home page applet.

You associate employees (or other types of users) with the roles using the User Administration screen.

You can also associate partner employees with roles using the User Administration screen. If you work with multiple employees of a single partner company, use the Partner Administration screen to display all the employees of a partner company.

To associate an employee or user with a role

1. Log in as an administrator and choose View > Site Map > User Administration > Employees.

   You can also use the following views to associate users with roles:

   - View > Site Map > User Administration > Users
   - View > Site Map > Partner Administration > Registered Partners > User Assignments

2. In the Employees list, select the record of the Employee you want to associate with a role.
3. In the More Info form, click the show more button.
4. In the More Info form, in the Role field, click the select button.
5. In the Role dialog box, if the role you want is not already in the Role list, click New and use the Add Roles dialog box to select the role.
6. In the Role dialog box, select the role you want to associate with the employee, make sure it is selected as the primary role, and click OK.

To associate a partner employee with a role

1. Navigate to the Partner Administration screen.
2. From the Show drop-down list, choose Registered Partners.
3. In the Partners list, select the partner company whose employees you want to associate with roles.
4. Click the User Assignments view tab.
5. In the User Assignments list, in the Role field, click the select button.
6. In the Role dialog box, if the role you want is not already in the Role list, click New and use the Add Roles dialog box to select the role.

7 In the Role dialog box, select the role you want to associate with the employee, make sure it is selected as the primary role, and click OK.

Creating Role-Based Personalization

You can use roles to define which applets appear on an application home page. This allows you to:

- Vary applets based on job function
- Avoid complicated home pages
- Optimize performance by minimizing unnecessary applets

The following is an example of restricting the Calendar Home Page To Do List based on roles. You can use it as a model for role-based personalization in your own applications.

To configure the Calendar Home Page To Do List applet based on roles

1 Log in as an administrator and choose View > Site Map > Personalization Administration > Applets.

   A list of applets appears.

2 Select the Calendar Home Page To Do List applet.

3 Change the Conditional Expression to the following:

```
GetProfileAttr("Primary User Role Name") IS NULL OR
GetProfileAttr("Primary User Role Name") = 'Field Sales
Representative' OR GetProfileAttr("Primary User Role Name")=
'Sales Operations' OR GetProfileAttr("Primary User Role Name")
= 'Consultant' OR GetProfileAttr("Primary User Role Name")
= 'Project Manager'
```

   This example restricts the Calendar Home Page To Do List applet to users not associated with any role or users associated with one of the following roles: Field Sales Representative, Sales Operations, Consultant, or Project Manager.

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 *Siebel Tools Reference*.

There are often circumstances where you need greater flexibility when determining what data should be shown in pop-up pick applets. For example:

- Most employees of your company only need to see positions for your organizations when they are assigning a sales representative to the sales team.
- Partner Managers need to see positions for your organization, as well as the partner organizations that they manage.

There are also many scenarios where your partners should have more restrictive visibility than your employees.

In order to meet this business requirement, Siebel eBusiness Applications have three capabilities that allow the developer to override the visibility set in the Business Component Popup Visibility Type property at the business component level in favor of another setting. The developer can:

- Set visibility of the Pick-List Object

- Use the visibility Auto All property
- Use the Special Frame Class and User Property

Setting Visibility of the Pick List Object

Developers can override the visibility set at the business component level by setting a different visibility type on the Pick List object, in the Visibility Type property.

When you do this, you override the visibility set at the business component level in a specific instance of that business component for all users of that instance.

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 PRM 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 Personal visibility view 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.

Troubleshooting Security Issues A

This section provides troubleshooting tips and information about security-related issues that may occur in Siebel eBusiness Applications.

Monitoring Application and User Activity

Siebel Systems provides log files, usage records, and statistics pages you can use to monitor activity and troubleshoot potential problems. To help maintain system security, it is recommended that you periodically check these records.

Siebel Web Server Extension Stats Page

The stats page provides information about the Siebel Web Server Extension (SWSE). Siebel administrators can use this page to have a better understanding of how the Web server is being used. For example, an administrator can periodically check the stats page to make sure network activity matches expectation and there are no unplanned or excessive activities that could signal a security issue.

Securing the Stats Page

Because the stats pages provides sensitive information about the type of requests running and potentially current active sessions, it is strongly recommended that this page be protected by the Web server (or a third party) authentication mechanism.

Accessing the Stats Page

By default, you can access the stats page at the following location:

```
http://host_name/application/stats.swe
```

Where *host_name* is the name of the host machine where the application is installed and *application* is the installation directory for the application.

Setting the Location of the Stats Page

You can change the location of the stats page, by editing the following item in the eapps.cfg file:

```
[SWE]

StatsPage = path/filename.swe
```

NOTE: The stats page must have the extension `.swe`.

For example, if the eapps.cfg file has the following entry:

```
[SWE]

StatsPage = /local/SiebelStats.swe
```

use the following URL to access the page:

```
http://host_name/application/local/SiebelStats.swe
```

In addition to the `StatsPage` parameter, you can enable or disable the Session Monitor. For example:

```
SessionMonitor = True
```

When the session monitor is enabled, statistics on all current sessions are collected and reported on the application’s stats page. This allows administrators to determine who is logged onto the system at any given time.

When the session monitor is disabled, sessions are not monitored by the statistical repository and will not be displayed in the application’s stats page.

NOTE: System performance is slightly degraded when the session monitor is enabled.

Viewing and Setting Contents of the Stats Page

When you view the stats page, you can configure the contents of the page by setting the Verbose option as part of the stats page address.

This option allows you to set the amount of information displayed on the page. Verbosity settings include:

Option	Description
Verbose = Low	This is the default. Displays only system- and application-level settings.
Verbose = Medium	Displays all of the above, plus Lock statistics.
Verbose = High	Displays all of the above, plus all currently active operations to the Siebel Server.

In addition to the Verbose option, you can configure a Reset option for the page. Reset values include:

Option	Description
Reset = True	Statistics for all non-counter and current operations are reset after viewing.
Reset = False	These statistics are not reset.

The following are some examples of request calls to the stats page:

```
http://host_name/application/SiebelStats.swe?Verbose=High&Reset=True
```

This request will display stats for the following categories: System, Applications, Current Sessions, Locks, and Current Operations Processing. Once the stats are viewed, all non-counter and current operations statistics will be reset.

```
http://host_name/application/SiebelStats.swe?Reset=True
```

This request displays stats for the following categories: System and Applications. Once the stats are viewed, all non-counter and current operations statistics will be reset.

Viewing Usage of Employee and Partner Applications

The Named User Monitor view contains a usage history record for each Siebel application running. The usage history record shows a running total of all named users who have logged into the application. The total is initialized at zero and incremented each time a new user logs on.

The usage history record for each application has a set of user log records associated with it: one user log record for each user ID who has logged into the application.

License Tracking scans for login identifiers every 5 minutes. Any login IDs not previously encountered are added to the User Log list for the application.

When a user's login is deactivated, the user log record is automatically deleted from the Named User Monitor view. For information about deactivating employees, see "Deactivating an Employee" on page 267.

To view named users

1. From the application-level menu, choose View > Site Map > Application Administration > Named User Monitor.
2. In the Usage History list, select the record for the application you want to review.

   Some fields are described in the following table.

Field	**Comment**
Limit Exceeded?	Yes or No.
Application/Module	The name of the Siebel application being monitored, for example Siebel Sales.
# of Named Licenses	The number of named-user licenses purchased for the application.
# of Named Users	Total number of named users who have logged on to date. An exception is flagged when this number exceeds the # of Named Licenses.

3 In the User Log list, review the log records associated with the record selected in Step 2.

Some fields are described in the following table.

Field	Comment
Login ID	User ID for login.
First Login	The first day and time a client logged into the application.
Last Login	The date and time of the user’s most recent login.

User Authentication Issues

This section describes problems that may occur when authenticating users.

User is unable to work in the Server Administration screen

The server administration component performs its own authentication by verifying that the Siebel user ID it gets from the Application Object Manager is the user name for a database account. 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 Server Administration screen; or, if the system is configured to allow this, audit trail problems may occur.

To allow administrator users to work in the Server Administration screen (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 Application Object Manager or a Siebel Dedicated Web Client—in each case, database authentication must be configured. For more information about database authentication, see “Database Authentication Overview” on page 97 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 SecExternalUserAdministration system preference is set to `FALSE`. For more information, see "System Preferences" on page 209.

Having trouble using database authentication for Mobile Web Clients

Check to see if password encryption is enabled for the client. You cannot use database encryption if you have enabled password encryption because this would require the Mobile Web Client to use an encrypted password to log into the local database.

Having trouble running the LDAP/ADSI Configuration Utility

Try running the utility from the machine that hosts the Siebel application you want to configure. The utility works best if run locally, rather than over the network.

Responsibilities in the directory conflict with responsibilities in Siebel applications

It is recommended that you assign user responsibilities in the directory or by using a Siebel application, but not both. For more information, see "Roles" on page 167.

Upgrading my Siebel application appears to disable checksum validation

You must recalculate the Security Adapter CRC checksum value whenever you upgrade your Siebel applications. For more information, see "Checksum Validation" on page 179.

"Web Authentication Failed" error message appears in an application log file

If your installation is configured for Web SSO (without anonymous browsing) and the `ProtectedVirtualDirectory` parameter is not set, this message may appear.

To fix this error, set the `ProtectedVirtualDirectory` parameter in the eapps.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 Workflow Administration screen

Your server or application is probably running on a different language from the database. For example, a DEU installation is running against an ENU database.

Check your setup. Using Server Manager, connect to the server and run `list param lang` to verify. If the language code is incorrect, you can run `change parameter lang=`*`language_code`*, where *`language_code`* is your three-letter database language code. Restart the server.

When I click New User, either nothing happens or an error appears

Possible causes include:

- One or more of the necessary User Registration workflows have not been activated.
- The language of your application setup does not match the language of the database.
- The workflow is not activated properly.

To correct this problem:

- Activate the workflow processes described in “Activating Workflow Processes” on page 229.
- Using Server Manager, connect to the server and run `list param lang` to verify. If the language code is incorrect, you can run `change parameter lang=`*`language_code`*, where *`language_code`* is your three-letter database language code. Restart the server.

When I click Finish, an “Error updating business component at step ‘Insert New User’” message appears

The problem is often that the user being created already exists in the LDAP directory server. The LDAP directory server is not refreshed and is shared by everyone. The user you are trying to create may be new to the database but may already exist in the LDAP directory. This problem commonly occurs if the directory is not refreshed after deployment testing.

Try to create another user or use the LDAP console to check whether the user exists in the directory. Connect to the LDAP server, but instead of creating a new user, right-click on People and select Search.

After I click Finish, the “View not accessible” message appears

The user was successfully created and was able to log in. However, the user that was created did not receive the appropriate responsibility and cannot access the view.

Change the New Responsibility field for the Anonymous User of the application to one that contains the necessary views.

When I click the New User link, nothing happens

Most likely, some or all of the User Registration workflow processes have not been activated; or if they are, the server needs to be restarted.

In the Server Administration screen, restart only the necessary Application Object Managers. Restarting the server will also work.

When I click Next in a User Registration view, nothing happens

There may be another workflow that is being triggered and is disrupting the User Registration workflow. It is also possible that not all necessary workflows have been activated. You must activate all the necessary workflows.

To deactivate a disruptive workflow:

- In the Runtime Events Administration screen, click the Events view.
- Query for Object Name is null. Aside from some application type events, there should be nothing else. In particular, be wary of any records whose Action Set Name begins with “Workflow.” Such a record indicates that the workflow is triggered every time the event specified in the Event field happens. This can be particularly disruptive if the event is common, such as ShowApplet or WriteRecord. The Object Name normally constrains the actions to trigger only when the specified event occurs within the context of the object; for example, a specific business component or applet.

- If there is a suspicious Event, drill down on the Action Set Name and note the ID following the string ProcessId in the Business Service Context field. Query against the database to find the suspect workflow: select NAME from S_WF_STEP where ROW_ID = '*xxx*', where *xxx* is the previously noted ID.

  That workflow is the disruptive one. Deactivate it.

When I click Finish, an error is returned

Possible causes include:

- The SecExternalUserAdministration system preference is not set to `FALSE`.
- The SecThickClientExtAuthent system preference is not set to `TRUE`.
- The server has not been restarted since setting the system preferences. For information about the system preferences related to user authentication, see "System Preferences" on page 209.

Check to see if the user exists in the Person view in the User Administration screen. If the user exists but was not given an entry in the LDAP server, then that user would not be able to log in. You can also verify this by trying to create a user in the User view. If you can set the user ID and password, try to log in as that person.

Access Control Issues

This section describes problems related to access control.

Employee user has trouble logging into a Siebel customer application

It is not recommended to use an Employee login account to access a customer application (such as Siebel eBrokerage). 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" on page 337.

Encryption Issues

This section describes problems related to encryption.

Having trouble encrypting numeric data with RC2 encryption

Siebel Systems does not support RC2 encryption for numeric data. To encrypt a calculated numeric field, map the field to a string field, and then set the encryption property of the string field to true.

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

Seed Data B

When you install your Siebel eBusiness Applications, you are provided seed data that is related to authentication and to user access to Siebel applications. This section includes instructions for using these seed data.

In the tables in this section, the term “customer applications” represents the group of Siebel eSales, eAuction, eService, eCustomer, eTraining, eEvents, and eMarketing.

Seed Employee

One Employee record is provided as seed data at installation, as described in Table 23. 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 “Name Server Parameters” on page 205.

For information about organization access control, see "About Access Control Mechanisms" on page 309.

Table 23. 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 24 describes non-employee User records provided as seed data.

Table 24. 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	PRM Partner Portal

Seed Responsibilities

Responsibility records are provided as seed data, as described in Table 25. 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 a list of responsibilities provided in seed data, refer to the *Release Notes* for your Siebel products.

Table 25. 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
eAuction Registered Bidder	Default Organization	Views for eAuction registered bidder	eAuction
eAuction Registered Lister	Default Organization	Views for eAuction registered lister	eAuction
eAuction Auction Administration	Default Organization	Views for administering auctions, catalogs, and categories, but not for administering users	eAuction

Table 25. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
Unregistered Partner Agent	Default Organization	Views provided for anonymous browsing	PRM Partner Portal
Self-Registered Partner Agent	Default Organization	Limited set of views provided for a user who self-registers	PRM Partner Portal
Partner Relationship Manager	Default Organization	Views for PRM Partner Portal partner relationship manager	PRM Partner Portal
Partner Operations Manager	Default Organization	Views for PRM Partner Portal partner operations manager, including views for administering users	PRM Partner Portal
Partner Sales Manager	Default Organization	Views for PRM Partner Portal partner sales manager	PRM Partner Portal
Partner Sales Rep	Default Organization	Views for PRM Partner Portal partner sales rep	PRM Partner Portal
Partner Service Manager	Default Organization	Views for PRM Partner Portal partner service manager	PRM Partner Portal
Partner Service Rep	Default Organization	Views for PRM Partner Portal partner service rep	PRM 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	eTraining
Training Administrator	Default Organization	Views that allow administration of courses and enrollees	eTraining

To see the views included in a responsibility

1. Navigate to the Application Administration screen.
2. From the Show drop-down list, select Responsibilities.

3 In the Responsibilities list, select a responsibility.

The views for the responsibility appear in the Views list.

Seed Position and Organization

The Proxy Employee Position and the Default Organization Division records are provided as seed data. The position exists within the division, and the division is its own organization. The position and division are both assigned to the seed data Employee record.

Seed Database Login

One database login is provided as seed data. It is intended to be used for all users logging in through an external authentication system, and should not be assigned to any individual user.

The login credentials are login = LDAPUSER and password = LDAPUSER. It is strongly recommended that an administrator change the password.

Addendum for Siebel Financial Services C

This section 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.

The applications listed in Table 26 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.

Throughout this guide, information is categorized for employee, partner, and customer applications.

Table 26. 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 eFinance Siebel eInsurance Siebel eHealthcare Siebel Teller Siebel Teller Officer
Siebel Financial Services ERM	Employees		Siebel Employee Relationship Management
Siebel Financial Services Marketing	Employees	Siebel Marketing only	Siebel eFinance Siebel eInsurance Siebel eHealthcare

Table 26. Siebel Financial Services Applications

Tools Application Object Name	Users	Options	Products
Siebel FINS Service Wireless	Employees	Siebel Service only	Siebel Wireless eFinance Siebel Wireless eInsurance
Siebel FINS Sales Wireless	Employees	Siebel Sales Siebel Call Center Siebel Partner Manager	Siebel Wireless eFinance Siebel Wireless eInsurance
Siebel Financial Partner Relationship Management (PRM)	Partners		Siebel PRM for Finance Siebel Agent Portal Siebel eHealthcare Group Portal Siebel eHealthcare Provider Portal
Siebel eBanking	Customers		Siebel eBanking
Siebel Financial eBrokerage	Customers		Siebel eBrokerage
Siebel Financial eService	Customers		Siebel Insurance/ Healthcare eService
Siebel Financial eEnrollment	Customers		Siebel eHealthcare Member Enrollment Portal
Siebel FINS eSales	Customers		Siebel eSales
Siebel Financial eCustomer	Customers		Siebel eCustomer
Siebel eEvents Management	Customers		Siebel eEvents for Finance
Siebel Banking Wireless	Customers		Siebel Wireless Banking and Brokerage

NOTE: Siebel eHealthcare Group Portal is used as a customer product; that is, users are typically your customers. Technically, Siebel eHealthcare 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 applications group that provide self-registration and external administration of users as default functionalities, see "Registering and Administering Users for Siebel Financial Services" on page 410.

Implementing LDAP and ADSI Security Adapter Authentication

Implementation of Siebel 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 eEvents 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 eEvents 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 399.

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 418 and "Seed Data" on page 399.

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 eEvents 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 eEvents 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 399.

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 418 and "Seed Data" on page 399.

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 and authentication parameters for an application appears once, in either the eapps.cfg file or in the eapps_fins.cfg file.

Table 27 lists the sections in the eapps.cfg file and in the eapps_fins.cfg file, which are provided for Siebel Financial Services applications.

Table 27. 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 FINS Service Wireless		`[/finswpserv]`
Siebel FINS Sales Wireless		`[/finswpsales]`
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 Banking Wireless		`[/wpbanking]`

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 417.

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 eEvents 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 eEvents 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 399.

For information about seed data specific to Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 418.

Unregistered Users and Anonymous Browsing

Anonymous browsing is a default functionality for the following Siebel Financial Services applications:

- Siebel Employee Relationship Management

- Siebel eEvents for Finance
- Siebel Financial PRM
- Siebel eBanking
- Siebel eBrokerage
- Siebel FINS eSales
- Siebel eHealthcare Member 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 418.

Self-Registration

User self-registration is a 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 Financial PRM
- Siebel eEvents for Finance
- Siebel eBanking
- Siebel eBrokerage
- Siebel FINS eSales

A user can self-register in Siebel Financial 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 Partner Administration screen in Siebel Financial Services to promote a prospective partner to approved partner and then to registered partner.

For information about using the Partner Administration 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 Partner Administration screen in Siebel Financial Services.

For information about using the Partner Administration screen, see *Siebel Partner Relationship Management Administration Guide*.

External Administration of Users

Delegated administration is a 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 399. 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.

Parties

Household is an additional party type. Table 28 augments the table describing parties in remaining sections of this guide.

Table 28. Parties

Party Type	Party	Examples	Distinguishing Features
Household	Household	■ A group of family members who reside at the same address ■ 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. It may have any combination of contacts, users, employees, and partner users as members. ■ An individual can belong to more than one household.

Access Control Mechanisms

The following note affects access control to Opportunities in any view that uses personal, position-based, or organization-based 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-based 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 section augments the sections on administering various party types.

Administering Households

You must do the following administrative tasks with households:

- Create households.
- Associate contacts with households.
- Maintain household data.

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. Choose View > Site Map > Catalog Administration > 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 Choose View > Site Map > Catalog Administration > 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 29 contains the names of application configuration files that are used by Siebel Financial Services applications.

Table 29. 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 FINS Service Wireless	finswpserv.cfg
Siebel FINS Sales Wireless	finswpsales.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
Siebel Banking Wireless	wpbanking.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 399 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 26 on page 405.

Seed Users

Table 30 shows modifications to the seed non-employee User records that are provided with Siebel Financial Services applications.

The GUESTCP seed User record, which is documented in “Seed Data” on page 399, 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 30. 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 31 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 the seed responsibilities for partner users.

Table 31. 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 eEvents for Finance. For Siebel eEvents 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 eEvents for Finance. For Siebel eEvents for Finance, use Web Registered User instead.
Registered Customer - Wireless Banking	Default Organization	Views provided for a registered user on a wireless device.	Siebel Banking Wireless.
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 "Access Control" on page 287.

Index