Siebel Security Guide

Siebel Innovation Pack 2014
November 2014

ORACLE

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Contents

Chapter 1: What's New in This Release

Chapter 2: About Security for Siebel Business Applications

About This Guide 17

General Security Concepts 18

Industry Standards for Security 18

About Supported Security Products 20

Siebel Security Architecture 20

- User Authentication for Secure System Access 20
- End-to-End Encryption for Data Confidentiality 23
- About Controlling Access to Data 25
- Support for Auditing in a Siebel Environment 26
- Secure Physical Deployment to Prevent Intrusion 27
- Security for Mobile Solutions 28
- Security Settings for the Web Browser 29

Web Sites with Security Information 29

Roadmap for Configuring Security 29

About Siebel Open UI 30

Chapter 3: Changing and Managing Passwords

About Managing and Changing Passwords 33

About Default Accounts 36

Changing System Administrator Passwords on Microsoft Windows 37

Changing the Siebel Administrator Password on UNIX 40

Changing the Table Owner Password 42

Troubleshooting Password Changes By Checking for Failed Server Tasks 43

About the Gateway Name Server Authentication Password 44

Changing the Siebel Enterprise Security Token 45

Encrypted Passwords in the eapps.cfg File 46

Encrypting Passwords Using the encryptstring Utility 47
About Encryption of Gateway Name Server Password Parameters 48

Chapter 4: Communications and Data Encryption

Types of Encryption 52
- Communications Encryption 52
- Data Encryption 55

Process of Configuring Secure Communications 56
About Certificates and Key Files Used for SSL or TLS Authentication 57
Installing Certificate Files 59
Configuring SSL Mutual Authentication 62
About Configuring Encryption for a Siebel Enterprise and SWSE 63
About Key Exchange for Microsoft Crypto or RSA Encryption 64
Configuring SSL or TLS Encryption for a Siebel Enterprise or Siebel Server 65
Configuring SSL or TLS Encryption for SWSE 68
Enabling TLS Acceleration for Web Server and Web Client Communications 71
About Configuring Encryption for Web Clients 72
Configuring Encryption for Mobile Web Client Synchronization 73
About Data Encryption 74
- How Data Encryption Works 74
- Requirements for Data Encryption 75
- Encrypted Database Columns 76
- Upgrade Issues for Data Encryption 77

Configuring Encryption and Search on Encrypted Data 77
Managing the Key File Using the Key Database Manager 80
- Adding New Encryption Keys 81
- Changing the Key File Password 81

About Upgrading Data to a Higher Encryption Level 82
Process of Upgrading Data to a Higher Encryption Level 83
- Requirements for Upgrading to a Higher Encryption Level 83
- Modifying the Input File 84
- Running the Encryption Upgrade Utility 86

About Siebel Strong Encryption 87
Implementing Siebel Strong Encryption 88
Increasing the Encryption Level 89

Reencrypting Password Parameters in the Siebns.dat File 92
Security Considerations for Unicode Support 95

Chapter 5: Security Adapter Authentication

About User Authentication 97
Comparison of Authentication Strategies 99
About Siebel Security Adapters 100
About Database Authentication 102
Implementing Database Authentication 103
Implementing Database Authentication with MS SQL Server 104
About LDAP or ADSI Security Adapter Authentication 106
LDAP and ADSI Security Adapter Authentication Process 106
Directory Servers Supported by Siebel Business Applications 107
Comparison of LDAP and ADSI Security Adapters 107
Requirements for the LDAP Directory or Active Directory 111
About Setting Up the LDAP Directory or Active Directory 112
Verifying the Active Directory Client Installation 114
About Installing LDAP Client Software 115
Process of Installing and Configuring LDAP Client Software 116
Considerations if Using LDAP Authentication with SSL 116
Installing the LDAP Client Software on Windows 117
Installing the LDAP Client Software on UNIX 117
Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client 119
Creating a Wallet for Certificate Files When Using LDAP Authentication with SSL 121
Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard 123
Process of Implementing LDAP or ADSI Security Adapter Authentication 128
Requirements for Implementing an LDAP or ADSI Authentication Environment 130
About Creating a Database Login for Externally Authenticated Users 131
Setting Up the LDAP Directory or Active Directory 131
Creating Users in the LDAP Directory or Active Directory 132
Adding User Records in the Siebel Database 134
Setting Security Adapter Parameters in the SWSE Configuration File (eapps.cfg) 135
Configuring Security Adapter Gateway Name Server Parameters 137
Configuring LDAP or ADSI Authentication for Developer Web Clients 141
Restarting Servers 143
Testing the LDAP or ADSI Authentication System 143

About Migrating from Database to LDAP or ADSI Authentication 145

Security Adapter Deployment Options 146

- Configuring the Application User 147
- Configuring Checksum Validation 149
- Configuring Secure Communications for Security Adapters 150
- Configuring the Shared Database Account 151
- Configuring Adapter-Defined User Name 154
- Configuring the Anonymous User 155
- Configuring Roles Defined in the Directory 157

About Password Hashing 158

Process of Configuring User and Credentials Password Hashing 160

- Guidelines for Password Hashing 160
- Configuring User Password Hashing 161
- Configuring Password Hashing of Database Credentials 162

Running the Password Hashing Utility 163

About Authentication for Gateway Name Server Access 165

Implementing LDAP or ADSI Authentication for the Gateway Name Server 166

Security Adapters and the Siebel Developer Web Client 167

About Authentication for Mobile Web Client Synchronization 170

About Securing Access to Siebel Reports 172

Chapter 6: Web Single Sign-On Authentication

About Web Single Sign-On 173

About Implementing Web Single Sign-On 174

Web Single Sign-On Authentication Process 176

Requirements for Standards-Based Web Single Sign-On 177

Set Up Tasks for Standards-Based Web Single Sign-On 178

Requirements for Microsoft Windows Integrated Authentication 179

Process of Implementing Windows Integrated Authentication 180

- Requirements for the Example Windows Integrated Authentication Environment 181
- Setting Up Active Directory to Store Siebel User Credentials for Windows Integrated Authentication 181
- Configuring the Microsoft IIS Web Server for Windows Integrated Authentication 182
- Creating Users in the Directory (Windows Integrated Authentication) 184
- Adding User Records in the Siebel Database 185

Setting Web Single Sign-On Authentication Parameters in the SWSE Configuration File 187
Setting Web Single Sign-On Authentication Parameters for the Gateway Name Server 188
Editing Web Single Sign-On Parameters in the Application Configuration File 189
Restarting Servers 190
Testing Web Single Sign-On Authentication 190
About Digital Certificate Authentication 191
Configuring the User Specification Source 192
Configuring the Session Timeout 193
Configuring Siebel CRM and Oracle BI Publisher for Web Single Sign-On 194
Configuring Siebel CRM for Integration with Oracle BI Publisher with Web Single Sign-On 195
Configuring Oracle BI Publisher for Integration with Siebel CRM with Web Single Sign-On 197
Enabling Reports Scheduling with Web Single Sign-On 197

Chapter 7: Security Features of Siebel Web Server Extension

Configuring a Siebel Web Client to Use HTTPS 201
Login Security Features 202
Implementing Secure Login 203
Logging Out of a Siebel Application 203
Login User Names and Passwords 204
Account Policies and Password Expiration 205
About Using Cookies with Siebel Business Applications 206
Session Cookie 207
Auto-Login Credential Cookie 210
Siebel QuickStart Cookie 211
Enabling Cookies for Siebel Business Applications 211

Chapter 8: User Administration

About User Registration 213
About Anonymous Browsing 214
Process of Implementing Anonymous Browsing 215
Anonymous Browsing and the Anonymous User Record 215
Setting Configuration Parameters for Anonymous Browsing 216
Configuring Views for Anonymous Browsing or Explicit Login 217
About Self-Registration 218

User Experience for Self-Registration 218

Process of Implementing Self-Registration 220

- Self-Registration and the Anonymous User Record 220
- Setting the PropagateChange Parameter for Self-Registration 221
- About Activating Workflow Processes for Self-Registration 222
- (Optional) Modifying Self-Registration Views and Workflows 224
- (Optional) Managing Duplicate Users 228

Identifying Disruptive Workflows 232

About Managing Forgotten Passwords 232

- Retrieving a Forgotten Password (Users) 233
- Defining Password Length for Retrieved Passwords 234
- Architecture for Forgotten Passwords 235
- About Modifying the Workflow Process for Forgotten Passwords 236
- Modifying Workflow Process to Query Null Fields 237
- Modifying Workflow Process to Request Different Identification Data 238

Internal Administration of Users 241

About Adding a User to the Siebel Database 241

- Adding a New Employee 242
- About Adding a New Partner User 244
- Adding a New Contact User 245
- Modifying the New Responsibility for a User Record 247

Delegated Administration of Users 248

- User Authentication Requirements for Delegated Administration 249
- Access Considerations for Delegated Administration 249
- Registering Contact Users (Delegated Administration) 250
- Registering Partner Users (Delegated Administration) 252

Maintaining a User Profile 253

- Editing Personal Information 254
- Changing a Password 254
- Changing the Active or Primary Position 255

Chapter 9: Configuring Access Control

About Access Control 258

- Access Control for Parties 260
- Access Control for Data 264

Access Control Mechanisms 266

- About Personal Access Control 266
- About Position Access Control 267
- About Single-Position Access Control 268

About Team (Multiple-Position) Access Control 268
About Manager Access Control 269
About Organization Access Control 271
About Single-Organization and Multiple-Organization Access Control 271
About Suborganization Access Control 273
About All Access Control 274
About Access-Group Access Control 275

Planning for Access Control 276
Access Control and Business Environment Structure 276
About Planning for Divisions 278
About Planning for Organizations 279
About Planning for Positions 280
About Planning for Responsibilities 282

Setting Up Divisions, Organizations, Positions, and Responsibilities 283

About View and Data Access Control 285

Listing the Views in an Application 286

Responsibilities and Access Control 287
About Associating a Responsibility with Organizations 288
Local Access for Views and Responsibilities 288
Read Only View for Responsibilities 289
Assigning a Responsibility to a Person 289
Using Responsibilities to Allow Limited Access to Server Administration Views 290

Viewing Business Component View Modes 291

Configuring Access to Business Components from Scripting Interfaces 295

Viewing an Applet's Access Control Properties 297

Listing View Access Control Properties 299

Example of Flexible View Construction 302

About Implementing Access-Group Access Control 304
Scenario That Applies Access-Group Access Control 304
Viewing Categorized Data (Users) 307

Implementing Access-Group Access Control 308
About Administering Catalogs of Data 308
Administration Tasks for Positions, Organizations, Households, and User Lists 309
Administering Access Groups 310
Associating Access Groups with Data 312

Managing Tab Layouts Through Responsibilities 315
Specifying Tab Layouts for Responsibilities 315
Assigning a Primary Responsibility 316

Exporting and Importing Tab Layouts 317
Managing Tasks Through Responsibilities 319
Administering Access Control for Business Services 321
Associating a Business Service with a Responsibility 322
Associating a Responsibility with a Business Service 323
Example of Associating a Responsibility with Business Service Methods 325
Clearing Cached Business Services 326
Disabling Access Control for Business Services 326
Administering Access Control for Business Processes 327
Clearing Cached Responsibilities 327
About Configuring Visibility of Pop-Up and Pick Applets 328
About Configuring Drilldown Visibility 330
Party Data Model 332
How Parties Relate to Each Other 333
Person (Contact) Data Model 334
User Data Model 334
Employee Data Model 335
Position Data Model 337
Account Data Model 338
Division Data Model 339
Organization Data Model 340
Partner Organization Data Model 341
Household Data Model 342
User List Data Model 343
Access Group Data Model 344

Chapter 10: Troubleshooting Security Issues

Troubleshooting User Authentication Issues 346
Troubleshooting User Registration Issues 348
Troubleshooting Access Control Issues 350

Appendix A: Configuration Parameters Related to Authentication

About Parameters in the eapps.cfg File 353
Authentication-Related Parameters in Eapps.cfg 355
SSL and TLS-Related Parameters in Eapps.cfg 360
Siebel Gateway Name Server Parameters 361
Parameters for Database Authentication 362

Parameters for LDAP or ADSI Authentication 364
Parameters for Custom Security Adapter Authentication 370
Parameters for Application Object Manager 371
Parameters in the Gateway.cfg File 372
Siebel Application Configuration File Parameters 376

Appendix B: Seed Data

Seed Employee 383
Seed Users 384
Seed Responsibilities 384
Listing the Views Associated with a Responsibility 385
Seed Position and Organization 386

Appendix C: Addendum for Siebel Financial Services

Siebel Financial Services Applications 387
User Authentication for Siebel Financial Services 389
User Registration and Administration for Siebel Financial Services 391
Seed Data 391
Unregistered Users and Anonymous Browsing 392
Self-Registration 392
Internal Administration of Users 393
External Administration of Users 393
Maintaining a User Profile 393
Basic Access Control for Siebel Financial Services 394
Access Control Mechanisms 394
Administration of Access-Group Access Control 394
Configuration File Names for Siebel Financial Services Applications 396
Seed Data for Siebel Financial Services 397
Seed Users 397
Seed Responsibilities 398

Index

1 What's New in This Release

What's New in Siebel Security Guide, Siebel Innovation Pack 2014

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

NOTE: Siebel Innovation Pack 2014 is a continuation of the Siebel 8.1/8.2 release.

Table 1. New Product Features in Siebel Security Guide, Siebel Innovation Pack 2014

Topic	Description
"Characters Supported in Siebel Passwords" on page 34	New topic. Lists the characters that are supported for Siebel passwords.
Changing Passwords in the Siebel Management Framework About Configuring SSL Encryption for the Siebel Management Framework	Deleted topics. Siebel Management Server and Siebel Management Agent are not supported for the current release. For more information, see the statement of direction on My Oracle Support, 1640801.1 (Article ID).
"About Encryption of Gateway Name Server Password Parameters" on page 48 "Reencrypting Password Parameters in the Siebns.dat File" on page 92	Modified topics. Passwords in the siebns.dat file on the Siebel Gateway Name Server are now encrypted using Advanced Encryption Standard (AES) encryption. If you are upgrading to the current release, you must reencrypt these password parameters.
"Using Secure Socket Layer v3.0 with Siebel CRM" on page 55	New topic. Secure Socket Layer (SSL) v3.0 communications encryption is not supported for environments with high-security requirements.
Various topics	Modified topics. Implement Transport Layer Security (TLS) communications encryption where possible.
"About Data Encryption" on page 74	Modified topic. Implement AES encryption using Siebel Strong Encryption for increased data security.
"LDAP and ADSI Security Adapter Authentication Process" on page 106	Modified topic. The Active Directory Services Interfaces (ADSI) security adapter, and the Lightweight Directory Access Protocol (LDAP) security adapter used with the Oracle LDAP Client, accept special characters in passwords.
"Comparison of LDAP and ADSI Security Adapters" on page 107	Modified topic. Password expiration warning functionality is supported with the LDAP security adapter on directory servers that implement the IETF password policy draft (09) standard.

Table 1. New Product Features in Siebel Security Guide, Siebel Innovation Pack 2014

Topic	Description
"ADSI Security Adapter Requirements" on page 111	Modified topic. Siebel Business Applications support authentication using Microsoft Global Catalog.
"About Installing LDAP Client Software" on page 115	Modified topic. If you install the Oracle Database Client provided with a Siebel Innovation Pack to enable LDAP authentication, you must also use this client to connect to your Oracle Database.
Using IBM LDAP Client Software	Deleted topic. Use the Oracle Database Client and Oracle Wallet Manager if you implement LDAP security adapter authentication with Siebel CRM.
"Enabling SSL for the Siebel LDAP Security Adapter" on page 122	Modified topic. Includes additional information about enabling SSL for the LDAP security adapter on a Windows platform.
"Retrieving a Forgotten Password (Users)" on page 233 "Defining Password Length for Retrieved Passwords" on page 234 "Architecture for Forgotten Passwords" on page 235	Modified topics. When using the Forgot Your Password feature, a user can enter the new password they want to use.
"Exporting and Importing Tab Layouts" on page 317	Modified topic. Added additional information about exporting and importing tab layouts for a responsibility from one Siebel environment to another.

Additional Changes

For Siebel CRM product releases 8.1.1.9 and later and for 8.2.2.2 and later, the system requirements and supported platform certifications are available from the Certifications tab on My Oracle Support. For information about Certifications, see article 1492194.1 (Article ID) on My Oracle Support.

What's New in Siebel Security Guide, Version 8.1/8.2

Table 2 lists the changes described in this version of the documentation to support this release of the software. The new features described in Table 2 are available in Siebel CRM version 8.1.1.11, Siebel CRM version 8.2.2.4, and later.

Table 2. New Product Features in Siebel Security Guide, Version 8.1/8.2

Topic	Description
"Configuring SSL Mutual Authentication" on page 62	Modified topic. The Transport Layer Security (TLS) protocol is not supported on the UNIX operating system for HTTPS calls to external Web servers.
"Directory Servers Supported by Siebel Business Applications" on page 107	New topic. It describes the directory servers that are supported by the LDAP and Active Directory Services Interfaces (ADSI) security adapters.
"About Installing LDAP Client Software" on page 115 "Process of Installing and Configuring LDAP Client Software" on page 116	Modified topics. These topics now describe how to install and configure the Oracle Database Client and Oracle Wallet Manager products, which replace the IBM LDAP Client and IBM GSKit as the default LDAP client software for Siebel Business Applications.
Using IBM LDAP Client Software	New topic. It is recommended that you use Oracle Database Client and Oracle Wallet Manager as your LDAP client software solution. If you choose to use the IBM LDAP Client software, certain restrictions apply.
"Parameters for Security Adapter (Profile/Named Subsystem)" on page 139 "Parameters for LDAP or ADSI Authentication" on page 364	Modified topics. If you are using the Oracle Database Client, then you must change the value of the Security Adapter Dll Name parameter from sscfldap.dll to sscforacleldap.dll.
"Storing Shared Database Account Credentials as Profile Parameters" on page 153 "Parameters for LDAP or ADSI Authentication" on page 364	Modified topics. You can store shared database account credentials defined for an Active Directory as profile parameters of the ADSI Security Adapter profile (alias ADSISecAdpt).

Additional Changes

Several topics were revised to improve the technical accuracy of this guide. The following topics provide additional information about Web Single Sign-On:

- "Configuring Internet Explorer for Windows Integrated Authentication" on page 179
- "Configuring the Session Timeout" on page 193
- "Configuring Siebel CRM and Oracle BI Publisher for Web Single Sign-On" on page 194

2 About Security for Siebel Business Applications

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

- About This Guide on page 17
- General Security Concepts on page 18
- Industry Standards for Security on page 18
- About Supported Security Products on page 20
- Siebel Security Architecture on page 20
- Web Sites with Security Information on page 29
- Roadmap for Configuring Security on page 29
- About Siebel Open UI on page 30

About This Guide

This guide provides recommendations for safeguarding your Siebel Business Applications deployment from internal (intranet) and external (Internet) security threats. The most important reason for securing an application is to protect the confidentiality, integrity, and availability of an organization's critical information. However, to protect your Siebel Business Applications data, you must secure both your Siebel Business Applications and the computing environment in which they run.

Siebel Security Hardening Guide and *Siebel Security Guide* (this book) provide the information you need to protect your Siebel Business Applications deployment:

- This guide, *Siebel Security Guide*, describes the Siebel security architecture and security concepts. It outlines the security controls provided by Siebel Business Applications, and gives detailed procedural information on how to implement these controls to secure your application.
- *Siebel Security Hardening Guide* provides general recommendations for securing Siebel Business Applications and their deployment environment (network, operating system, database). *Siebel Security Hardening Guide* provides detailed procedural information on implementing Siebel security controls only where such information is not provided elsewhere in the *Siebel Bookshelf*.

NOTE: The Siebel Bookshelf is available on Oracle Technology Network (http://www.oracle.com/technetwork/indexes/documentation/index.html) and Oracle Software Delivery Cloud. It might also be installed locally on your intranet or on a network location.

General Security Concepts

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

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

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

Classifications of security services include:

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

This guide describes security services available with Siebel Business Applications. These services are intended to counter security attacks; they use one or more security mechanisms to provide the service.

Industry Standards for Security

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

Supported standards include:

- **Lightweight Directory Access Protocol (LDAP) and Active Directory Service Interfaces (ADSI).** Siebel Business Applications provide preconfigured integration with LDAP and ADSI for user authentication purposes. For more information, see “Security Adapters for LDAP and ADSI Authentication” on page 22 and Chapter 5, “Security Adapter Authentication.”
- **Communications encryption.** Siebel Business Applications support the use of the following technologies for communications encryption:
  - **Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encryption and authentication.** SSL or TLS can be used to protect communications between the following:

- Siebel Business Applications components, that is, Siebel Servers and Web servers.
- Siebel Web servers and Siebel Web Clients, if support for the protocol is provided by the Web server. The use of SSL or TLS for Web server and Siebel Web Client communications is transparent to Siebel Business Applications.
- Siebel Servers and Microsoft Exchange Server email servers (SSL) or Siebel Servers and Microsoft Exchange Server 2007 or 2010 email servers (TLS).

NOTE: Oracle does not support the use of SSL v3.0 encryption for environments with high-security requirements. It is recommended that you implement TLS encryption where possible. For additional information, see "Using Secure Socket Layer v3.0 with Siebel CRM" on page 55.

The following table lists topics that provide information on configuring SSL and TLS.

Information Type	Topic
Restricting access to specific views to URLs that use TLS.	"Configuring a Siebel Web Client to Use HTTPS" on page 201
Configuring SSL or TLS for communication between Siebel components.	"Process of Configuring Secure Communications" on page 56
Using SSL or TLS to secure user login credentials	"Implementing Secure Login" on page 203
Using SSL or TLS to secure communications between Siebel Servers and directory servers.	"Configuring Secure Communications for Security Adapters" on page 150

- **RSA communications encryption.** Communication between Siebel components can be encrypted using RSA encryption algorithms. For more information, see "Process of Configuring Secure Communications" on page 56.

  For supported UNIX operating systems, Windows operating systems, or cross-operating system environments, Siebel Business Applications support RSA BSAFE. RSA BSAFE is FIPS 140-1 certified.

- **Microsoft Crypto.** For supported Windows operating systems, Siebel Business Applications support Microsoft Crypto. If the Siebel Server and the Web server are installed on the same computer running Microsoft Windows, then you cannot use Microsoft Crypto. You can use it only when these components run on different Microsoft Windows computers. For more information, see "Process of Configuring Secure Communications" on page 56 and "Types of Encryption" on page 52.

- **X.509 certificates.** Siebel Business Applications use the TLS capabilities of supported Web servers to enable authentication based on X.509 client certificates. For more information, see "About Digital Certificate Authentication" on page 191.

- **RSA SHA-1 password hashing.** Siebel user passwords can be hashed using the RSA SHA-1 algorithm. For more information, see "About Password Hashing" on page 158.

- **AES.** Siebel data can be encrypted using Advanced Encryption Standard (AES). Multiple key lengths are supported for AES using Siebel Strong Encryption. For more information, see "About Data Encryption" on page 74.

NOTE: Siebel Business Applications do not provide direct support for the Security Assertion Markup Language (SAML) standard.

About Supported Security Products

To augment the security of your Siebel Business Applications deployment, Oracle has alliances with leading security providers. For information, visit the Oracle Partner Network Web site at

http://www.oracle.com/us/partnerships/index.html

Oracle also provides a suite of security products, some of which have been certified for use with Siebel Business Applications. For information on the Oracle Identity Management products, go to

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

For information about third-party products supported or validated for use with Siebel Business Applications, see the Certifications tab on My Oracle Support.

Siebel Security Architecture

The components of Siebel security architecture include:

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

User Authentication for Secure System Access

Siebel Business Applications provide an open authentication architecture that integrates with a customer's selected authentication infrastructure. For more information, see Chapter 5, "Security Adapter Authentication," and Chapter 6, "Web Single Sign-On Authentication." Siebel Business Applications support three types of user authentication. A logical view of each type of authentication is illustrated in Figure 1, where each arrow represents a Siebel CRM authentication mechanism:

1. **Database authentication.** A database security adapter is provided to support database credential collection and verification of users.

2 **LDAP and ADSI authentication.** LDAP and ADSI security adapters are provided to support credential collection and verification of users in an LDAP or ADSI-compliant directory.

3 **Web Single Sign-On (Web SSO).** A configurable mechanism for communicating with Web SSO infrastructures is provided, allowing for Siebel user authentication by a third party at the Web-site level.

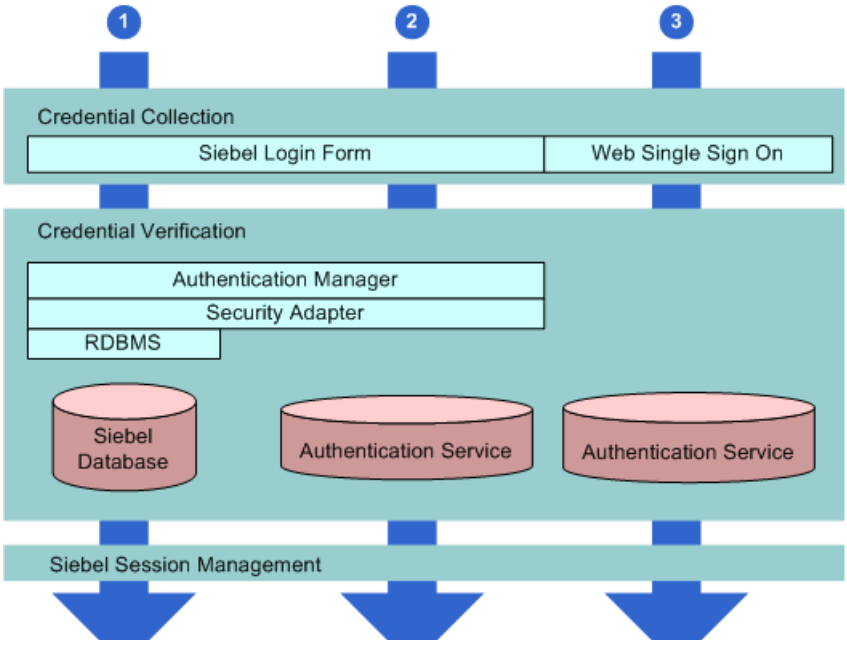

Figure 1. Logical Diagram of User Authentication Methods Within a Siebel Site

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

The authentication mechanisms illustrated in Figure 1 apply whether users access Siebel Business Applications from within a LAN or WAN, or remotely. Additional information on each method of authentication is provided in the following topics.

Security Adapter for Database Authentication

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

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

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

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

Security Adapters for LDAP and ADSI Authentication

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

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

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

Siebel CRM provides security adapters for leading authentication services:

- LDAP security adapter integration is supported for directory servers that are compliant with the LDAP 3.0 standard.
- ADSI security adapter integration is certified and supported for Microsoft Active Directory.

For information about third-party LDAP directory servers supported or validated for use with Siebel Business Applications, see “Directory Servers Supported by Siebel Business Applications” on page 107. You can also build security adapters to support a variety of authentication technologies. For information on custom security adapters, see “Security Adapter SDK” on page 23.

Web Single Sign-On

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

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

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

Security Adapter SDK

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

For example, a security adapter might be created for a portable device that provides users with a key that changes at frequent intervals. When a security adapter for this device is deployed, only by supplying both the currently displayed key and the user's password or other credentials can the user gain access to the Siebel application.

The security adapter interface is critical to the Siebel architecture because, for most Siebel Business Applications customers, authentication has become an enterprise decision, rather than an application-specific decision. The authentication service can be a shared resource within the Enterprise, thereby centralizing user administration. The Siebel Security Adapter SDK is described in 476962.1 (Article ID) on My Oracle Support.

End-to-End Encryption for Data Confidentiality

Stored data can be selectively encrypted at the field level, and access to this data can be secured. In addition, data can be converted into an encrypted form for transmission over a network. Encrypting communications safeguards such data from unauthorized access. Transmitted data must be protected from intrusive techniques (such as sniffer programs) that can capture data and monitor network activity.

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

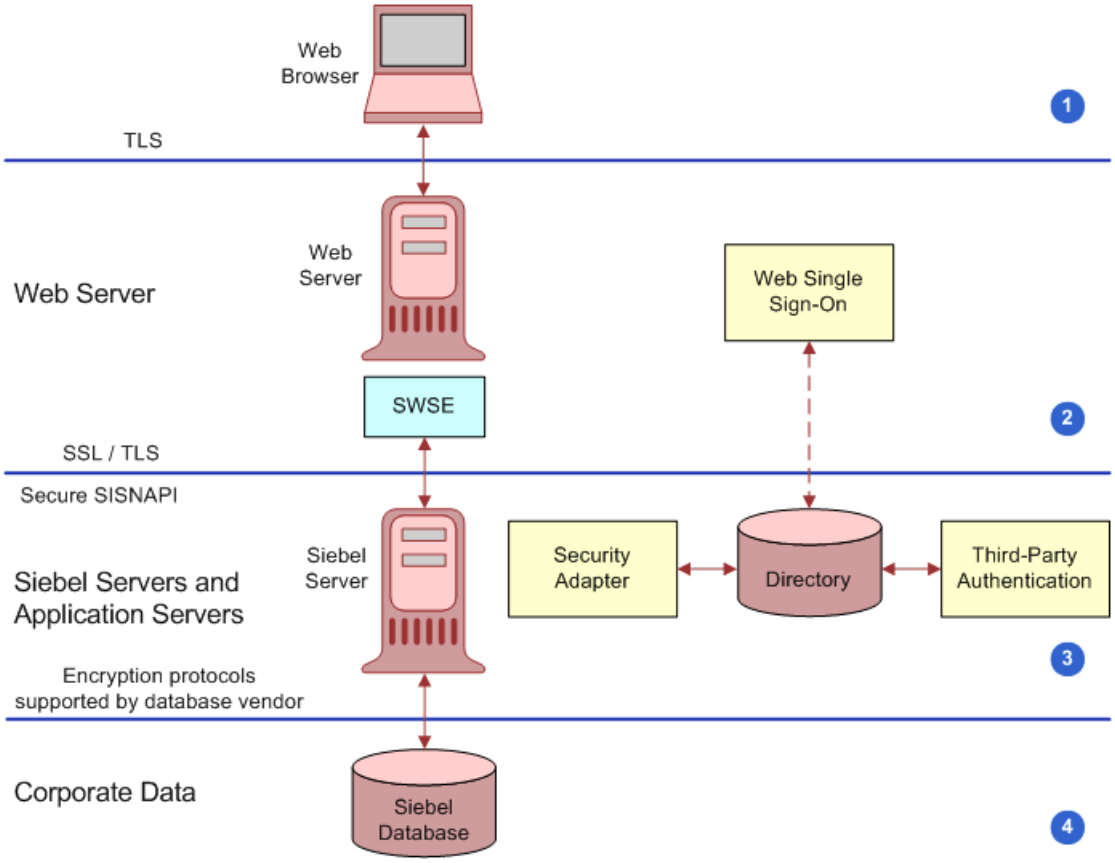

Figure 2. Encryption of Communications in the Siebel Environment

Communications encryption is available between the following:

1 **Client Browser to Web Server.** Siebel Business Applications run using the Siebel Web Client in a standard Web browser. When a user accesses a Siebel application, a Web session is established between the browser and the Siebel Server, with the Web server in between. To protect against session hijacking when sensitive data is transmitted, it is recommended that you use the TLS protocol for communications between the browser and Web server, if support for this protocol is provided by your Web server.

   The SWSE can be configured to allow only URLs that use TLS over HTTP (HTTPS protocol) to access views in a Siebel application in the following scenarios:

   - Use HTTPS only on the login view to protect password transmission. See "Login Security Features" on page 202.

- Use HTTPS for additional specific views (this option is available for standard interactivity applications only). See "Configuring a Siebel Web Client to Use HTTPS" on page 201.
- Use HTTPS for the entire application. See "Configuring a Siebel Web Client to Use HTTPS" on page 201.

2. **Web Server to Siebel Server.** Siebel Business Applications components communicate over the network using a Siebel TCP/IP-based protocol called SISNAPI (Siebel Internet Session API). Customers have the option to secure SISNAPI using SSL, TLS, or embedded encryption from RSA or Microsoft Crypto APIs. These technologies allow data to be transmitted securely between the Web server and the Siebel Server. For more information, see "Process of Configuring Secure Communications" on page 56.
3. **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.
4. **Database Storage.** Siebel Business 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 Business Applications to encrypt data before it is written to the database and decrypt the same data when it is retrieved. This prevents attempts to view sensitive data directly from the database. Siebel Business Applications support data encryption using AES algorithms. For more information, see "About Data Encryption" on page 74.

NOTE: Oracle does not support the use of SSL v3.0 encryption for environments with high-security requirements. It is recommended that you implement TLS encryption where possible. For additional information, see "Using Secure Socket Layer v3.0 with Siebel CRM" on page 55.

About Controlling Access to Data

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

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

Access control provides Siebel customers with a unified method of administering access to many content items for many users. For more information, see Chapter 9, "Configuring Access Control."

View-Level Access Control

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

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

Record-Level Access Control

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

Siebel Business Applications use three types of record-level access: position, organization, and access group. When a particular position, organization, or access group is assigned to a data record, only employees who have been assigned 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 you to classify users so that the hierarchy between them can be used for access to data.

  For example, a supervisor would have access to much of the data that a subordinate has access to; the same applies to others who report to the same manager.

- Similarly, an organization, such as a branch of an agency or a division of a company, is a grouping of positions that map to the physical hierarchy of a company. Those employees assigned to a position within a certain organization are granted access to the data that has been assigned to that organization. Visibility to data can be set up to restrict employees from accessing data outside their own organization.

- An access group is a less-structured collection of users or group of users, such as a task force. Groups can be based on some common attribute of users, or created for a specific purpose, pulling together users from across different organizations and granting them access to the same data.

Support for Auditing in a Siebel Environment

Siebel Business Applications support various degrees of auditing:

- At the simplest level, each data record has created and last updated fields (when and by whom). With additional configuration, you can generate an activity for additional levels of auditing. This is best used when there are limited needs for auditing, for example, just a few areas to track.

- Siebel Business Applications can maintain an audit trail of information that tells when business component fields have been changed, who made the change, and what has been changed. It is also possible to maintain an audit trail of when the business component fields have been viewed or exported and who viewed or exported fields. Siebel Audit Trail is a configurable feature that allows users to choose business components and fields to audit, and to determine the scope of the audit.

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

- Using Siebel Workflow, you can configure workflow processes to save information on changes to specific business components.

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

- Siebel customers can use 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 a security person to review the audit information.)

  If you implement a shared database account with LDAP, ADSI, or Web Single Sign-On authentication mechanisms, then database auditing cannot provide detailed information about an individual user's database access. For additional information, see "Configuring the Shared Database Account" on page 151.

Secure Physical Deployment to Prevent Intrusion

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

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

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

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

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

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

Security for Mobile Solutions

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

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

- For information about security issues for Siebel Business Applications accessed from a browser on a mobile device, see *Siebel Mobile Guide: Connected* and *Siebel Mobile Guide: Disconnected*.
- For information about security issues for Siebel Mobile Web Client, which can be installed on mobile devices such as laptop computers, see "Configuring Encryption for Mobile Web Client Synchronization" on page 73 and "About Authentication for Mobile Web Client Synchronization" on page 170. *Siebel Remote and Replication Manager Administration Guide* provides additional information on Mobile Web Client security measures.
- For information about security issues for Siebel Wireless applications, see *Siebel Wireless Administration Guide*.
- For information about security issues for Siebel Handheld applications, see documentation for particular Siebel Business Applications that use the Siebel Handheld client on *Siebel Bookshelf*.

Secure Real-Time Wireless Communications

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

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

Multiple methods of securing the data are available, including the Wireless Transport Security Layer for wireless devices and third-party products.

Mobile Device User Authentication

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

Security Settings for the Web Browser

Certain features and functions in Siebel Business Applications work in conjunction with security or other settings on the Web browser. Detailed information about the browser settings used in deploying Siebel clients is provided in *Siebel System Administration Guide*. For information about the Web browsers supported for high interactivity clients, and for information about the browser standards required for Siebel Open UI, see the Certifications tab on My Oracle Support and "About Siebel Open UI" on page 30. For more information about settings in your Web browser, see the documentation for your browser.

Web Sites with Security Information

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

- Oracle Security Solutions page at

  http://www.oracle.com/us/technologies/security/security-solutions-151411.html

- RSA Laboratories home page at

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

- RSA Laboratories Crypto FAQ at

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

- CERT Coordination Center, Carnegie Mellon University at

  http://www.cert.org

- Microsoft Safety and Security home page at

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

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

Roadmap for Configuring Security

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

NOTE: Perform any vendor-recommended tasks for securing your server or database before you install Siebel Business Applications. Perform other security tasks after you have installed Siebel Business Applications and have verified that it is functioning correctly.

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

1. During Siebel Business Applications installation, plan your Siebel Server and third-party HTTP load balancer TCP port usage for firewall access.

   For guidelines on implementing firewalls and port usage, see *Siebel Security Hardening Guide*.

2. After you install Siebel CRM, change the passwords for Siebel accounts regularly:

   - Change the password for the Siebel administrator account regularly.
   - Add a password for updating Web server images.

   For more information, see Chapter 3, "Changing and Managing Passwords."

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

4. Implement security adapter authentication or Web Single Sign-On to validate users. For more information, see Chapter 5, "Security Adapter Authentication," and Chapter 6, "Web Single Sign-On Authentication."

5. Set up an access control system to control user visibility of data records and Siebel application views. For more information, see Chapter 9, "Configuring Access Control."

6. Enable audit trail functionality to monitor database updates and changes.

   For information on Siebel audit trail functionality, see *Siebel Security Hardening Guide* and *Siebel Applications Administration Guide*.

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

   Enable encryption for Mobile Web Clients. See "Configuring Encryption for Mobile Web Client Synchronization" on page 73.

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

About Siebel Open UI

You can optionally deploy Siebel Business Applications using the Siebel Open UI. Siebel Open UI is the most secure Siebel CRM client available and is therefore recommended if your Siebel implementation has high-security requirements.

From a security perspective, there are a number of important differences in the way in which Siebel Open UI functions compared with the Siebel high-interactivity and standard-interactivity user interface modes:

- Siebel Open UI uses an open architecture that allows you to run Siebel Business Applications on any Web browser that is compliant with the World Wide Web Consortium (W3C) standards. Siebel Open UI also supports a number of operating systems, including Windows, Mac OS, or Linux.

  In contrast, Siebel Business Applications that use high-interactivity and standard-interactivity user interface modes run only in Internet Explorer.

- The Siebel Open UI client is compatible with any security features supported by the Web browser on which it runs.

- Siebel Open UI uses only three technologies to render the client code: HTML, CSS, and JavaScript. Because of the small set of underlying technologies that are used to render the client and the absence of third-party plug-ins such as ActiveX and Java, Siebel Open UI provides the smallest possible attack surface.
- Siebel Open UI clients enforce session security by requiring that session IDs can only be passed in session cookies. For information, see "Session Cookie" on page 207.

For additional information about Siebel Open UI, see *Deploying Siebel Open UI* and *Configuring Siebel Open UI*.

NOTE: The procedures in this guide assume that you do not use left-hand navigation. However, you can set up left-hand navigation if you choose. For information about implementing left-hand navigation, see *Siebel Fundamentals for Siebel Open UI*.

3 Changing and Managing Passwords

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

- About Managing and Changing Passwords on page 33
- About Default Accounts on page 36
- Changing System Administrator Passwords on Microsoft Windows on page 37
- Changing the Siebel Administrator Password on UNIX on page 40
- Changing the Table Owner Password on page 42
- Troubleshooting Password Changes By Checking for Failed Server Tasks on page 43
- About the Gateway Name Server Authentication Password on page 44
- Changing the Siebel Enterprise Security Token on page 45
- Encrypted Passwords in the eapps.cfg File on page 46
- Encrypting Passwords Using the encryptstring Utility on page 47
- About Encryption of Gateway Name Server Password Parameters on page 48

About Managing and Changing Passwords

It is recommended that a password management policy is implemented in all Siebel Business Applications implementations to ensure that only authorized users can access the applications. The password management policy that is most appropriate varies according to site-specific variables, such as the size of the implementation and users' business needs. However, all password management policies ought to provide guidelines relating to how frequently end users must change their passwords, whether or not password expiry periods are enforced, and the circumstances in which passwords must be changed.

Password management policies must also be applied to accounts that are used to manage and maintain the Siebel implementation, such as the Siebel administrator account. The topics in this chapter provide information on changing and managing the passwords for these accounts. For information on how end users can change their passwords, see "Changing a Password" on page 254. For additional information on implementing password management policies, see *Siebel Security Hardening Guide*.

NOTE: Use the configuration wizards installed with Siebel Business Applications to perform the initial configuration of the Gateway Name Server, Siebel Server, and Web server. This initial configuration process includes specifying names and passwords for accounts described in this chapter, and choosing whether or not to encrypt passwords. Using the configuration wizards simplifies the task of setting password-related values for accounts and reduces configuration errors.

Guidelines for Changing Passwords

Before changing passwords in your environment, review the following general points:

- For end users, the availability of the Password and Verify Password fields in the Siebel application (User Preferences screen, User Profile view) depends on several factors:
  - For an environment using Lightweight Directory Access Protocol (LDAP) or Active Directory Service Interfaces (ADSI) authentication, the underlying security mechanism must allow this functionality. See also "Requirements for the LDAP Directory or Active Directory" on page 111.

    In addition, the Propagate Change parameter (alias PropagateChange) must be TRUE for the LDAP or ADSI security adapter (default is TRUE). For Siebel Developer Web Clients, the system preference, SecThickClientExtAuthent, must also be TRUE. For more information, see Chapter 5, "Security Adapter Authentication."
  - For an environment using database authentication, the Propagate Change parameter (alias DBSecAdpt_PropagateChange) must be TRUE for the database security adapter. The default is FALSE for the parameter defined in the Siebel Gateway Name Server, FALSE for the same parameter defined in application configuration files for the Developer Web Client. For more information, see Chapter 5, "Security Adapter Authentication."
- If you are using a third-party load balancer for Siebel Server load balancing, then make sure load-balancer administration passwords are set. Also make sure that the administrative user interfaces for your load-balancer products are securely protected.
- If you set and change passwords at the Siebel Enterprise level, then the changes are inherited at the component level. However, if you set a password parameter at the component level, then from that point forward, the password can be changed only at the component level. Changing it at the Enterprise level does not cause the new password to be inherited at the component level, unless the override is deleted at the component level. For more information, see *Siebel System Administration Guide*.

For information about changing the local DBA password on Mobile Web Clients, see *Siebel Remote and Replication Manager Administration Guide*. For information about configuring and using hashed user passwords and database credentials passwords through your security adapter, see "About Password Hashing" on page 158.

Characters Supported in Siebel Passwords

It is recommended that you implement a password policy in your organization that defines the requirements for creating and changing Siebel passwords. For example:

- The password value must not be the same as the user name.
- Password values must be a minimum length, usually 8 characters.
- Password values must include a variety of supported characters.

Supported Characters

Siebel CRM supports the use of the following characters in passwords:

- The alphabetic characters a to z (uppercase and lowercase)
- The numerals 0 to 9

- The following special characters:
  - Number sign (#)
  - Dollar sign ($)

Unsupported Characters

You cannot use the special characters shown in Table 3 when creating or changing passwords used in your Siebel implementation.

NOTE: The ADSI security adapter and the LDAP security adapter used with the Oracle LDAP Client allow special characters in passwords, including characters not supported in Siebel passwords.

Table 3. Special Characters Not Supported in Siebel Passwords

Character	Description	Hexadecimal
!	exclamation point	21
"	double quote	22
%	Percent sign	25
&	ampersand	26
'	Single quote	27
(	Left parenthesis	28
)	Right parenthesis	29
*	Asterisk (star)	2A
+	Plus	2B
,	Comma	2C
-	Minus (hyphen)	2D
.	Period	2E
/	Forward slash	2F
:	Colon	3A
;	Semi-colon	3B
<	Less-than sign	3C
=	Equal sign	3D
>	Greater-than sign	3E
?	Question mark	3F
@	At-sign	40
[	Left square bracket	5B
\	Back slash	5C

Table 3. Special Characters Not Supported in Siebel Passwords

Character	Description	Hexadecimal
]	Right square bracket	5D
^	Caret	5E
_	Underscore	5F
`	Grave accent	60
{	Left curly brace	7B
|	Vertical bar	7C
}	Right curly brace	7D
~	tilde	7E
´	Acute accent	B4

About Default Accounts

The Siebel installation process and the seed data provided with Siebel Business Applications create several default accounts. These accounts are used to manage and maintain your Siebel implementation. You assign passwords to these accounts when they are created. However, to safeguard the security of your implementation, change the passwords for these accounts regularly or delete any accounts you do not require.

Database Accounts

The following database accounts are created during the Siebel installation process. If you are using an Oracle or Microsoft SQL Server database, then you create these accounts when you run the grantusr.sql script. If you are using a DB2 database, then the database administrator manually creates these accounts. You must ensure these accounts have been created in the RDBMS and you must assign passwords to these accounts before you can configure the Siebel database:

- Siebel administrator database account (default user ID is SADMIN)
- A database account for users who are authenticated externally (default user ID is LDAPUSER)
- A database table owner (DBO) account

For information on creating and assigning passwords to the SADMIN, database table owner, and LDAPUSER accounts, see *Siebel Installation Guide* for the operating system you are using. For information on changing and managing the passwords for the SADMIN and database table owner accounts, see the following topics:

- "Changing System Administrator Passwords on Microsoft Windows" on page 37
- "Changing the Siebel Administrator Password on UNIX" on page 40
- "Changing the Table Owner Password" on page 42
- "Troubleshooting Password Changes By Checking for Failed Server Tasks" on page 43

For additional information on the LDAPUSER account, see "About Creating a Database Login for Externally Authenticated Users" on page 131.

Siebel User Accounts

The following Siebel application user account records are provided as seed data during the Siebel installation process. These user accounts are not installed with default passwords and their use is optional:

- A seed system administrator user record (SADMIN)
- A seed employee user record for customer users (PROXYE)
- Seed guest accounts: GUESTCST (customer applications), GUESTCP (Siebel Partner Portal), GUESTERM (Siebel Financial Services ERM)

You can use a seed guest account as the Siebel user account for the anonymous user. To use a seed guest account, you must set the following parameters, either when configuring the SWSE logical profile (recommended), or by editing the eapps.cfg file manually:

- **AnonUserName.** Set this parameter to the user ID of the anonymous user, for example, GUESTCST.
- **AnonPassword.** Set this parameter to the password associated with the anonymous user.

  If the EncryptedPassword parameter is set to True in the eapps.cfg file, then the password value entered for the AnonPassword parameter must be encrypted.

  The anonymous user password is written to the eapps.cfg file in encrypted form by default if you add or change this value using the Siebel Configuration Wizard. If, however, you must manually change or add an encrypted value for the AnonPassword parameter in the eapps.cfg file, then use the encryptstring.exe utility to generate the encrypted value. For information on this task, see "Encrypting Passwords Using the encryptstring Utility" on page 47.

For information on defining the anonymous user when you configure the SWSE logical profile, see *Siebel Installation Guide* for the operating system you are using. For additional information on configuring the anonymous user, see "Configuring the Anonymous User" on page 155.

Changing System Administrator Passwords on Microsoft Windows

Before you run the Database Configuration Wizard to configure the Siebel database on the RDBMS, you must create a Siebel administrator account, either manually (on IBM DB2) or using the grantusr.sql script. The default user ID for the Siebel administrator account is SADMIN (case-sensitive). You must also create a password for the account. The password you assign to the administrator account cannot be the same as the user name of the account.

To increase the security of your Siebel implementation, it is recommended that you change the Siebel administrator password at regular intervals. You might also have to change the password for the Siebel service owner account, which is the Windows user who starts the Siebel Server system service. This topic outlines procedures for performing both tasks. For more information about setting up these accounts for initial use, see the *Siebel Installation Guide* for the operating system you are using.

Changing the Password for the Siebel Service Owner Account

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

NOTE: If a password expiration policy for Windows user accounts exists, then make sure that the Siebel service owner password is updated before it is due to expire to maintain the availability of the Siebel Servers.

To change the password for the Siebel service owner account

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

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

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

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

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

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

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

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

3. Stop and restart the Siebel Server system service. For details, see *Siebel System Administration Guide*.

Changing the Password for the Siebel Administrator Account

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

To change the Siebel administrator password

1. Change the value of the Siebel administrator's Enterprise password parameter using either the Server Manager command or the Siebel user interface.

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

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

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

c. Click the Parameters tab.

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

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

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

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

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

4. On each Siebel Server in your Siebel Enterprise, delete the existing Siebel Server system service, then re-create it with the new administrator password as follows:

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

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

      where:

      - *EnterpriseName* is the name of your Siebel Enterprise
      - *SiebelServerName* is the name of the Siebel Server

      For example:

      ```
      siebctl -d -S siebsrvr -i "sia8x_app01"
      ```

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

      ```
      siebctl -h SIEBSRVR_ROOT -S siebsrvr -i "EnterpriseName_SiebelServerName" -a
      -g "-g GatewayServerHostname:port -e EnterpriseName -s SiebelServerName -u
      sadmin" -e NewPassword -u Account -p Password
      ```

      where:

      - *SIEBSRVR_ROOT* is the full path to the Siebel Server installation directory
      - *EnterpriseName* is the name of your Siebel Enterprise
      - *SiebelServerName* is the name of the Siebel Server
      - *GatewayServerHostname* is the name of the Gateway Name Server host
      - *port* is the port number of the Gateway Name Server
      - *sadmin* is the administrator user ID
      - *NewPassword* is the new Siebel administrator password in plaintext. The siebctl utility encrypts the password.
      - *Account* is the Siebel service owner account name
      - *Password* is the Siebel service owner account password

      For example:

      ```
      D:\sia8x\siebsrvr\BIN>siebctl -h "d:\sia8x\siebsrvr" -S siebsrvr -i
      "sia8x_app01" -a -g "-g localhost:2320 -e sia8x -s app01 -u sadmin" -e sadmin
      -u .\SADMIN -p xxxxxxxx
      ```

5 Start the Siebel Server system service.

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

Changing the Siebel Administrator Password on UNIX

Before you run the Database Configuration Wizard to configure the Siebel database on the RDBMS, you must create a Siebel administrator account, either manually (on IBM DB2) or using the grantusr.sql script. The default user ID for the Siebel administrator account is SADMIN (case-sensitive). You must also create a password for the account. For information about setting up this account for initial use, see the *Siebel Installation Guide* for the operating system you are using.

NOTE: The password you assign to the administrator account cannot be the same as the user name of the account.

To increase the security of your Siebel implementation, it is recommended that you change the Siebel administrator password at regular intervals as described in the following procedure.

To change the Siebel administrator password on UNIX

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

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

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

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

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

a Log in at the Enterprise level:

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

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

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

3 Change the password in the database.

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

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

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

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

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

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

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

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

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

where:

- ''$*Siebsrvr*'' is the installation directory of the Siebel Server
- *EnterpriseName* is the name of your Siebel Enterprise
- *SiebsrvrName* is the name of the Siebel Server
- *GatewayServerHostName* is the name of the Gateway Name Server host
- *gtwyport* is the port number of the Gateway Name Server
- *sadmin* is the administrator user ID
- *NewPassword* is the new Siebel administrator password (in plaintext). The siebctl utility encrypts the password.

For example:

```
siebctl -r "/data/siebel/sia8x/siebsrvr" -S siebsrvr -i TRN_ENTP:TRSIEBSRV2 -
a -g "-g HBGNOVOAS04:2320 -e TRN_ENTP -s TRSIEBSRV2 -u sadmin" -e
passwordnewxyz -L ENU
```

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

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

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

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

6 Restart all Siebel Servers using the following command:

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

Perform this step for each applicable Siebel Server.

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

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

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

Changing the Table Owner Password

This topic describes the steps to perform if you want to change the table owner password. Before you run the Database Configuration Wizard to configure the Siebel database on the RDBMS, you must create a database table owner (DBO) account with the appropriate permissions to modify the Siebel database tables. The table owner is used to reference table names in SQL statements that are generated by the Siebel application (for example, SELECT * FROM SIEBEL.S_APP_VER).

You create the database table owner account manually (on IBM DB2) or using the grantusr.sql script (Oracle or Microsoft SQL Server). For information on creating the table owner account, see the *Siebel Installation Guide* for the operating system you are using. Select a user ID for the table owner that meets your organization's naming conventions. Also specify a password for the database table owner account.

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

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

Note the following requirements for changing the table owner password:

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

To change the password for the table owner account

1 Change the table owner password for the Enterprise as follows:

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

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

   c Click the Parameters tab.

d In the Enterprise Parameters list, locate the Table Owner Password parameter (alias TableOwnPass).

e In the Value field, type in the new value, then commit the record.

2 Change the password in the database.

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

3 Restart the Siebel Server.

Troubleshooting Password Changes By Checking for Failed Server Tasks

If you change the Siebel administrator (SADMIN) password or the Table Owner password, then you can verify that the password change has not caused errors by checking that all server tasks are still running. If a server task has failed, then update the password for the task. The following procedure describes how to troubleshoot password changes.

To troubleshoot password changes

1 After the Siebel Server restarts:

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

b Navigate to the Administration - Server Management screen, then the Servers view.

c In the Siebel Servers list, select the applicable Siebel Server.

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

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

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

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

b Click the Component Definitions tab.

c Select the component that initiated the failed task.

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

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

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

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

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

About the Gateway Name Server Authentication Password

To make sure that only authorized users can make changes to the enterprise configuration parameters on the Gateway Name Server, users connecting to the Gateway Name Server must supply a valid authentication user name and password. Authentication user name and password values are verified by the security adapter specified for the Gateway Name Server, either the database security adapter or an LDAP, ADSI, or custom security adapter.

The user account you use for Gateway Name Server authentication must have the same privileges as the Siebel administrator account created during the Siebel installation process; these privileges are required to connect to the Gateway Name Server.

You can choose to use the Siebel administrator account for Gateway Name Server authentication, or you can create a new database user account, ensuring you assign it the same level of rights and privileges as the Siebel administrator account. If you are using LDAP, ADSI or a custom security adapter, then you must also add the Gateway Name Server authentication user name and password to the directory server.

You can change the Gateway Name Server authentication password at any point by changing the password for the Gateway Name Server authentication account in the database and in the LDAP directory or in Active Directory (if you are using LDAP or Active Directory authentication). For more information, refer to your RDBMS documentation or your directory server documentation. For additional information on Gateway Name Server authentication, see "About Authentication for Gateway Name Server Access" on page 165 and *Siebel Installation Guide* for the operating system you are using.

Using Siebel Utilities to Access the Gateway Name Server

When using any of the Siebel utilities that connect to the Gateway Name Server, for example the srvrmgr utility, you must specify the Gateway Name Server authentication user name and password.

You can pass the Gateway Name Server authentication user name and password in the command line as command flags, for example:

```
srvrmgr /g gateway1 /e enterprise1 /s server1 /u username /p password (Windows)

srvrmgr -g gateway1 -e enterprise1 -s server1 -u username -p password (UNIX)
```

where:

- *username* is a valid user name that has been assigned Siebel administrator privileges
- *password* is the password associated with *username*

You must enter a value for the /u *username* or -u *username* flag. If you do not specify a value for the /p *password* or -p *password* flag, then you are prompted for this value when you submit the command.

Changing the Siebel Enterprise Security Token

The Siebel Enterprise security token is a value that you specify when you create a Siebel Web Server Extension (SWSE) logical profile. This token serves as a password that authenticates a Siebel administrator refreshing application images (and other static content) from the Siebel Server to the Web server without requiring a restart of the Web server.

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

If the EncryptedPassword parameter is set to FALSE, then passwords are not stored as encrypted values and new passwords must not be entered as encrypted values. For more information about password encryption for the eapps.cfg file, and about the encryptstring utility, see "Encrypted Passwords in the eapps.cfg File" on page 46. For more information about managing Web images and other files for your Siebel Business Applications, see *Configuring Siebel Business Applications*.

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

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

1. The Web public root directory (the location of Web file caching for Siebel Business Applications) is set automatically when you apply the SWSE logical profile by running the Siebel Configuration Wizard for SWSE. Or, you can specify it by adding a line in each application section of the eapps.cfg file.

   For example, to specify the Web public root directory for Siebel eService (for a Web server on a Windows computer), add a parameter like this:

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

   where:

   - *SWEAPP_ROOT* is the SWSE installation directory, such as `D:\sba8x\SWEApp`

- *LANGUAGE* is the application language, such as ENU for U.S. English

Files are copied to this location from all of the language-specific subdirectories of the directory *SIEBSRVR_ROOT*\webmaster, where *SIEBSRVR_ROOT* is the Siebel Server installation directory.

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

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

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

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

NOTE: Typically, password encryption is in effect for the eapps.cfg file, as described in "Encrypted Passwords in the eapps.cfg File" on page 46. If encryption is in effect and if you edit the file manually, then you must use the encryptstring utility to generate an encrypted version of the new password to store in the file.

Siebel administrators can then use this password to update cached static files from a browser, without restarting the Web server. For example, specify a URL like the following:

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

Specify the password in clear text form, whether or not encryption is used.

Encrypted Passwords in the eapps.cfg File

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

- AnonPassword (whether this parameter appears only in the [defaults] section or also in the application-specific sections of the eapps.cfg file)
- SiebEntSecToken (Siebel Enterprise security token)
- TrustToken

For more information about the SiebEntSecToken parameter, see "Changing the Siebel Enterprise Security Token" on page 45.

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

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

NOTE: If the EncryptedPassword parameter does not exist in the eapps.cfg file, then the default behavior is the same as if EncryptedPassword is set to FALSE. It is recommended that you set the value of the EncryptedPassword parameter to TRUE.

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

The account and password are created using the standard Siebel database scripts, and must already exist in the Siebel database when you configure the SWSE. If you change the password for this account after setting up your system, then you must update the password stored in the eapps.cfg file. For information about updating encrypted passwords, see "Encrypting Passwords Using the encryptstring Utility" on page 47.

Encrypting Passwords Using the encryptstring Utility

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

Although the anonymous user has limited privileges, it is generally recommended to use more secure passwords for production deployments of your Siebel Business Applications. For anonymous user accounts, changing passwords involves changing passwords for database accounts and changing passwords in the eapps.cfg file.

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

The following procedure describes how to encrypt a password using the encryptstring utility.

To encrypt a password using the encryptstring.exe utility

1. Locate the encryptstring utility.

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

2. To generate an encrypted value for a password, enter the following command:

```
encryptstring password
```

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

```
encryptstring GUESTCST
```

The output in this case might be something similar to the following:

```
fhYt8T9N4e8se4X3VavTjQXwAEqm
```

The specific value that is returned changes each time you use the encryptstring utility.

NOTE: The encryptstring utility does not support the use of special characters such as quotation marks, greater than signs, less than signs, plus signs, caret symbols, or ampersands. If you run the encryptstring utility for a password that includes these characters, then an encrypted version of the password is not generated by the utility.

About Encryption of Gateway Name Server Password Parameters

The siebns.dat file stores information required by the Siebel Gateway Name Server. This includes operational and connectivity information as well as configuration information for the Siebel Enterprise and Siebel Servers. If a Gateway Name Server configuration parameter requires a password value, then the Siebel encryptor writes the password to the siebns.dat file in encrypted format.

NOTE: End user passwords are not specified as Gateway Name Server parameter values and are not stored in siebns.dat.

In the current release, passwords in siebns.dat are encrypted using the AES algorithm. The encryptor generates the encrypted password using an encryption key that is unique to each parameter. The encryption key itself is generated based on repository information.

If you choose, you can use Siebel Strong Encryption to increase the encryption key length for encrypting passwords. If you do increase the encryption key length for encrypted passwords in siebns.dat, then the passwords have to be encrypted again using the new key. For a list of some of the password parameters that are encrypted in siebns.dat, and for information on how to reencrypt them, see “Reencrypting Password Parameters in the Siebns.dat File” on page 92.

Upgrading to Siebel CRM

In Siebel CRM Innovation Pack 2014, passwords in the siebns.dat file are encrypted using AES encryption. If you are upgrading to the current release, once the patch installation is completed, you must reset encrypted passwords in the siebns.dat file so that they now use AES encryption. For information on performing this task, see "Reencrypting Password Parameters in the Siebns.dat File" on page 92.

NOTE: When you upgrade to the current release, the Siebel Server system service password, which is required to connect the Siebel Server to the Gateway Name Server, is automatically reencrypted using AES encryption. The Gateway Name Server Password parameter, which is set at the Siebel Enterprise level, is also automatically reencrypted. You do not have to reencrypt these passwords manually.

4 Communications and Data Encryption

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

- Types of Encryption on page 52
- Process of Configuring Secure Communications on page 56
- About Certificates and Key Files Used for SSL or TLS Authentication on page 57
- Installing Certificate Files on page 59
- Configuring SSL Mutual Authentication on page 62
- About Configuring Encryption for a Siebel Enterprise and SWSE on page 63
- About Key Exchange for Microsoft Crypto or RSA Encryption on page 64
- Configuring SSL or TLS Encryption for a Siebel Enterprise or Siebel Server on page 65
- Configuring SSL or TLS Encryption for SWSE on page 68
- Enabling TLS Acceleration for Web Server and Web Client Communications on page 71
- About Configuring Encryption for Web Clients on page 72
- Configuring Encryption for Mobile Web Client Synchronization on page 73
- About Data Encryption on page 74
- Configuring Encryption and Search on Encrypted Data on page 77
- Managing the Key File Using the Key Database Manager on page 80
- About Upgrading Data to a Higher Encryption Level on page 82
- Process of Upgrading Data to a Higher Encryption Level on page 83
- About Siebel Strong Encryption on page 87
- Implementing Siebel Strong Encryption on page 88
- Increasing the Encryption Level on page 89
- Reencrypting Password Parameters in the Siebns.dat File on page 92
- Security Considerations for Unicode Support on page 95

Types of Encryption

Encryption is a method of encoding data for security purposes. Siebel Business Applications support industry standards for secure Web communications, and for encryption of sensitive data such as passwords. The following topics outline the standards supported:

- "Communications Encryption" on page 52
- "Data Encryption" on page 55

  Siebel Business Applications limit the encryption key length to 56-bits in its products. If you want to use encryption keys longer than 56-bits for transport layer encryption and data encryption, then you can do so by using Siebel Strong Encryption. For more information, see "About Siebel Strong Encryption" on page 87.

Communications Encryption

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

- **TLS encryption for Web client connections.** For data security over the Internet, Siebel Business Applications support the use of the Transport Layer Security (TLS) capabilities of supported Web servers to secure transmission of data between the Web browser and the Web server. The use of TLS for Web server and Siebel Web Client communications is transparent to Siebel Business Applications. For information on configuring TLS for Web server communications with the browser, see the vendor documentation.

  Siebel Business Applications can be configured to run completely under HTTPS, have specific pages run under HTTPS (for standard interactivity only), or simply handle login requests under HTTPS. For more information, see "Configuring a Siebel Web Client to Use HTTPS" on page 201 and "Login Security Features" on page 202.

- **Encryption for SISNAPI connections (SSL, TLS, 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 SSL, TLS, or on Microsoft Crypto API or RSA algorithms. SSL, TLS and RSA are supported on multiple operating systems. By default, SISNAPI encryption based on SSL and TLS uses the DES algorithm with a 56-bit key that performs both encryption and decryption. To upgrade to the AES algorithm with 256-bit encryption keys, use Siebel Strong Encryption. For information, see "About Siebel Strong Encryption" on page 87.

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

  NOTE: Oracle does not support the use of SSL v3.0 encryption for environments with high-security requirements. It is recommended that you implement TLS encryption where possible. For additional information, see "Using Secure Socket Layer v3.0 with Siebel CRM" on page 55.

- **SSL or TLS encryption for connections to directory servers.** SSL encryption is supported for connections to certified LDAP directories. TLS encryption is supported for connection to Active Directory.
- **SSL or TLS encryption for connections to email servers.** SSL encryption is supported for connections to email servers using Siebel Communications Server components. TLS encryption is supported for connections to Microsoft Exchange Server 2007 or 2010 email servers. For information, see *Siebel Email Administration Guide*.
- **Encryption of communications between the Siebel Server and the Siebel database.** The encryption technologies available to encrypt communications between the Siebel Server and the database depends on the encryption methods supported by your RDBMS vendor. For information on how to configure communications encryption between the Siebel Server and the Siebel database, contact your third-party RDBMS vendor.

Figure 3 shows some of the types of communications encryption available in a Siebel Business Applications environment.

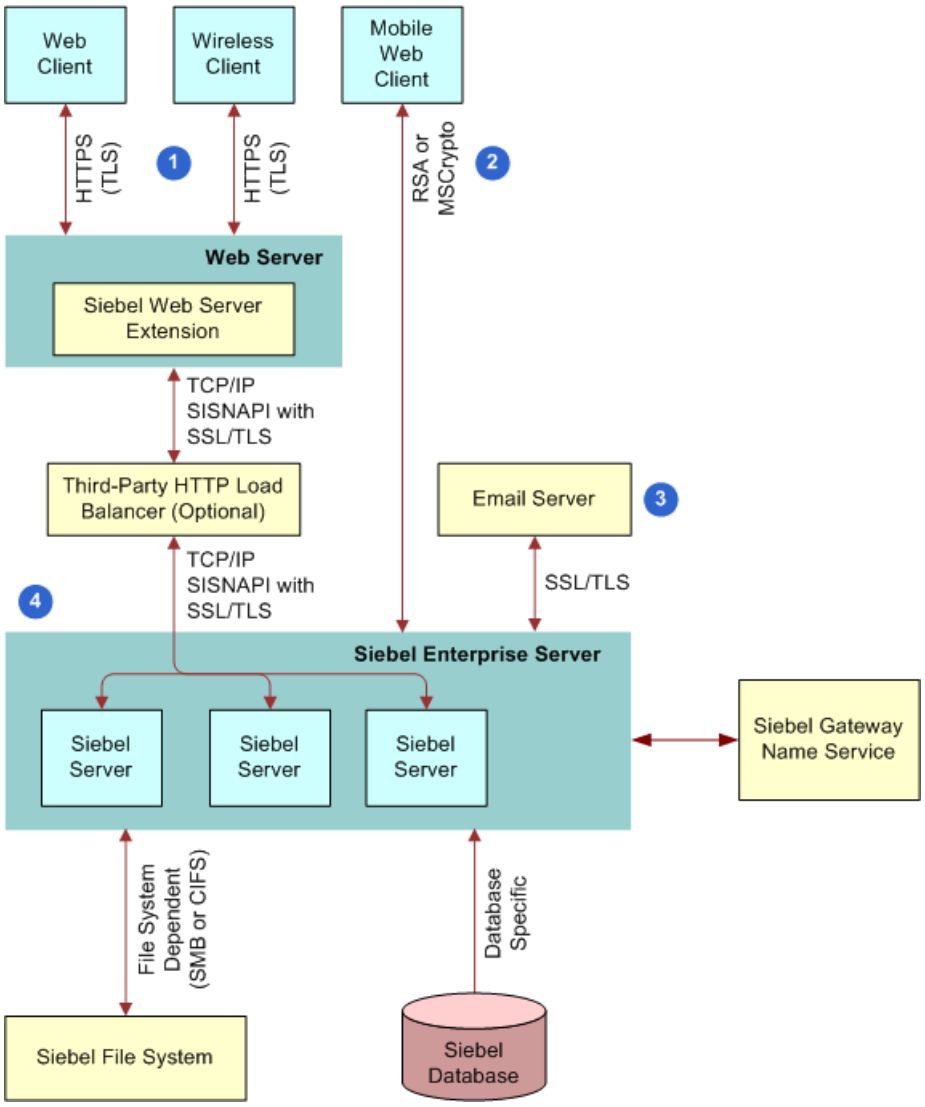

Figure 3. Communications Encryption in the Siebel Application Environment

The encryption mechanisms illustrated in Figure 3 are as follows:

1. **Web client and wireless client connections.** If supported by your Web server, TLS can be used to secure transmission of data between the Web browser and the Web server.
2. **Siebel Mobile Web Client connections.** You can use either MSCRYPTO or RSA encryption for Mobile Web Client communications with the Siebel Remote server.
3. **Email server connections.** SSL or TLS encryption for connections to email servers is supported.

4 **SISNAPI connections.** SISNAPI encryption of communications between Siebel components can be based on SSL, TLS, or on Microsoft Crypto API or RSA algorithms.

Using Secure Socket Layer v3.0 with Siebel CRM

Oracle does not support the use of SSL v3.0 encryption for environments with high-security requirements as a result of security vulnerabilities recently discovered in the design of SSL v3.0. It is recommended that you implement the Transport Layer Security (TLS) protocol instead of SSL whenever possible.

SSL and TLS can potentially be implemented for the following services and communications paths in a Siebel CRM implementation:

- Siebel Web server to Siebel Web Client communications
- Encryption for SISNAPI communications between Siebel Enterprise components, for example, communications between the Siebel Server to Siebel Web server (SWSE), or between Siebel Servers
- Encryption for SMTP, IMAP, and POP3 sessions between a Siebel Server and an email server
- Communications between an LDAP or ADSI security adapter and a directory server
- Communications using the Siebel Business Applications external interfaces (EAI), which use Web services to send and receive messages over HTTP

TLS encryption is not currently available for all the Siebel services or communication paths listed. For information about the support for TLS encryption provided by Siebel CRM, see 1944467.1 (Article ID) on My Oracle Support.

Data Encryption

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

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

  Customers can configure Siebel Business Applications to encrypt a column's data before it is written to the database and decrypt the same data when it is retrieved. This encryption prevents attempts to view sensitive data directly from the database. Sensitive data can be encrypted by using AES encryption at various key lengths. Encryption can be enabled using Siebel Tools. For more information, see "About Data Encryption" on page 74.

  NOTE: Implement AES encryption using Siebel Strong Encryption for increased data security.

  Siebel Business Applications also use AES encryption to encrypt passwords stored in the siebns.dat file. The siebns.dat file stores information required by the Siebel Gateway Name Server. For more information about encrypted passwords in the siebns.dat file, see "About Encryption of Gateway Name Server Password Parameters" on page 48.

- **RC4 encryption**. Siebel Business Applications use RC4 encryption to encrypt passwords stored in the Auto-Login Credential Cookie. For more information about the Auto-Login Credential Cookie, see "Auto-Login Credential Cookie" on page 210.
- **RSA SHA-1 password hashing.** Siebel administrators can enable password hashing for user passwords or for database credentials. Hashing uses a one-way hashing algorithm. The default password hashing method is RSA SHA-1. (The previous mangle algorithm is still available for existing customers.)

  The Siebel administrator password is stored in the Gateway Name Server file, siebns.dat, and is not hashed; passwords in siebns.dat are encrypted using AES encryption.

  Password hashing invalidates the password to unauthorized external applications and prevents direct SQL access to the data by anything other than Siebel Business Applications. For more information, see "About Password Hashing" on page 158.
- **Encryption of the Siebel File System and server disks containing Siebel Business Applications data**. It is recommended that you encrypt the Siebel File System and all server disks containing Siebel Business Applications data using third-party products or encryption features provided by your operating system. For information on the encryption technologies available, see the relevant operating system or third-party documentation. For additional information about securing the Siebel File System, see *Siebel Security Hardening Guide*.

Process of Configuring Secure Communications

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

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

- "Installing Certificate Files" on page 59
- "Configuring SSL Mutual Authentication" on page 62
- "Configuring SSL or TLS Encryption for a Siebel Enterprise or Siebel Server" on page 65
- "Configuring SSL or TLS Encryption for SWSE" on page 68
- "Enabling TLS Acceleration for Web Server and Web Client Communications" on page 71
- "Configuring Encryption for Mobile Web Client Synchronization" on page 73

The encryption options described in this topic are not used to encrypt data in the database. For information about data encryption, see "About Data Encryption" on page 74. Also, these encryption options are not used for communications with the database; for such encryption, check with your database vendor.

About Certificates and Key Files Used for SSL or TLS Authentication

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

Certificate files must adhere to the following requirements:

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

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

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

  NOTE: You can convert PEM-based certificate files to the ASN-based format.
- Certificate files on each computer must be unique and belong to that computer if PeerAuth is set to TRUE on the remote computer.
- If an intermediate certification authority is used, then both the intermediate and the root certificate authority certificates must be in the same file. You specify the name of this file for the CACertFileName parameter when you configure SSL or TLS for communication between Siebel components.

Certificate files and private key files are typically installed on each computer that hosts a component or module for which you configure SSL or TLS, such as a Siebel Server or SWSE. You do not have to authenticate or encrypt communications between components on the same computer. For information on installing certificate files, see “Installing Certificate Files” on page 59.

About Supported Values for Certificate Encryption Keys

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

In general, for SSL or TLS authentication for a Siebel Enterprise, Siebel Server, or SWSE, Siebel Business Applications support certificates that use an encryption key size of 1024 bits. If you require a higher encryption key size, for example, 2048 or 4096 bits, then you must use Siebel Strong Encryption.

The size of the certificate key supported depends on the components for which you are configuring SSL or TLS communications. Table 4 shows the certificate key sizes supported for communications between different components in a Siebel Business Applications deployment.

Table 4. Encryption Key Sizes Supported For SSL or TLS Certificates

SSL or TLS Communication Type	Supported Key Size
SSL or TLS communications using SISNAPI. Communications between the Siebel Server and the Web server (SWSE), and between Siebel Servers.	1024-bit certificate keys only are supported by default. To use certificate key sizes larger than 1024 bits, for example, 2048-bit or 4096-bit keys, you must follow the instructions in "Increasing the Certificate Key Sizes Supported For SISNAPI Communications" on page 58.
TLS communications between Web clients and the Web server.	The acceptable protocols and key sizes are determined by the underlying operating system and Web server software. In most cases, these systems support larger private key sizes.
SSL communications between developer clients (including Siebel Tools) and components in the Siebel environment.	1024-bit certificate keys only are supported.
SSL or TLS communications between the Siebel Server and the Siebel database.	The key size supported is determined by the third-party database used and database client software.
SSL or TLS communications between Siebel security adapters and external directory servers.	These connections can support larger bit sizes for SSL certificate keys.
SSL or TLS communications for Web services.	1024-bit certificate keys only are supported.

NOTE: Oracle does not support the use of SSL v3.0 encryption for environments with high-security requirements. It is recommended that you implement TLS encryption where possible. For additional information, see "Using Secure Socket Layer v3.0 with Siebel CRM" on page 55.

Increasing the Certificate Key Sizes Supported For SISNAPI Communications

For SSL or TLS authentication for Siebel Enterprise, Siebel Server, or SWSE communications, Siebel Business Applications support certificates that use an encryption key size of 1024 bits. If you want to use certificates with larger encryption key sizes, for example, certificates that use 2048-bit or 4096-bit encryption keys, then perform the steps in the following procedure.

To increase the certificate key sizes supported for SISNAPI communications

1 Navigate to the directory where the Siebel Strong Encryption (SSE) files were installed on the Siebel Server, Siebel Gateway Name Server, or the Web server:

- Web server
  - Windows: *SWEAPP_ROOT*\BIN\SSEP
  - UNIX: *SWEAPP_ROOT*/BIN/SSEP

  where *SWEAPP_ROOT* is the Siebel Web Server Extension installation directory.
- Siebel Server or Siebel Gateway Name Server
  - Windows: *COMPONENT_ROOT*\BIN\SSEP
  - UNIX: *COMPONENT_ROOT*/LIB/SSEP

  where *COMPONENT_ROOT* is either the Siebel Server installation directory or the Gateway Name Server installation directory.

For additional information, see "Implementing Siebel Strong Encryption" on page 88.

2 Copy the sslcnapi128 file from the SSEP directory to the directory where the sslcnapi file is located on the Siebel Server, Gateway Name Server, or the Web server as appropriate. The sslcnapi file is located as follows:

- Web server
  - Windows:*SWEAPP_ROOT*\BIN\sslcnapi.dll
  - UNIX:*SWEAPP_ROOT*/BIN/sslcnapi.so
- Siebel Server or Gateway Name Server
  - Windows:*component*\BIN\sslcnapi.dll
  - UNIX:*component*/lib/libsslcnapi.so

3 Rename the sslcnapi128 file to either sslcnapi or libsslcnapi to replace the existing sslcnapi file.

Installing Certificate Files

This topic describes how to install certificate files on Microsoft Windows and on Unix operating systems. For information on using certificate files, see "About Certificates and Key Files Used for SSL or TLS Authentication" on page 57.

This task is a step in "Process of Configuring Secure Communications" on page 56.

About Installing Certificate Files on Windows

If you have enabled Oracle's Siebel Open UI, and if you are not using Internet Explorer to run your Siebel application, see your browser documentation for information on installing certificate files.

If you are using a Siebel high-interactivity or standard-interactivity client, then you import certificate authority files and certificate files using Microsoft Internet Explorer's Certificate Import Wizard. For information on how to use this wizard, see the Microsoft documentation.

About Installing Certificate Files on UNIX

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

- **TLS encryption for Siebel Web Client connections to the Web server.** Refer to your Web server documentation for information on encrypting data transmission and on certificate requirements.
- **SSL or TLS Encryption for SISNAPI connections.** Obtain the required certificate files and locate them on a local volume; they do not have to be installed.
- **SSL encryption for connections to LDAP directories or TLS encryption to Active Directory.** The LDAP security adapter uses Oracle Wallet Manager to handle the installation of certificates. For information, see "Creating a Wallet for Certificate Files When Using LDAP Authentication with SSL" on page 121.
- **Communications encryption between the Siebel Server and the Database Server.** Refer to your third-party RDBMS vendor for information on configuring communications encryption and certificate requirements.

Installing Certificate Files on UNIX for Client Authentication

When using the EAI HTTP Transport business service with the SSL protocol, you might have to install certificate files, for example, if you want to enable client authentication. For information on client authentication, see "Configuring SSL Mutual Authentication" on page 62.

If you are using a UNIX-based operating system, then Siebel Business Applications provide a utility, the mwcontrol utility, that enables you to install on your Siebel Server and SWSE computers the certificate authority and certificate files required when using EAI HTTP Transport with SSL.

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

The following procedure describes how to use the mwcontrol utility to install certificate files. Execute the mwcontrol utility on each Siebel Server and SWSE computer where you want to install client authentication certificate files.

To invoke the mwcontrol utility and install certificate files

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

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

   - For C shell:

     ```
     source siebenv.csh
     ```

2. Set your DISPLAY environment variable to the IP address of the computer that hosts the mwcontrol utility:
   - For Bourne shell or Korn shell:

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

- For C shell:

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

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

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

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

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

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

The wizard appears.

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

The Certificate Manager appears.

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

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

6. Click Import to display the Certificate Manager Import Wizard, then click Next to navigate to the location where you stored the certificate file you want to install.
7. Select the certificate, and click Next.
8. Select the check box Automatically select the certificate store based on the type of certificate, then click Next.
9. Click Next, then Finish to complete the installation, and terminate the execution of the mwcontrol utility.

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

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

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

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

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

siebel_server_name:*network_protocol*:*sync_port_#*:*service*:*encryption*

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

An example of a DockConnString parameter value is as follows:

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

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

The encryption you specify must match the encryption used by the Siebel Server. If no value is specified (or the value is NONE), then encryption is not enabled. For example, to configure for RSA encryption, use one of the following:

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

12 Save your changes and exit the file.

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

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

Configuring SSL Mutual Authentication

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

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

If you choose to enable client authentication, then the Siebel Server presents a client certificate to an external Web server by supplying values for the HTTPCertSerialNo and HTTPCertAuthority EAI HTTP Transport parameters. The following procedure describes how to configure client authentication using the EAI HTTP Transport business service.

This task is a step in "Process of Configuring Secure Communications" on page 56.

To configure client authentication using EAI HTTP Transport

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

- A certificate authority file

- A client certificate file that is in PKCS#12 format.

For information on installing certificate files, see "About Installing Certificate Files on Windows" on page 59 or "Installing Certificate Files on UNIX for Client Authentication" on page 60.

2 Configure the Web server for client authentication.

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

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

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

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

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

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

NOTE: The TLS protocol is not supported on the UNIX operating system for HTTPS calls to external Web servers. Make sure that the external Web server allows the use of the SSL 3.0 protocol; otherwise WinInet error 12157 occurs on the Siebel Server.

About Configuring Encryption for a Siebel Enterprise and SWSE

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

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

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

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

When configuring the Siebel Enterprise using the Siebel Configuration Wizard, the Security Encryption Level or Type screen displays the following options for configuring the encryption type:

- SISNAPI Without Encryption.
- SISNAPI Using RSA Encryption Algorithm.
- SISNAPI Using TLS 1.2.
- SISNAPI Using SSL 3.0.
- SISNAPI Using Enhanced SSL 3.0 (requires a hardware proxy).
- MSCRYPT (Microsoft Crypto Enhanced API Encryption)

NOTE: Oracle does not support the use of SSL v3.0 encryption for Siebel implementations with high-security requirements. It is recommended that you implement TLS encryption where possible. For additional information, see “Using Secure Socket Layer v3.0 with Siebel CRM” on page 55.

For Siebel installations that include both UNIX and Microsoft Windows operating systems, it is recommended that you use an encryption method supported across operating systems, such as TLS or RSA.

For information about running the Siebel Configuration Wizard, see the *Siebel Installation Guide* for the operating system you are using. For information on configuring SSL or TLS, see the following topics:

- “Configuring SSL or TLS Encryption for a Siebel Enterprise or Siebel Server” on page 65
- “Configuring SSL or TLS Encryption for SWSE” on page 68

About Key Exchange for Microsoft Crypto or RSA Encryption

If you are using Microsoft Crypto or RSA encryption for communications between the Siebel Server and the Web server (SWSE), or between Siebel Servers, then 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.

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

Configuring SSL or TLS Encryption for a Siebel Enterprise or Siebel Server

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

This task is a step in "Process of Configuring Secure Communications" on page 56.

Configuring SSL or TLS communications between Siebel Servers and the Web server also requires that you configure the SWSE to use SSL or TLS. When configuring SSL or TLS for Siebel Server and the SWSE, you can also configure connection authentication for the relevant modules. In other words, when a module connects to another module, modules might be required to authenticate themselves against the other using third-party certificates.

Connection authentication scenarios are:

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

If you select the peer authentication option, mutual authentication is performed.

Configuring a Siebel Enterprise or Siebel Server to use SSL or TLS encryption involves the following tasks:

1 Run the Siebel Configuration Wizard for the Siebel Enterprise or Siebel Server and select the appropriate option to deploy either SSL or TLS.

   This task is described in "Deploying SSL or TLS for a Siebel Enterprise or Siebel Server" on page 66.

2 For each Application Object Manager that is to use either SSL or TLS, set the CommType parameter to SSL or TLS as appropriate.

   This task is described in "Setting Additional Parameters for Siebel Server SSL or TLS" on page 68.

Deploying SSL or TLS for a Siebel Enterprise or Siebel Server

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

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

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

1. Before you begin, obtain and install the necessary certificate files that you need if you are configuring SSL or TLS authentication.
2. If you are running the Siebel Configuration Wizard to configure the Siebel Enterprise, then do the following:
   a. Start the Siebel Configuration Wizard and configure values for the Enterprise.

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

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

   c. On the Security Encryption Level or Type screen, select the SISNAPI Using TLS 1.2 option, the SISNAPI Using SSL 3.0 option, or the SISNAPI Using Enhanced SSL 3.0 option.

   d. Proceed to Step 4 on page 66.
3. Alternatively, to run the Siebel Configuration Wizard directly on a Siebel Server computer, do the following:
   a. Start the Siebel Server Configuration Wizard directly and configure values for the Siebel Server.

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

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

   c. On the Security Encryption Level or Type screen, select the SISNAPI Using TLS 1.2 option or the SISNAPI Using SSL 3.0 option.

   d. Proceed to Step 4 on page 66.
4. Specify the name and location of the certificate file and of the certificate authority file.

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

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

The password you specify is stored in encrypted form.

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

6 Specify whether or not you want to enable peer authentication.

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

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

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

7 Specify whether or not you require peer certificate validation.

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

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

Depending on the Siebel Configuration Wizard you are running, you return to either the Siebel Enterprise or the Siebel Server configuration process.

8 Continue to configure values for the Siebel Enterprise or Siebel Server, then review the settings, finish configuration, and restart the server.

9 Perform the tasks in "Setting Additional Parameters for Siebel Server SSL or TLS" on page 68.

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

Make sure you also configure each SWSE in your environment. For information, see "Configuring SSL or TLS Encryption for SWSE" on page 68.

Setting Additional Parameters for Siebel Server SSL or TLS

After configuring SSL or TLS for a Siebel Server, you must set additional Gateway Name Server parameters to enable SSL or TLS for the Siebel Server as described in the following procedure.

To set additional parameters for Siebel Server SSL or TLS

1. Using Siebel Server Manager, set the Communication Transport parameter (alias CommType) to either SSL or TLS as appropriate for each Application Object Manager that is to use SSL or TLS. (TCP/IP is used by default.)

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

2. If you previously used Microsoft Crypto or RSA encryption, then, using Siebel Server Manager, set the Encryption Type parameter (alias Crypt) to NONE for the Siebel Enterprise.

Configuring SSL or TLS Encryption for SWSE

This topic describes how to configure the SWSE to use either SSL or TLS encryption and, optionally, authentication for SISNAPI communications with Siebel Servers using the Siebel Configuration Wizard. Configuring SSL or TLS communications between Siebel Servers and the Web server also requires that you configure a Siebel Enterprise or Siebel Server to use SSL or TLS. For information on this task, see "Configuring SSL or TLS Encryption for a Siebel Enterprise or Siebel Server" on page 65.

This task is a step in "Process of Configuring Secure Communications" on page 56.

NOTE: The information in this topic describes how to implement either SSL or TLS for communications between the SWSE and the Siebel Servers. For information on implementing TLS for communications between a Siebel Web Client and the SWSE, see "Configuring a Siebel Web Client to Use HTTPS" on page 201.

Configuring the SWSE to use SSL or TLS encryption involves the following tasks:

1. Run the Siebel Enterprise Configuration Wizard to configure a new Siebel Web Server Extension Logical Profile and select the appropriate option to deploy SSL or TLS.

   This task is described in "Deploying SSL or TLS for Siebel Web Server Extension" on page 69.

2. Modify the ConnectString parameter in the eapps.cfg file and specify either SSL or TLS encryption as appropriate.

   This task is described in "Configuring SSL or TLS Encryption for SWSE" on page 70.

NOTE: Oracle does not support the use of SSL v3.0 encryption for Siebel implementations with high-security requirements. It is recommended that you implement TLS encryption where possible. For additional information, see "Using Secure Socket Layer v3.0 with Siebel CRM" on page 55.

Deploying SSL or TLS for Siebel Web Server Extension

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

To deploy SSL or TLS encryption for the Siebel Web Server Extension

1. Before you begin, obtain and install the necessary certificate files you need if you are configuring SSL or TLS authentication.
2. Launch the Siebel Enterprise Configuration Wizard.

   For information on this task, see *Siebel Installation Guide* for the operating system you are using.
3. Choose the Create New Configuration option, then the Configure a New Siebel Web Server Extension Logical Profile option.

   For information on configuring the SWSE logical profile, see *Siebel Installation Guide* for the operating system you are using.
4. Configure values for the SWSE logical profile until the Select the Connection Protocol and Encryption screen appears.
5. Specify whether you are using TCP/IP, SSL or TLS for communication between Siebel Servers and the SWSE.

   If you select either TLS or SSL, then the Deploy SSL or TLS in the Enterprise screen is displayed.
6. Select the appropriate check box to enable either SSL or TLS communications between the SWSE and the Siebel Server.

   TLS or SSL settings for SWSE must be compatible with those for Siebel Servers that connect to the Web server.
7. Specify the names of the certificate file and of the certificate authority file.

   The equivalent parameters in the eapps.cfg file are CertFileName and CACertFileName.
8. Specify the name of the private key file, and the password for the private key file, then confirm the password.

   The password you specify is stored in encrypted form.

   The equivalent parameters in the eapps.cfg file that the SWSE logical profile applies to the installed SWSE are KeyFileName and KeyFilePassword.

9 Specify whether you require peer authentication.

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

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

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

10 Specify whether you require peer certificate validation.

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

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

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

12 Using the Siebel Web Server Extension Configuration Wizard, apply the SWSE logical profile to each SWSE in your Siebel environment for which you want to secure communications using SSL or TLS.

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

13 For each Application Object Manager that will connect to the SWSE using SSL or TLS, modify the ConnectString parameter as described in "Configuring SSL or TLS Encryption for SWSE" on page 70.

Configuring SSL or TLS Encryption for SWSE

When you configure the SWSE to use either SSL or TLS using the Configuration Wizards, parameters are added to the eapps.cfg file in a new section called [connmgmt]. For descriptions of the SSL or TLS-related parameters listed in the [connmgmt] section, see "About Parameters in the eapps.cfg File" on page 353. The [connmgmt] section looks similar to the following:

```
[connmgmt]
CACertFileName = c:\security\cacertfile.pem
CertFileName = c:\security\certfile.pem
KeyFileName = c:\sba8x\admin\keyfile.txt
KeyFilePassword = ^s*)Jh!#7
PeerAuth = TRUE
PeerCertValidation = FALSE
```

For each Application Object Manager that will connect to the SWSE using SSL or TLS, modify the ConnectString parameter to specify SSL or TLS 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 one of the following as appropriate:

- For SSL:

  ```
  siebel.ssl.None.None://siebsrvrname:scbrokerport/siebel/SSEObjMgr_enu
  ```

- For TLS:

  ```
  siebel.tls.None.None://siebsrvrname:scbrokerport/siebel/SSEObjMgr_enu
  ```

Enabling TLS Acceleration for Web Server and Web Client Communications

This topic describes how to configure TLS acceleration for communications between the Siebel Web server and Siebel Web Clients.

This task is a step in "Process of Configuring Secure Communications" on page 56.

If you are using a third party HTTP-based load balancer for your Siebel Server load balancing and you want to off-load the processing of TLS encryption and decryption algorithms to the hardware accelerator on your load balancer, then you must enable the EnforceSSL parameter. Doing so improves application performance and ensures that TLS is used to encrypt URLs. EnforceSSL is False by default. To enforce the use of TLS acceleration, you change the EnforceSSL parameter for an Application Object Manager to True.

To enable TLS acceleration

1. To enable TLS acceleration, set the Application Object Manager parameter, EnforceSSL, to True as follows:
   a. Navigate to the Administration - Server Configuration screen, then the Servers view.
   b. In the Siebel Servers list, select the Siebel Server of interest.
   c. Click the Components view tab.
   d. In the Components list, select the Application Object Manager of interest, such as Call Center Object Manager (ENU).
   e. Click the Parameters subview tab.
   f. In the Parameter field, perform a case-sensitive query on EnforceSSL.
   g. Click in the Value on Restart field and type True.
2. Set the value of the SecureLogin and SecureBrowse parameters to FALSE.

   For information on these parameters, see "Parameters for Application Object Manager" on page 371.
3. Restart the Siebel Servers.

About Configuring Encryption for Web Clients

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

Siebel Business Applications support the following types of clients:

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

  Siebel Business Applications support the use of the TLS capabilities of supported Web servers to secure communications between the Siebel Web Client and the Web server. For information on configuring Siebel Business Applications to specify whether or not URLs must use TLS over HTTP (HTTPS protocol) to access views in a Siebel application, see "Configuring a Siebel Web Client to Use HTTPS" on page 201.

- **Siebel Mobile Web Client.** This client is designed for local data access, without having to be connected to a server. Periodically, the client must access the Siebel Remote server using a modem, WAN, LAN or other network to synchronize data. You can use either MSCRYPTO or RSA encryption for Mobile Web Client synchronization.

  For information on setting encryption for transmissions between Mobile Web Client and Siebel Remote server, see "Configuring Encryption for Mobile Web Client Synchronization" on page 73. See also *Siebel Remote and Replication Manager Administration Guide*.

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

  The encryption technologies available to encrypt communications between the Siebel Developer Web Client and the Siebel database depends on the encryption methods supported by your RDBMS vendor. For information on how to configure communications encryption between the Siebel Developer Web Client and the Siebel database, contact your third-party RDBMS vendor.

About Session Cookies and Web Clients

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

Instead of storing the session ID in clear text in the client's browser, Siebel Business Applications create an encrypted session ID and attach an encryption key index to the encrypted session ID. Session cookie encryption uses a 56-bit key by default. In Siebel Remote, the encryption algorithm and key exchange are the same as for session-based components.

Configuring Encryption for Mobile Web Client Synchronization

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

This task is a step in "Process of Configuring Secure Communications" on page 56.

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

NOTE: SSL or TLS are not supported encryption methods for the Siebel Developer Web Client or for synchronization of the local database on the Siebel Mobile Web Client.

For information about authentication for Siebel Mobile Web Client and Siebel Remote, see "About Authentication for Mobile Web Client Synchronization" on page 170. For general information on configuring encryption for Web clients, see "About Configuring Encryption for Web Clients" on page 72. For information about other security issues for Siebel Mobile Web Client, including encrypting the local database, see *Siebel Remote and Replication Manager Administration Guide*.

To enable encryption of synchronization on the Mobile Web Client

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

   NOTE: When you edit configuration files, do not use a text editor that adds additional, nontext characters to the file.

   - Configuration files for a client are stored in the client's `bin\`*`LANGUAGE`* directory, where *`LANGUAGE`* represents an installed language pack, such as ENU for U.S. English.
   - When synchronization is performed within an application (using File, Synchronize, and then Database), configuration is read from the configuration file associated with the application, for example, siebel.cfg for Siebel Sales. For more information about working with Siebel application configuration files, see *Siebel System Administration Guide*.

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

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

   `siebel_server_name``:`*`network_protocol`*`:`*`sync_port_#`*`:`*`service`*`:`*`encryption`*

   Encryption is the fifth element in the DockConnString parameter. This element indicates the type of encryption used during synchronization. An example of a DockConnString parameter value is:

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

About Data Encryption

You can encrypt sensitive data in the Siebel database, such as customer credit card numbers, using AES encryption provided by Siebel Strong Encryption. For further information, see "About Siebel Strong Encryption" on page 87.

NOTE: Implement AES encryption for increased data security.

See the following topics for information about data encryption:

- "How Data Encryption Works" on page 74
- "Requirements for Data Encryption" on page 75
- "Encrypted Database Columns" on page 76
- "Upgrade Issues for Data Encryption" on page 77

You configure encryption using Siebel Tools. For details, see "Configuring Encryption and Search on Encrypted Data" on page 77.

How Data Encryption Works

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

After the data is encrypted, it is sent back to the database. When a user accesses this data, the encrypted data is sent through the encryptor again to be decrypted. The data is decrypted using the same encryption key from the key file that was used for encryption. The decrypted data is then sent to the business component field to be displayed in the application. For information on configuring encryption for a database column, see "Configuring Encryption and Search on Encrypted Data" on page 77.

The key file stores a number of encryption keys that encrypt and decrypt data. The key file is named keyfile.bin and is located in the *SIEBSRVR_ROOT*/admin directory of each Siebel Server. Additional encryption keys can be added to the key file. For security, the keyfile.bin file is itself encrypted with the key file password. For information on using the Key Database Manager utility to add encryption keys and to change the key file password, see "Managing the Key File Using the Key Database Manager" on page 80.

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

Requirements for Data Encryption

This topic outlines the restrictions and requirements to bear in mind when encrypting data.

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

The following requirements exist for data encryption:

- Because encryption and decryption have performance implications, encrypt only column data that is truly sensitive, such as credit card numbers and social security numbers.
- Siebel Assignment Manager does not decrypt data before making assignments. Assignment rules must take this limitation into consideration.
- When creating a link object to define a one-to-many relationship between a master business component and a detail business component, the source and destination fields specified in the link object definition must not be encrypted fields. If encrypted fields are specified, then the Siebel application cannot create the association between the two business components. For detailed information on configuring links, see *Configuring Siebel Business Applications*.
- Data that is moved into or out of the Siebel database using Siebel EIM is not encrypted or decrypted by EIM.

  For additional information on encrypting EIM data after it is imported into an encrypted column, see "Running the Encryption Upgrade Utility" on page 86.
- To configure AES encryption, use Siebel Strong Encryption.
- Encrypted data is retrieved, decrypted, and displayed from the fields in the encrypted column when records are selected. Users can perform exact-match queries on the unencrypted values for these fields if you create a hash column to store the hash values. For information, see "Configuring Encryption and Search on Encrypted Data" on page 77.
- You can only apply AES encryption to data in database columns that are at least 32 bytes long. You cannot encrypt database columns of type VarChar that are less than 30 bytes long.
- Encrypted data requires more storage space in the database than unencrypted data. You must specify appropriate data length for the affected columns. Use the following formulae when you allocate storage space for encrypted data:
  - For ASCII characters, the column size must be: (number of characters * [multiplied by] 2) + [plus] 10.

  - For non-English characters, the column size must be: (number of characters * [multiplied by] 4) + [plus] 10.
  - If you create a Hash Column (to enable search on encrypted data), then specify VarChar as the physical type of the column. The column size must be at least 30 characters; this is a requirement for use of the RSA SHA-1 algorithm.
- Field-level AES encryption is not supported for Developer Web Clients.
- Encryption is not supported for List of Values (LOV) columns or multilingual LOV (MLOV) columns.
- Encryption is not supported for join columns or foreign key columns.
- Encryption for a Mobile Web Client.

  Rather than encrypt data using AES encryption, the local database is encrypted. For information about encrypting the local database, see *Siebel Remote and Replication Manager Administration Guide*. For information about configuring encryption when the Mobile Web Client's local database is synchronized, see "Configuring Encryption for Mobile Web Client Synchronization" on page 73.

Encrypted Database Columns

Siebel Business Applications provide a number of database columns that are encrypted by default. Table 5 lists the database table columns encrypted by default in the Siebel database. For information on how to encrypt a database column, see "Configuring Encryption and Search on Encrypted Data" on page 77.

Table 5. Encrypted Database Table Columns

Table	Table Column
S_AGREE_TERMS	CC_NUMBER
S_CM_CNCTR_PARM	ENCRYPTED_VALUE
S_CONTACT_FNX	YL_PASSWD
S_DOC_ORDER	CC_NUMBER
	CCV_NUMBER
S_INV_PROF	CC_NUMBER
	CCV_NUMBER
S_ORDER	CC_NUMBER
S_PTY_PAY_PRFL	PAY_ACCNT_NUM
	VERIFICATION_NUM
S_SMQ_ADDR	SECURITY_TOKEN
S_SRC_PAYMENT	CC_NUM
S_SSO_SYS_USER	SSO_PASSWORD

Table 5. Encrypted Database Table Columns

Table	Table Column
S_USER	CHALLENGE_ANSWER
	CHALLENGE_QUESTION
T_DETAIL	ENCRPTD_COL

The CC_NUMBER and CC_NUM columns listed in Table 5 are used to store credit card number data. The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of standards designed to enhance the security of credit card data in organizations that process such data. It is contrary to the PCI standards to store credit card numbers in a database. The CC_NUMBER and CC_NUM columns are provided for backwards-compatibility purposes only and might be removed in a future release.

Upgrade Issues for Data Encryption

This topic describes data encryption issues to consider when upgrading from a previous release of Siebel Business Applications to a Siebel 8.*x* release.

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

When you upgrade from a release earlier than Siebel version 8.0 to the current release, the upgrade process automatically migrates business component field user properties to database table column properties so that all fields in the encrypted column are encrypted.

NOTE: If data encryption is to work in release 8.*x*, then the encrypted column and the key index column must reside in the same database table. For information on encrypting database columns in Siebel 8.*x* releases, see “Configuring Encryption and Search on Encrypted Data” on page 77.

Configuring Encryption and Search on Encrypted Data

This topic describes how to use Siebel Tools to enable encryption for a column in a database table and to enable search on the encrypted column.

NOTE: For help with encrypting columns in database tables, you must contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.

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

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

- The encrypted column, hash column, and the column that stores the index number to the key file must come from the same database table.
- You cannot encrypt a column that has a denormalized column, because this feature is not supported.

  For example, column NAME of account table S_ORG_EXT has a denormalized column in: S_ACCNT_POSTN.ACCOUNT_NAME.
- The encrypted column and the hash column must be of type String (VARCHAR), while the column that stores the index number to the key file must be of type Integer.

  For more information on requirements for data encryption, see "Requirements for Data Encryption" on page 75.

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

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

     ```
     SiebelEncrypt.AES ([ColumnName])
     ```

     For information on the Siebel AES encryption options, see "About Data Encryption" on page 74. To implement AES (recommended), you must use Siebel Strong Encryption. For more information, see "About Siebel Strong Encryption" on page 87.
   - **Encrypt Key Specifier.** Specify the column that stores the index number to the key file.
4. If you want to allow search on encrypted data, then create another column with a name of your choice or with the following name format:

C_HASH_NAME

where *Name* is the name of the column you selected in Step 2 on page 78.

C_HASH_NAME stores the value that results from applying the RSA SHA-1 algorithm to the plain text values of the column you selected in Step 2 on page 78.

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

Scenario	Enter these values

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

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

Now do one of the following:

- If the column that you have enabled for encryption does not yet contain data, then there are no further steps to perform.
- If the column that you have enabled for encryption does contain data, then proceed to Step 5 on page 79.

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

Encrypt existing data immediately after you configure a column for encryption. You can create searchable hash values for the column at a later time if you choose. For information on using the encryptupg.exe utility, see "About Upgrading Data to a Higher Encryption Level" on page 82.

Managing the Key File Using the Key Database Manager

This topic describes how to run the Key Database Manager utility to add new encryption keys to the key file (keyfile.bin) and to change the key file password. The AES Encryptor uses the key in the key file to encrypt new data.

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

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

To run the Key Database Manager

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

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

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

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

   For descriptions of the flags and parameters, see Table 6 on page 80.

3. When prompted, enter the key file password:

   - To add a new encryption key, see "Adding New Encryption Keys" on page 81.
   - To change the key file password, see "Changing the Key File Password" on page 81.

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

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

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

Table 6 on page 80 lists the flags and parameters for the Key Database Manager utility.

Table 6. Key Database Manager Flags and Parameters

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

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

- "Adding New Encryption Keys" on page 81
- "Changing the Key File Password" on page 81

Adding New Encryption Keys

You can add new encryption keys to the key file, keyfile.bin, which is located in the *SIEBSRVR_ROOT*/admin directory. The AES Encryptor uses the latest key in the key file to encrypt new data; existing data is decrypted using the original key that was used for encryption, even if a newer key is available. There is no limit to the number of encryption keys that you can store in the key file.

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

To add new encryption keys

1. Shut down any server components that are configured to use encryption.
2. From the *SIEBSRVR_ROOT*/bin directory, run Key Database Manager.

   For details, see "Managing the Key File Using the Key Database Manager" on page 80.
3. To add an encryption key to the key file, enter *2*.
4. Enter some seed data to provide random data used in generating the new encryption key.

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

   When exiting the Key Database Manager utility, monitor any error messages that are generated. If an error occurs, then you might have to restore the backup version of the key file.
6. Distribute the new key file by copying the file to the *SIEBSRVR_ROOT*/admin directory of all Siebel Servers in the Enterprise.

   CAUTION: When copying the keyfile.bin file to Siebel Servers, take care that the file does not become damaged. If the key file is damaged, then it is not possible to recover encrypted data without a backup key file.
7. Restart any server components that were shut down in Step 1 on page 81.

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

Changing the Key File Password

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

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

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

To change the key file password

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

   For more information, see "Managing the Key File Using the Key Database Manager" on page 80.
3. To change the key file password, enter *1*.
4. Enter the new password.
5. Confirm the new password.
6. Exit the utility by entering *3*.

   When exiting the Key Database Manager utility, monitor any error messages that might be generated. If an error occurs, then you might have to restore the backup version of the key file.
7. Distribute the new key file to all Siebel Servers by copying the file to the admin subdirectory in the Siebel Server root directory.
8. Restart any server components that were shut down in Step 1 on page 82.

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

About Upgrading Data to a Higher Encryption Level

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

- Upgrade encrypted data to a higher encryption level, for example, from RC2 (56 bits) to AES encryption, provided you use Siebel Strong Encryption.

  For information on Siebel Strong Encryption, see "About Siebel Strong Encryption" on page 87.
- Upgrade data that was encrypted using the standard encryptor to the AES encryption method.

  NOTE: You must upgrade data that was encrypted using the standard encryptor (based on the mangle algorithm) to a higher level of encryption before you upgrade to a Siebel CRM version 8. For additional information, see "Requirements for Upgrading to a Higher Encryption Level" on page 83.

In Siebel CRM releases earlier than release 7.5.*x*, data was encrypted using the standard encryptor. As of Siebel CRM version 7.5.x, Siebel Business Applications use the AES encryption algorithm to encrypt data, and the standard encryptor is supported for backwards-compatibility purposes only. For Siebel CRM version 7.5.3 or higher, you must use AES encryption.

If you want to upgrade encrypted data from Siebel CRM version 6.x or 7.0.x to Siebel CRM version 7.5.3, 7.7, or 7.8, then it is recommended that you upgrade the encrypted data to the AES standard to make sure that the data can be read accurately by the later release. If you want to upgrade encrypted data from Siebel CRM version 6.x or 7.0.x to any Siebel CRM version 8 release, then you must upgrade the encrypted data to the AES standard.

NOTE: You cannot upgrade directly from a Siebel CRM release earlier than 7.5.x to Siebel CRM version 8.x. If you want to upgrade from Siebel CRM version 6.x, then you must first upgrade to Siebel CRM version 7.7, even if you want to upgrade to a Siebel CRM release later than version 7.7.

Process of Upgrading Data to a Higher Encryption Level

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

1. Verify that all requirements are met.

   For information, see "Requirements for Upgrading to a Higher Encryption Level" on page 83.

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

   For information, see "Modifying the Input File" on page 84.

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

   For information, see "Managing the Key File Using the Key Database Manager" on page 80.

4. Upgrade the data to a higher level of encryption.

   For information, see "Running the Encryption Upgrade Utility" on page 86.

Requirements for Upgrading to a Higher Encryption Level

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

This task is a step in "Process of Upgrading Data to a Higher Encryption Level" on page 83.

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

- The Siebel Gateway Name Server and Siebel Server are installed.
- The Siebel repository has been upgraded to the schema for the current release, so that a new column has been created to store the key index for the encrypted column.

- If you created or customized columns to use the standard encryptor of Release 6.x or 7.0.x, for each encrypted column that you want to upgrade, you must create a new column to store the key index.
- If, in releases prior to release 8.0, you customized business component fields to use the standard encryptor, then verify that you define the correct properties for the columns in the database table that holds encrypted data. For further information, see "Configuring Encryption and Search on Encrypted Data" on page 77.
- Verify that column sizes for custom extension columns are large enough to hold the new AES values.
- The key database file (keyfile.bin) must already exist. (A default key file was created in the *SIEBEL_ROOT*/siebsrvr/admin directory when you installed the Siebel Server.)
- If you require AES encryption, then you must use Siebel Strong Encryption and you must upgrade the key database file to use a higher level of encryption. For more information on these tasks, see the following topics:
  - "Implementing Siebel Strong Encryption" on page 88
  - "Increasing the Encryption Level" on page 89

Modifying the Input File

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

This task is a step in "Process of Upgrading Data to a Higher Encryption Level" on page 83.

The following procedure describes how to modify the input file.

To modify the encrypt_colums.inp file

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

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

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

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

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

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

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

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

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

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

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

About Using the Where Clause and Flags in the Input File

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

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

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

- If you have imported data from EIM into an encrypted column, then use the WHERE clause to specify that only the unencrypted EIM records, that is, records where the value of the key index column is NULL, are to be encrypted. For example, the following entry is for a table named S_PER_PAY_PRFL. This table contains an encrypted column, PAY_ACCNT_NUM, which has a key index column, ENCRPKEY_REF:

  ```
  [S_PER_PAY_PRFL]
  PAY_ACCNT_NUM S_PER_PAY_PRFL CCNUM_ENCRPKEY_REF
  WHERE S.CCNUM_ENCRPKEY_REF IS NULL
  ```

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

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

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

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

This creates a hash column which stores the values that are returned when you apply the RSA SHA-1 algorithm to the plain text values of the encrypted column.

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

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

For information about search on encrypted data, see "Configuring Encryption and Search on Encrypted Data" on page 77.

Running the Encryption Upgrade Utility

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

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

This task is a step in "Process of Upgrading Data to a Higher Encryption Level" on page 83.

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

To run the encryption upgrade utility

1. Verify that the input file encrypt_colums.inp includes all the columns that you want to upgrade. If necessary, review "Modifying the Input File" on page 84.
2. Run encryptupg.exe by navigating to *SIEBEL_ROOT*\siebsrvr\bin and entering the following command:

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

   where:

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

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

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

- *ToEncryptionStrength* is the encryption strength that you want to upgrade to. The recommended value to enter for this parameter is AES.
- *InputFileName* is the filename of your input file (the default is `encrypt_columns.inp`).
- *Language* is the language code, for example, to specify U.S. English, enter `ENU`.
- *UserName* is the user name for the database.
- *Password* is the password for the database.
- *ConfigurationFile* is the application configuration file where you specify the data source for the Encryption Upgrade utility to retrieve data from.
- *LogFile* is the log file that the Encryption Upgrade utility writes to; the default file is `encryptupg.log`.

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

```
encryptupg /f RC2 /t AES /j d:\sba8x\siebsrvr\bin\encryptupg.inp /l ENU /u sadmin
p dbpw /c d:\sba8x\siebsrvr\bin\enu\siebel.cfg
```

3 After the upgrade is complete, make sure that the encrypted database columns specify the value for the encryption method used in the Computation Expression parameter. For more information, see "Configuring Encryption and Search on Encrypted Data" on page 77.

4 Compile a new Siebel repository file (.SRF).

For information about how to compile a.SRF file, see *Using Siebel Tools*.

About Siebel Strong Encryption

If you require encryption, then you must use Siebel Strong Encryption, which provides secure encryption for your Siebel Enterprise. Siebel Strong Encryption provides the following:

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

- Key Database Upgrade utility

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

AES encryption for data is provided as a Siebel business service and is configured using Siebel Tools. For more information, see "Configuring Encryption and Search on Encrypted Data" on page 77.

Implementing Siebel Strong Encryption

Siebel Strong Encryption is installed during the Siebel Enterprise and Siebel Web Server installations. However, there are various tasks you must perform to use Siebel Strong Encryption. This topic describes these tasks. For an overview of Siebel Strong Encryption, see "About Siebel Strong Encryption" on page 87.

NOTE: Siebel Strong Encryption is only available in U.S. English (enu); however, it can be implemented in a Siebel environment that uses other languages.

Requirements for Implementing Siebel Strong Encryption

Before implementing Siebel Strong Encryption, carry out the following tasks:

- Install and configure a Siebel Enterprise.

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

- Read "About Upgrading Data to a Higher Encryption Level" on page 82.

- Change the key file password.

  For more information, see "Managing the Key File Using the Key Database Manager" on page 80.

Implementing Siebel Strong Encryption

To implement Siebel Strong Encryption, perform the steps in the following procedure.

To implement Siebel Strong Encryption

1. Verify that you have completed the tasks listed in "Requirements for Implementing Siebel Strong Encryption" on page 88.
2. Navigate to one of the following directories to locate the SSE files:
   - To implement Siebel Strong Encryption on the Siebel Web Server Extension (SWSE), navigate to the following directory:
     - Windows: *SWEAPP_ROOT* \BIN\SSEP
     - UNIX: *SWEAPP_ROOT*/BIN/SSEP

     where *SWEAPP_ROOT* is the Siebel Web Server Extension installation directory.
   - To implement Siebel Strong Encryption on the Siebel Server or Gateway Name Server, navigate to the following directory:

- Windows: *SIEBEL_ROOT**Component*\BIN\SSEP
- UNIX: *SIEBEL_ROOT*/*Component*/LIB/SSEP

where:

- *SIEBEL_ROOT* is the installation directory for your Siebel Enterprise.
- *Component* is either siebsrvr or gtwysrvr.

The SSEP directory contains the files shown in the following table.

File	Purpose
sslcrsa128.dll (Windows) libsslcrsa128.so (UNIX)	Provides AES 128-bit data encryption.
sslcrsa256.dll (Windows) libsslcrsa256.so (UNIX)	Provides AES 192-bit or 256-bit data encryption.
sslcnapi128.dll (Windows) sslcnapi128.so (UNIX)	Used to increase the certificate key sizes supported for SISNAPI communications.

3 To increase the certificate key sizes supported for SISNAPI communications, see "Increasing the Certificate Key Sizes Supported For SISNAPI Communications" on page 58.

4 To increase the key length used for data encryption, copy the files as indicated:

- **Windows.** Depending on the key length you want to use, copy either sslcrsa128.dll or sslcrsa256.dl to the *SIEBEL_ROOT*\siebsrvr\BIN, *SIEBEL_ROOT*\gtwysrvr\BIN, or *SWEAPP_ROOT*\BIN directory.
- **UNIX.** Depending on the key length you want to use, copy either libsslcrsa128.so or libsslcrsa256.so to the directory *SIEBEL_ROOT*/siebsrvr/LIB, or to *SIEBEL_ROOT*/gtwysrvr/LIB, or to *SWEAPP_ROOT*/BIN.

5 Upgrade the key database file to use the level of data encryption you chose in Step 4 on page 89 by running the keydbupgrade.exe utility.

For information on this task, see "Increasing the Encryption Level" on page 89.

Increasing the Encryption Level

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

You can upgrade the key database file to use AES encryption provided you have implemented Siebel Strong Encryption as described in "Implementing Siebel Strong Encryption" on page 88. Table 7 shows the supported data encryption upgrade scenarios.

Table 7. Supported Encryption Upgrade Scenarios

Encryption Level to Upgrade from	Upgrade to 128-bit AES Encryption	Upgrade to 192-bit AES Encryption	Upgrade to 256-bit AES Encryption
No encryption	Yes	Yes	Yes
Standard Encryptor encryption	Yes	Yes	Yes
56-bit RC2 encryption	Yes	Yes	Yes
128-bit RC2 encryption	Yes	Yes	Yes
128-bit AES encryption	Not Applicable	Yes	Yes
192-bit AES encryption	Not Applicable	Not Applicable	Yes

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

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

1. Implement Siebel Strong Encryption as described in "Implementing Siebel Strong Encryption" on page 88.
2. Make sure that the Siebel Gateway Name Server and Siebel Servers within the Siebel Enterprise are running.
3. On the Siebel Server where the Siebel Strong Encryption files are located, open a command-line window and navigate to the following directory:

   SIEBEL_ROOT\siebsrvr\bin

4. Execute the appropriate command:

   On Windows:

   keydbupgrade.exe /u *db_username* /p *db_password* /l *language* /c *config_file*

   On UNIX:

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

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

Flag	Parameter	Description
/u	*db_username*	User name for the database user
/p	*db_password*	Password for the database user

Flag	Parameter	Description
/l	*language*	Language type
/c	*config_file*	Full path to the application configuration file, such as siebel.cfg for Siebel Sales

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

6 Select the key length to upgrade to.

7 Enter the key database manager password.

The utility upgrades the encryption level to the level you specified in Step 6. For information about the key database manager password, see "Managing the Key File Using the Key Database Manager" on page 80.

8 To verify that the encryption level has been upgraded, note if the timestamp for keyfile.bin matches the time when you executed the keydbupgrade utility.

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

a Add a new encryption key.

For information, see "Adding New Encryption Keys" on page 81.

b Change the Siebel administrator password so that it is reencrypted using the new encryption algorithm provided by Siebel Strong Encryption. For information on this task, refer to one of the following topics:

- "Changing System Administrator Passwords on Microsoft Windows" on page 37. After changing the password, delete the Siebel Server system service and re-create it using the new password.
- "Changing the Siebel Administrator Password on UNIX" on page 40

c Reencrypt Gateway Name Server parameters that are encrypted in the siebns.dat file.

For information, see "Reencrypting Password Parameters in the Siebns.dat File" on page 92.

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

SIEBEL_ROOT\siebsrvr\admin\

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

For information on this task, see "About Upgrading Data to a Higher Encryption Level" on page 82.

Reencrypting Password Parameters in the Siebns.dat File

This topic provides information on how to reencrypt Gateway Name Server parameters that are encrypted in the siebns.dat file after you have increased the level of encryption you use with Siebel Business Applications. For information on how to increase the encryption level using Siebel Strong Encryption, see "About Siebel Strong Encryption" on page 87 and "Increasing the Encryption Level" on page 89.

Masked parameters are parameters that have their values encrypted. In the siebns.dat file, parameters that specify password values are masked when they are written to the file. You must reencrypt masked parameters after increasing the encryption level because otherwise the Siebel Server attempts to decrypt the encrypted password using the original encryption key and compares the result to the password entered. If this happens, then the Siebel Server writes an error to the keydbmgr.log log file.

Table 8 on page 93 lists the parameters that are encrypted in the siebns.dat file that must be reencrypted when you increase the encryption level. Most, but not all, of the masked parameters are Siebel Server parameters that can be changed using the Server Manager program. The following procedure describes how to reset encrypted parameters to use a new encryption level using Server Manager.

NOTE: In Siebel CRM Innovation Pack 2014, passwords in the siebns.dat file are encrypted using AES encryption. If you are upgrading to the current release, reset encrypted passwords in the siebns.dat file so that they now use AES encryption. For additional information, see "About Encryption of Gateway Name Server Password Parameters" on page 48.

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

1. Log in to the Server Manager command-line interface (srvrmgr program). For more information on how to start and use the srvrmgr program, see *Siebel System Administration Guide*.
2. Change each of the masked parameters so that it uses the increased encryption level; see Table 8 on page 93 for a list of the masked parameters.

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

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

Table 8 lists the parameters that you must reencrypt if you increase the encryption level and indicates how you can reencrypt each parameter.

Table 8. Encrypted Parameters

Parameter	Description	How to Reencrypt the Parameter
ApplicationPassword	This parameter is defined for named subsystems of type InfraSecAdpt_LDAP [the default names are LDAPSecAdpt and ADSISecAdpt]. This parameter is set if LDAP or ADSI security adapter authentication is used.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file.
CRC CustomSecAdpt_CRC	These parameter are defined for named subsystems of type InfraSecAdpt_DB, InfraSecAdpt_LDAP, or InfraSecAdpt_Custom. These parameters specify the checksum validation value for the security adapter DLL file and are set for LDAP, ADSI, database, and custom security adapters. For further information on checksum validation, see "Configuring Checksum Validation" on page 149. **CAUTION:** Do not reset or change the value of the DBSecAdpt_CRC parameter. Changing the value of the CRC parameter for the database security adapter can disrupt the correct functioning of your Siebel application.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file.
ClientDBAPwd	This parameter is specified for the Database Extract server component.	Use the Server Manager command.
DSPassword	This parameter is defined for named subsystems of type InfraDataSource (it can be set for the ServerDataSrc named subsystem, or another data source). It is specified for database security adapter authentication.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file.
DSPrivUserPass PrivUserPass	These parameters are specified for the Generate Triggers Siebel Server component.	Use the Server Manager command.

Table 8. Encrypted Parameters

Parameter	Description	How to Reencrypt the Parameter
DbaPwd NewDbaPwd	These parameters are specified for the Generate New Database Siebel Server component used with Siebel Remote.	Use the Server Manager command. For information on changing these parameters, see *Siebel Remote and Replication Manager Administration Guide*.
ExtDBPassword	This parameter provides credentials for the database specified in the external database subsystem.	Use the Server Manager command.
KeyFilePassword	The key file stores the encryption keys that encrypt and decrypt data. The file is encrypted with the key file password.	Using the Key Database Manager utility. For further information, see "Changing the Key File Password" on page 81. This parameter is also changed in the eapps.cfg file.
MailPassword	This parameter is set for the email account that Siebel Email Response uses to connect to the SMTP/POP3 or SMTP/IMAP email servers.	Use the Server Manager command. For information on this parameter, see the topics on assigning parameter overrides for a communications profile in *Siebel Email Administration Guide*.
Password	This parameter, set at the Siebel Enterprise level, is the password for the system user (for example, SIEBADMIN) specified by the Username parameter. It is recommended that you do not change the value for this parameter when you reencrypt it.	Use the Server Manager command.

Table 8. Encrypted Parameters

Parameter	Description	How to Reencrypt the Parameter
TableOwnPass	This parameter specifies the password for the Database Table Owner (DBO) account, which is used to modify the Siebel database tables.	Siebel Web Clients can use the Server Manager command. Siebel Developer Web Clients must edit the appropriate application configuration file. Change the parameter in the Siebel database. See "Changing the Table Owner Password" on page 42 for instructions.
TrustToken CustomSecAdpt_TrustToken	These parameters apply in a Web SSO environment only, and are defined for named subsystems of type InfraSecAdpt_LDAP and InfraSecAdpt_Custom. These parameters are also specified for the SWSE; the setting must be the same on both the SWSE and the security adapter.	Siebel Web Clients can use the Server Manager command. Siebel Mobile Web Clients or Developer Web Clients must edit the appropriate application configuration file. Edit the eapps.cfg file for SWSE.

Security Considerations for Unicode Support

Siebel Business Applications support Unicode. For comprehensive Unicode compliance, consider the following encryption and authentication issues.

Using Non-ASCII Characters in a Unicode Environment

- For database authentication, the user ID and password must use characters that are supported by the Siebel database.
- Login problems might 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 In to a Siebel Application

Make sure that the characters used in the login form are supported by the Siebel database.

Encrypted Data

Siebel Business Applications provide AES encryption to encrypt data for sensitive information such as credit card numbers. For encryption with Unicode, you *must* use AES encryption, rather than the Standard Encryptor, which is no longer supported. For more information, see "About Data Encryption" on page 74.

5 Security Adapter Authentication

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

- About User Authentication on page 97
- Comparison of Authentication Strategies on page 99
- About Siebel Security Adapters on page 100
- About Database Authentication on page 102
- Implementing Database Authentication on page 103
- Implementing Database Authentication with MS SQL Server on page 104
- About LDAP or ADSI Security Adapter Authentication on page 106
- Requirements for the LDAP Directory or Active Directory on page 111
- About Installing LDAP Client Software on page 115
- Process of Installing and Configuring LDAP Client Software on page 116
- Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard on page 123
- Process of Implementing LDAP or ADSI Security Adapter Authentication on page 128
- About Migrating from Database to LDAP or ADSI Authentication on page 145
- Security Adapter Deployment Options on page 146
- About Password Hashing on page 158
- Process of Configuring User and Credentials Password Hashing on page 160
- Running the Password Hashing Utility on page 163
- About Authentication for Gateway Name Server Access on page 165
- Implementing LDAP or ADSI Authentication for the Gateway Name Server on page 166
- Security Adapters and the Siebel Developer Web Client on page 167
- About Authentication for Mobile Web Client Synchronization on page 170
- About Securing Access to Siebel Reports on page 172

About User Authentication

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

- **Security adapter authentication.** Siebel Business Applications provide a security adapter framework to support several different user authentication scenarios:
  - **Database authentication.** Siebel Business Applications support authentication against the underlying database. In this architecture, the security adapter authenticates users against the Siebel database. Siebel Business Applications provide a database security adapter (it is configured as the default security adapter).
  - **Lightweight Directory Access Protocol (LDAP) or Active Directory Service Interfaces (ADSI) authentication.** Siebel Business Applications support authentication against LDAP-compliant directories or Microsoft Active Directories. In this architecture, the security adapter authenticates users against the directory. Siebel Business Applications provide the following two security adapters to authenticate against directory servers:
    - ADSI Security Adapter
    - LDAP Security Adapter

    For more information, see "About LDAP or ADSI Security Adapter Authentication" on page 106.
  - **Custom.** You can use a custom adapter you provide, and configure the Siebel Business Applications to use this adapter. For more information, see "Security Adapter SDK" on page 23.
- **Web Single Sign-On (Web SSO).** This approach uses an external authentication service to authenticate users before they access the Siebel application. In this architecture, a security adapter does not authenticate the user. The security adapter simply looks up and retrieves a user's Siebel user ID and database account from the directory based on the identity key that is accepted from the external authentication service. For more information, see Chapter 6, "Web Single Sign-On Authentication."

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

Configuration parameter values determine how your authentication architecture components interact. For information about the purpose of configuration parameters, see Appendix A, "Configuration Parameters Related to Authentication." For information about the seed data related to authentication, user registration, and user access that is installed with Siebel Business Applications, see Appendix B, "Seed Data."

Authentication for Self-Service Applications

If you are using LDAP, ADSI, or Web Single Sign-On authentication with the Siebel Self-Service Applications available with Siebel CRM Release 8.1, then see the following Siebel Self-Service Applications documentation for additional information on user authentication:

- *Siebel Self-Service Application Deployment Guide*
- *Siebel Self-Service Application Developer's Guide*

Issues for Developer and Mobile Web Clients

The following special issues apply for authentication for deployments using Siebel Developer Web Client or Mobile Web Client:

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

Comparison of Authentication Strategies

Table 9 highlights the capabilities of each authentication approach to help guide your decision. Several options are available for each basic strategy. Comparisons do not apply for Siebel Mobile Web Client, for which only database authentication is available.

Table 9. Functionality Supported in Different Authentication Approaches

Functionality	Database Security Adapter	LDAP or ADSI Security Adapter	Web SSO
Requires additional infrastructure components.	No	Yes	Yes
Centralizes storage of user credentials and roles.	No	Yes	Yes
Limits number of database accounts on the application database.	No	Yes	Yes
Supports dynamic user registration. Users are created in real-time through self-registration or administrative views.	No	Yes	Siebel Business Applications do not support the feature, but it might be supported by third-party components For Web SSO, user registration is the responsibility of the third-party authentication architecture. It is not logically handled by the Siebel architecture.

Table 9. Functionality Supported in Different Authentication Approaches

Functionality	Database Security Adapter	LDAP or ADSI Security Adapter	Web SSO
Supports account policies. You can set policies such as password expiration, password syntax, and account lockout.	Only password expiration is supported and only on supported IBM DB2 RDBMS operating systems.	Yes	Siebel Business Applications do not support the feature, but it might be supported by third-party components. For Web SSO, account policy enforcement is handled by the third-party infrastructure.
Supports Web Single Sign-On, the capability to log in once and access all the applications within a Web site or portal.	No	No	Yes

The Siebel LDAP security adapter supports the Internet Engineering Task Force (IETF) password policy draft (09) for handling password policy violations and error reporting. As a result, the LDAP security adapter returns meaningful error messages and takes appropriate actions when password policy violations occur, provided the adapter is used with directory servers that are compliant with the draft. For additional information on the IETF password policy draft, go the IETF Web site at

http://tools.ietf.org/html/draft-behera-ldap-password-policy-09

About Siebel Security Adapters

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

- Database security adapter (enabled by default)

  For more information, see "About Database Authentication" on page 102.

- ADSI (Active Directory Services Interface) security adapter
- LDAP (Lightweight Directory Access Protocol) security adapter

The security adapter is a plug-in to the authentication manager. The security adapter uses the credentials entered by a user (or supplied by an authentication service) to authenticate the user, as necessary, and allow the user access to the Siebel application.

You can implement a security adapter other than one of those provided by Siebel Business Applications provided the adapter you implement supports the Siebel Security Adapter Software Development Kit. For more information, see "Security Adapter SDK" on page 23.

You can implement LDAP or ADSI authentication for application object manager components and for EAI components. Do not use the ADSI security adapter or LDAP security adapter to authenticate access to batch components such as, for example, the Communications Outbound Manager. Configure batch components to use the database security adapter instead. Batch components access the Siebel database directly and, as a result, must use the database security adapter. Note also that Siebel Server infrastructure and system management components such as Server Manager, Server Request Broker, and Server Request Processor access the Siebel database directly. For this reason, these components cannot use the LDAP or ADSI security adapter.

Authentication Directories

An LDAP directory or an Active Directory is a store in which information that is required to allow users to connect to the Siebel database, such as database accounts or Siebel user IDs, is maintained external to the Siebel database, and is retrieved by the security adapter. For specific information about third-party directory servers supported by the security adapters provided with Siebel Business Applications, see "Directory Servers Supported by Siebel Business Applications" on page 107 and the Certifications tab on My Oracle Support.

Security Adapter Authentication

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

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

Depending on how you configure your authentication architecture, the security adapter might function in one of the following modes, with respect to authentication:

- **With authentication (LDAP or ADSI security adapter authentication mode).** The security adapter uses credentials entered by the user to verify the user's existence and access rights in the directory. If the user exists, then 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 security adapter passes an identity key supplied by a separate authentication service to the directory. Using the identity key to identify the user in the directory, the adapter retrieves the user's Siebel user ID, a database account, and, optionally, a set of roles that are passed to the 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: The security adapter does not provide authentication for Web SSO. Web SSO is the ability to authenticate a user one time for access to multiple applications, including Siebel Business Applications. However, when implementing Web SSO, you must also deploy a security adapter.

For information on the most commonly reported error messages when implementing standard Siebel security adapters, see 477528.1 (Article ID) on My Oracle Support.

Event Logging for Siebel Security Adapters

Siebel Business Applications provide the following event types to set log levels for security adapters:

- Security Adapter Log

  This event type traces security adapter events.

- Security Manager Log

  This event type traces security manager events.

Modify the values for these two event types to set the log levels that the Application Object Manager writes to the log file. For more information about how to set the log levels for event types, see *Siebel System Monitoring and Diagnostics Guide*.

About Database Authentication

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

Database Authentication Process

The stages in a database authentication process are:

1. The user enters a database account's user name and password to a Siebel application login form.
2. The Siebel Web Server Extension (SWSE) passes the user credentials to the Application Object Manager, which in turn passes them to the authentication manager.
3. The authentication manager hashes the password, if DBHashUserPwd is TRUE for the data source specified for the database security adapter, and passes the user credentials to the database security adapter.
4. If the user credentials match a database account, then the user is logged into the database and is identified with a user record whose user ID is the same as the database account's user name.

   In other words, the database security adapter validates each user's credentials by trying to connect to the Siebel database.

Features Not Available for Database Authentication

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

- A single user-authentication method that is valid for Siebel Business Applications and other applications

- User self-registration (typically used with customer applications)
- External delegated administration of users (typically used with partner applications)
- Creation of users from the Administration - User screen in the Siebel application

Implementing Database Authentication

This topic describes how to implement database authentication. Database authentication is typically implemented for a Siebel employee application, such as Siebel Call Center or Siebel Sales. Database authentication is configured as the default authentication method and is the easiest of the authentication approaches supported by Siebel Business Applications to implement.

About Implementing the Database Security Adapter

Although configuration might not be required, you can implement the database security adapter using the Security Adapter Mode (SecAdptMode) and Security Adapter Name (SecAdptName) parameters. The Security Adapter Mode and Security Adapter Name parameters can be set for the Siebel Gateway Name Server, the Siebel Enterprise Server, for a particular Siebel Server, for an individual Application Object Manager component, or for the Synchronization Manager component (for Siebel Remote).

You can configure the Security Adapter Mode and Security Adapter Name parameters using Siebel Server Manager. To do this, you specify parameter values for a named subsystem (enterprise profile). For the Developer Web Client, parameters can be configured by editing the application configuration file directly. For Gateway Name Server authentication, parameters can be configured by editing the gateway.cfg file.

CAUTION: If you want to configure a server component or a Siebel Server to use different database authentication settings than those already configured at a higher level (that is, configured for the Siebel Enterprise or Siebel Server), then you must create a new database security adapter. If you do not, then settings you make reconfigure the existing security adapter wherever it is used.

The following procedure describes how to implement database authentication.

To implement database authentication

1. Specify that you want to use the database security adapter by setting values for the following parameters:
   a. Set the Security Adapter Mode parameter to DB (the default value).
   b. Set the Security Adapter Name parameter to DBSecAdpt (the default value), or to a security adapter (enterprise profile or named subsystem) with a different name.

   For more information about parameters for the database security adapter, see Appendix A, "Configuration Parameters Related to Authentication."

2 If you want to implement user password hashing, then set the Hash User Password parameter to True.

For detailed information on this task, see "Configuring User Password Hashing" on page 161.

User password hashing maintains a hashed password in the database account while an unhashed version of the password is provided to the user for logging in. When user password hashing is enabled, a hashing algorithm is applied to the user's password before it is compared to the hashed password stored in the database. It is recommended that you implement password hashing for user passwords.

NOTE: For database authentication, password hashing parameters are specified for a data source referenced from the database security adapter, rather than specified directly for the security adapter.

3 Provide each user with access to Siebel Business Applications and the Siebel database as follows:

a Create a database account for the user using your database management functionality.

b Create a Siebel user record in the Siebel database; the user ID must match the user name for the database account.

You add users to the Siebel database through an employee application such as Siebel Call Center. For detailed information about adding users, see "About Adding a User to the Siebel Database" on page 241.

4 If you are implementing database authentication with an MS SQL Server database, then perform the task described in "Implementing Database Authentication with MS SQL Server" on page 104.

About Password Expiration

If you use database authentication, then it is recommended that you implement database password expiration policies on the database server if this functionality is supported by your RDBMS. For example, it is recommended that you configure database passwords to expire after a defined time period unless they are changed.

On some RDBMSs this functionality is provided by default; on others this functionality, if provided, must be configured. For information on the password expiration policies supported by your RDBMS, see the appropriate RDBMS vendor documentation.

NOTE: Support for password expiration policies and database user account password change through Siebel Business Applications is available only on supported IBM DB2 RDBMS operating systems.

Implementing Database Authentication with MS SQL Server

This topic describes additional tasks you must perform when implementing database authentication if you are using Siebel Business Applications with an MS SQL Server database. For information on implementing database authentication, see "Implementing Database Authentication" on page 103.

When you install the Siebel Server, an ODBC data source name (DSN) is created, which the Siebel Server uses to connect to the Siebel database. If you implement database authentication, and you are using Siebel Business Applications with a Microsoft SQL Server database, then make sure that you select the correct ODBC DSN configuration settings; if you do not, Siebel Web Clients can log in to the Siebel application without providing a password.

When you configure the ODBC DSN settings for an MS SQL Server database, you can choose from the following authentication options:

- Windows NT authentication using the network login ID

  This option allows users to access applications on the server by entering a network login ID only. If you select this option, then Siebel Web Clients attempting to access the Siebel application are not required to enter a password.

- SQL Server authentication using a login ID and password entered by the user

  This option requires users attempting to access applications on the server to enter a valid user ID and password. Select this option to make sure that Siebel Web Clients must enter both a Siebel user ID and a password to access the Siebel application.

The following procedure describes how to set the MS SQL Server ODBC data source settings on your Siebel Server.

To set ODBC data source values for MS SQL Server

1. On the Siebel application server, from the Start menu, choose Settings, Control Panel, Administrative Tools, and then the Data Sources (ODBC) item.
2. On the ODBC Data Source Administrator dialog box, select the System DSN tab.
3. Select the Siebel data source name, and click Configure. The default Siebel data source name (DSN) is *EnterpriseName*_DSN, where *EnterpriseName* is the name you assigned the Siebel Enterprise when you configured it.

   The Microsoft SQL Server DSN Configuration screen appears.
4. You are presented with the following authentication options:
   - Windows NT authentication using the network login ID.

     Do not select this option.
   - SQL Server authentication using a login ID and password entered by the user.

     Select this option to make sure that Siebel Web Clients must enter both a Siebel user ID and a password to access the Siebel application.
5. Amend any other configuration options as required, then click Next.
6. Click Finish.

About LDAP or ADSI Security Adapter Authentication

Siebel Business Applications include security adapters that are based on the LDAP and ADSI standards, allowing customers to use LDAP directory products or Microsoft Active Directory (AD) for user authentication. LDAP or ADSI security adapter authentication can offer the following benefits:

- User authentication external to the database
- Automatic updating of the directory with new or modified user information entered through the Siebel Business Applications user interface by an internal administrator, a delegated administrator, or a self-registering user

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

The process of implementing security adapter authentication is similar for both the LDAP and ADSI security adapters although there are some differences, for example:

- You must install the Oracle Database Client on the Siebel Server computer if you choose the LDAP security adapter. For more information, see "Process of Installing and Configuring LDAP Client Software" on page 116.
- How you configure communications encryption between the Siebel security adapter and the directory server differs depending on the security adapter you use. In addition, SSL encryption is supported with the LDAP security adapter and TLS encryption is supported with the ADSI security adapter. For more information, see "Configuring Secure Communications for Security Adapters" on page 150.

For additional information about the LDAP and ADSI security adapters, see

- "LDAP and ADSI Security Adapter Authentication Process" on page 106
- "Directory Servers Supported by Siebel Business Applications" on page 107
- "Comparison of LDAP and ADSI Security Adapters" on page 107

LDAP and ADSI Security Adapter Authentication Process

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

1. The user enters credentials to a Siebel Business Applications login form.

   These user credentials (a user name and password) can vary depending on the way you configure the security adapter. For example, the user name could be the Siebel user ID or an identifier such as an account or telephone number. The user credentials are passed to the Siebel Web Server Extension (SWSE) and then to the Application Object Manager, which in turn passes them to the authentication manager.

2 The authentication manager determines how to process the user credentials and calls the security adapter to validate the credentials against the directory.

NOTE: The ADSI security adapter and the LDAP security adapter used with the Oracle LDAP Client allow special characters in passwords. Be aware, however, that only a limited number of special characters are supported for use in Siebel passwords. For additional information, see "Characters Supported in Siebel Passwords" on page 34.

3 The security adapter returns the Siebel user ID and a database credential assigned to this user to the authentication manager. (If roles are used, they are also returned to the authentication manager.)

4 The Application Object Manager (or other module that requested authentication services) uses the returned credentials to connect the user to the database and to identify the user.

Directory Servers Supported by Siebel Business Applications

This topic outlines the directory servers supported by the Siebel LDAP and ADSI security adapters.

Siebel Business Applications support the following directories:

- **LDAP directory servers.** Siebel Business Applications support any directory server that meets *both* of the following requirements:
  - The LDAP directory server is compliant with the LDAP 3.0 standard
  - Password management is handled in *either* one of the following ways:
    - The directory server implements the IETF password policy draft (09) standard
    - Password management functions, such as password expiry and other password-messaging features, are handled externally to the directory server
- **Active Directory servers.** Siebel Business Applications support any Active Directory server that is supported by Microsoft.

  Siebel support for Microsoft Active Directory requires the native connector shipped with the operating systems that are supported for Siebel Business Applications on Microsoft Windows servers. Support for Active Directory is limited to *either*:
  - Specific active directory connectors based on the operating systems supported by the release. The Active Directory connector used to connect with an Active Directory schema must be deemed compatible by Microsoft.
  - Use of only the LDAP version 3-compliant set of features supported by Active Directory. In this instance, Active Directory functions as an LDAP server.

Comparison of LDAP and ADSI Security Adapters

This topic outlines the differences in functionality provided by the LDAP and ADSI security adapters. The relative benefits of each type of security adapter are shown in Table 10 on page 108.

The ADSI security adapter can authenticate against ADSI-compliant directories (Microsoft Active Directory). The ADSI security adapter can only be used with Microsoft Windows operating systems. If you want to authenticate against Microsoft Active Directory and you are using a non-Windows operating system such as Linux or HP-UX, you must use the LDAP security adapter.

The LDAP security adapter can be used to authenticate against supported LDAP-compliant directories and is also supported for integration to Active Directory. It is recommended that you use the LDAP security adapter for authenticating against both Active Directory and LDAP-based external directories. The LDAP security adapter is standards-based, it supports the IETF password policy draft (09) standard for handling passwords, and it can be used on multiple computer platforms.

If you use the LDAP security adapter to authenticate users against Active Directory, and if you want to manage user passwords or create new users in the Active Directory, then you must configure SSL between the LDAP security adapter and the Active Directory. Implementing SSL in these circumstances is a requirement of Microsoft Windows and Active Directory.

NOTE: SSL encryption is supported with the LDAP security adapter. TLS encryption is supported with the ADSI security adapter. The SSL encryption standard is not secure. It is recommended that you implement additional methods of securing connections between the LDAP security adapter and directory servers.

Table 10. Comparison of LDAP and ADSI Security Adapter Functionality

Functionality	LDAP Security Adapter	LDAP Security Adapter with AD Directory	ADSI Security Adapter
Shared database account credentials can be stored as security adapter profile parameters eliminating the necessity for a shared credentials user record in the external directory.	Yes	Yes	Yes
Password expiration warning.	Yes Provided the directory server implements the IETF password policy draft (09) standard	Yes	Yes

Table 10. Comparison of LDAP and ADSI Security Adapter Functionality

Functionality	LDAP Security Adapter	LDAP Security Adapter with AD Directory	ADSI Security Adapter
Administration of the directory through Siebel Business Applications (manage user passwords or create new users). For additional information, see "About Administering the Directory through Siebel Business Applications" on page 109.	Yes	Yes, provided that SSL is enabled between the LDAP security adapter and the Active Directory server.	Yes, provided that the Active Directory client can establish a secure connection to the Active Directory server. This can be achieved by: ■ Including all systems as part of a single Microsoft Windows domain forest ■ By configuring TLS
Communication with more than one directory server.	See "Communicating with More Than One Authentication Server" on page 110.		

About Administering the Directory through Siebel Business Applications

If you choose to administer the LDAP or Active Directory directory through Siebel Business Applications, then be aware that in large implementations timeout issues can occur, particularly if using the ADSI security adapter. To prevent timeout issues:

- Use the LDAP security adapter.
- Do not set the Base DN to the root level of your directory server.

For help with overall design recommendations and performance improvement, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.

Using the LDAP Security Adapter with Active Directory: Setting the Base DN

If you use the LDAP security adapter with Active Directory, then problems can occur if you set the base distinguished name (Base DN), which specifies the root directory under which users are stored, to the root level of the Active Directory.

When the LDAP security adapter searches the Active Directory, it searches everything under the Base DN. If the Base DN is set to the Active Directory root, then the LDAP security adapter searches all directory entities, including configuration and schema entities to which the application user does not have access. To prevent this situation from occurring, do not set the base DN to the Active Directory root directory; this recommendation also applies to implementations in which the ADSI security adapter performs the authentication function.

Communicating with More Than One Authentication Server

This topic describes the specific circumstances in which the LDAP and ADSI security adapters can connect to more than one directory server, either to authenticate users in more than one directory, or for failover purposes.

ADSI Security Adapter

The ADSI security adapter does not support authentication of users in different domains or forests. However, the ADSI security adapter can connect to multiple AD servers for authentication or failover purposes provided that the following conditions are met:

- The Active Directory servers are all in the same domain
- The Siebel Server is in the same domain as the Active Directory servers or, if the Siebel Server is in a different domain to the Active Directory servers, a trust relationship exists between the two domains

To enable the ADSI security adapter to connect to multiple AD servers, specify the NetBIOS name of the domain containing the Active Directory servers, instead of the name of a specific Active Directory server, for the Server Name parameter of the ADSI security adapter profile.

LDAP Security Adapter

The LDAP security adapter provided with Siebel Business Applications currently does not support communication with more than one directory server. However, the following options are available:

- Failover functionality can be implemented to a limited degree for the LDAP security adapter. To implement failover functionality, specify the names of the primary and secondary servers for the Server Name parameter of the LDAP security adapter profile. For example:

  ```
  ServerName=ldap1 ldap2
  ```

  If communication cannot be established between the Siebel Application Object Manager and the primary LDAP server, then failover to the secondary LDAP server occurs. If the Application Object Manager can communicate with the primary server, but LDAP functionality on the server is not available, then failover to the secondary server does not occur.

- Oracle provides products, for example, Oracle Virtual Directory, that enable LDAP security adapters to communicate with multiple LDAP-compliant directories and Active Directories. For additional information on Oracle Virtual Directory, go to

  http://www.oracle.com/technetwork/testcontent/index-093158.html

Requirements for the LDAP Directory or Active Directory

If you implement LDAP or ADSI security adapter authentication with Siebel Business Applications, then you must provide a directory product that meets the requirements outlined in this topic. The directory product you provide can be one of the directory servers supported by the security adapters provided with Siebel Business Applications, or another directory server of your choice. The following options are available:

- If you provide one of the directory servers supported by Siebel Business Applications (that is, a supported LDAP directory or Microsoft Active Directory), then you can use a security adapter provided by Siebel Business Applications, or you can create your own security adapter that complies with Siebel Business Applications.
- If you provide a directory other than those supported by the security adapters provided with Siebel Business Applications, then you are responsible for implementing a security adapter that supports this directory.

For specific information about directory server products supported by Siebel Business Applications, see the Certifications tab on My Oracle Support.

LDAP Security Adapter Requirements

If you are using LDAP authentication, then you must install the Oracle Database Client software that is provided with Siebel Business Applications. Your Siebel application uses DLL files provided by the Oracle Database Client to communicate with the supported LDAP directory server product you have chosen to use. For Oracle Database Client installation instructions, see "Process of Installing and Configuring LDAP Client Software" on page 116.

ADSI Security Adapter Requirements

If you are running the Siebel Server on supported Microsoft Windows operating systems and you are using ADSI authentication, then you must meet the requirements described in this topic. For more information about some of these requirements, refer to your Microsoft Active Directory documentation.

The ADSI security adapter requirements are:

- To allow users to set or change passwords, the Active Directory client software must be able to establish a secure connection to the Active Directory server. This requirement can be met in multiple ways:
  - Including all systems as part of a single Microsoft Windows domain forest

    It is recommended that all Siebel Servers and Active Directory servers be located in the same domain forest.
  - Configuring trust relationships

- Configuring Transport Layer Security (TLS)

  To perform user management in the Active Directory through the Siebel client, you must configure the Active Directory server at the server level for TLS communications between the Active Directory client and server. This is different from TLS communications between the security adapter and the directory, which is configured through Siebel Business Applications.

- Specify a specific user for the Siebel service owner account and define this Siebel service user:
  - On each Siebel Server computer in the Siebel Enterprise
  - In the Siebel Server Active Directory domain
  - In the Active Directory server domain, that is, the domain the ADSI security adapter connects to in order to retrieve Siebel user credentials
- DNS servers on your network must be properly configured with DNS entries for Active Directory. Client computers using the ADSI security adapter must be configured to be able to retrieve these entries from the appropriate DNS servers.
- If you require ADSI security adapter functionality for Siebel Developer Web Client deployments, then you must install the ADSI client software on each such client computer, where applicable.

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

About Setting Up the LDAP Directory or Active Directory

To provide user access to a Siebel application implementing an LDAP or ADSI security adapter, the Siebel application must be able to retrieve credentials to access the database and the user's Siebel user ID. Therefore you must set up a directory from which a database account and a Siebel user ID can be retrieved for each user.

Your LDAP directory or Active 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. You can have any amount of white space between the two key-value pairs, but you cannot have any space within each pair. The keywords, username and password, must be lowercase.

  If you choose, you can configure a designated directory entry to contain credentials of a database account that is shared by many users; this is the shared database account. If you implement a shared database account, then you can specify the value for the shared database account user name and password in profile parameters for the LDAP Security Adapter profile or the ADSI Security Adapter profile instead of in an attribute value for the directory entry. For more information, see "Configuring the Shared Database Account" on page 151.

  NOTE: Even if you use a shared database account with external directory authentication, you must create a separate database account for any user who requires administrator access to Siebel Business Applications functionality, for example, any user who has to perform Siebel Server management and configuration tasks. The database account user ID and password you create for the user must match the user ID and password specified for the user in the external directory.

- **Username.** This attribute value is the key passed to the directory that identifies the user. In a simple implementation, the user name might be the Siebel user ID, and so it might not have to be a separate attribute.

- **Password.** The storage of a user's login password differs between LDAP servers and Active Directory servers.

  - **LDAP.** Whether or not the password is stored in the directory depends on whether or not you are using Web SSO:

    - If the user authenticates through the LDAP directory using the LDAP security adapter, then the login password must be stored in the userPassword attribute of the LDAP directory.
    - If the user authenticates through Active Directory using the LDAP security adapter, then the login password must be stored in either the UserPassword or the unicodePWD attribute of the LDAP directory, depending on the code page used by the directory server.
    - If the user is authenticated by an authentication service, such as in a Web SSO implementation, then a password attribute is not required.

    The Password Attribute Type parameter is used to specify the attribute type under which the user's login password is stored in the directory. For additional information on the Password Attribute Type parameter, see "Siebel Gateway Name Server Parameters" on page 361.

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

    - If the user authenticates through Active Directory using the ADSI security adapter, then the login password must be provided.
    - If the user is authenticated by an authentication service, such as in a Web SSO implementation, then a password is not required.

It is recommended that you implement password hashing for both user passwords and database credentials stored in the directory. You can also define access control lists (ACLs) to restrict access to directory objects containing password information. For information on setting up directory ACLs, see your directory vendor documentation. For information on password hashing, see "About Password Hashing" on page 158.

You can use additional user attributes to store data, for example, first and last name, as required by your authentication solution.

If you create a new attribute object for your directory to store Siebel attributes (for example, Siebel User ID), then you can use the Private Enterprise Number that Siebel Business Applications has registered with the Internet Assigned Numbers Authority (http://www.iana.org) to provide a unique X.500 Object ID. This number is 1.3.6.1.4.1.3856.*.

An additional type of data, *roles*, is supported, but is not required. Roles are an alternate means of associating Siebel responsibilities with users. Responsibilities are typically associated with users in the Siebel database, but they can instead be stored in the directory. Leave role values empty to administer responsibilities from within Siebel Business Applications. For more information, see "Configuring Roles Defined in the Directory" on page 157.

About Creating the Application User in the Directory

Depending on your authentication and registration strategies, and the options that you implement for your deployment, you must define a user, called the application user, in the directory.

The application user is the only user who can read or write user information in the directory. Therefore, it is critical that the application user has appropriate search and write privileges to the directory. For information on creating the application user, see "Configuring the Application User" on page 147.

For ADSI authentication, it is recommended that you use the Active Directory Delegation Control Wizard to define privileges for users in Active Directory.

NOTE: If you are configuring an ADSI security adapter, then the application user must either be a domain user or have access to the directory server. If the application user cannot access the directory server, then the authentication process fails.

Verifying the Active Directory Client Installation

The following procedure describes how to verify that the Active Directory client is successfully installed.

To verify an Active Directory client installation

1. Navigate to the system32 subdirectory of the installation location for the Microsoft Windows operating system (for example, `C:\WINDOWS\system32`).
2. Verify that the correct versions of each DLL required for the Active Directory client are present in the subdirectory (for example, the files adsiis.dll and adsiisex.dll). For more information, refer to Microsoft's documentation.

3 For each DLL, right-click on the file and choose Properties.

4 Click the Version tab to see the version number.

About Installing LDAP Client Software

You must install the Oracle Database Client and Oracle Wallet Manager software if you implement LDAP security adapter authentication. The Oracle Database Client allows Siebel Business Applications to authenticate against supported LDAP directory servers when used with the LDAP security adapter. Oracle Wallet Manager, optionally installed with the Oracle Database Client, allows Siebel Business Applications to communicate with supported LDAP directory servers over SSL.

NOTE: The SSL encryption standard is not secure. It is recommended that you implement additional methods of securing connections between the LDAP security adapter and directory servers.

Consider the following requirements for the Oracle Database Client installation in a Siebel environment:

- The Oracle Database Client must be installed on each Siebel Server computer for which LDAP authentication is to be supported using the LDAP security adapter. The Oracle Database Client software can be installed either before or after you install the Siebel Server.
- For Siebel Developer Web Client deployments for which LDAP authentication is to be supported, the Oracle Database Client must be installed on each local client computer. The Oracle Database Client software can be installed either before or after you install the Siebel Developer Web Client.
- Oracle Wallet Manager must be installed if you are supporting SSL. Oracle Wallet Manager is an application you use to generate wallets, which are containers that store authentication and signing credentials, such as trusted certificates, which are required for Siebel Business Applications to communicate with LDAP directory servers over SSL. Oracle Wallet Manager can be installed on any computer using a supported operating system. If you require this module, then you only have to install it once for each deployment.

The Oracle Database Client and Oracle Wallet Manager software are available from the Siebel installation image directory, provided the ORACLE LDAP Client option was selected when the Siebel installation image was created. For information about creating a Siebel installation image, see the *Siebel Installation Guide* for the operating system you are using.

NOTE: If you are using LDAP security adapter authentication, you must install the Oracle Database Client provided with the current Siebel Innovation Pack, even if you are using Siebel Business Applications with an Oracle Database and have previously installed the Oracle Database Client. Siebel Innovation Packs provide the most recent version of the Oracle Database Client, which is required for LDAP authentication. Be aware that only one Oracle Database Client can be used in a Siebel CRM implementation, so if you install the Oracle Database Client provided with a Siebel Innovation Pack to enable LDAP authentication, you must also use this client to connect to your Oracle Database.

Process of Installing and Configuring LDAP Client Software

This topic outlines the steps involved in installing and configuring the Oracle Database Client and Oracle Wallet Manager.

To install the Oracle LDAP client software, and to configure it for your environment, perform the following tasks:

1. Review "Considerations if Using LDAP Authentication with SSL" on page 116
2. Perform one of the following tasks, as appropriate:
   - "Installing the LDAP Client Software on Windows" on page 117
   - "Installing the LDAP Client Software on UNIX" on page 117
3. (UNIX operating systems only) "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 119
4. (Optional) "Creating a Wallet for Certificate Files When Using LDAP Authentication with SSL" on page 121

Considerations if Using LDAP Authentication with SSL

This topic provides information on using LDAP authentication with SSL. The Oracle Database Client requires that Oracle Wallet Manager is installed if SSL must be supported. The LDAP libraries and utilities provided with the Oracle Database Client use the SSL libraries provided with Oracle Wallet Manager.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 116.

- If Oracle Wallet Manager is installed, then the LDAP libraries dynamically load the SSL libraries and use them to enable SSL, when SSL is configured.
- If Oracle Wallet Manager is not installed and the SSL libraries are not available, then the LDAP library is fully functional, with the exception of SSL support.

By using SSL with server authentication, an LDAP application can use simple LDAP authentication (user ID and password) over an encrypted communication connection between the LDAP client application and the LDAP server. In addition, SSL provides data confidentiality (encryption) on connections protected by SSL. Authentication of servers to clients is accomplished with X.509 certificates.

NOTE: The SSL encryption standard is not secure. It is recommended that you implement additional methods of securing connections between the LDAP security adapter and directory servers.

It is assumed that SSL capability is, or will be, required for Siebel LDAP authentication. Therefore, the LDAP client installation process includes Oracle Wallet Manager installation as an integral part. If you are absolutely sure that SSL will never be turned on for Siebel LDAP authentication, then you do not have to install Oracle Wallet Manager.

Installing the LDAP Client Software on Windows

This topic describes how to obtain the Oracle Database Client installation files on Microsoft Windows and how to install the Oracle Database Client and Oracle Wallet Manager.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 116.

To install the Oracle Database Client and Oracle Wallet Manager on Windows

1. Log on to Microsoft Windows.
2. Navigate to the Siebel image location for the current release, then navigate to the directory `Release\Windows\Server_Ancillary\Oracle_LDAP_Client\enu`.
3. Copy the files in the `\enu` directory to a directory on the Siebel Server where you want to install the Oracle Database Client.
4. Install the Oracle Database Client, selecting the Runtime option when you are prompted to select the type of installation you want to perform.

   For detailed information on installing Oracle Database Client, see *Oracle® Database Client Installation Guide 11g Release 2 (11.2) for Microsoft Windows*. When the installation has completed, the following software is available on the Siebel Server:

   - Oracle LDAP SDK
   - Oracle LDAP client library
   - Oracle Wallet Manager

   NOTE: The Oracle LDAP client software components are embedded in the Oracle Database Client and are not listed as separately installed programs on the Siebel Server.
5. Set the value of the ORACLE_HOME environment variable to the location of the directory into which you installed the Oracle Database Client files, for example:

   ```
   set ORACLE_HOME=C:\oracle\SUN64\11gR2\11.2.0.3
   ```

   NOTE: If you are using Siebel Business Applications with an Oracle Database, and if you have a previous Oracle Database Client installation, change the value of ORACLE_HOME to specify the location of the Oracle Database Client you have just installed.
6. Set the value of the Security Adapter Dll Name parameter to sscforacleldap.dll.

   For information on the Security Adapter Dll Name parameter, see "Parameters for LDAP or ADSI Authentication" on page 364.
7. Stop and restart the Siebel Server.

Installing the LDAP Client Software on UNIX

This topic describes how to obtain the Oracle Database Client installation files on a UNIX operating system platform and how to install the Oracle Database Client and Oracle Wallet Manager.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 116.

To install the Oracle Database Client and Oracle Wallet Manager on UNIX

1. Login as root.
2. Navigate to the Siebel image location for the current release, then navigate to the directory Release/*UNIX_operating_system*/Server_Ancillary/Oracle_LDAP_Client/enu, where *UNIX_operating_system* is either Solaris, AIX, HP-UX, or Linux.

   The /enu directory contains the Oracle Database Client files and patches you must apply to the Oracle Database Client if you are using either the Solaris, AIX, or HP-UX operating systems.
3. Copy the files in the /enu directory to a directory on the Siebel Server where you want to install the Oracle Database Client. Make sure you also copy the appropriate patch for your operating system as follows:
   - **Solaris.** p16852128_112030_SOLARIS.zip
   - **AIX.** p12375092_112030_AIX.zip
   - **HP-UX.** p17758083_112030_HPUX-IA32.zip
4. Install the Oracle Database Client, selecting the Runtime option when you are prompted to select the type of installation you want to perform.

   For detailed information on installing Oracle Database Client, see *Oracle® Database Client Installation Guide 11g Release 2 (11.2) for Linux*. When the installation is completed, the following software is available on the Siebel Server:
   - Oracle LDAP SDK
   - Oracle LDAP client library
   - Oracle Wallet Manager

   NOTE: The Oracle LDAP client software components are embedded in the Oracle Database Client and are not listed as separately installed programs on the Siebel Server.
5. Set the value of the ORACLE_HOME environment variable to the location of the directory into which you installed the Oracle Database Client files, for example:
   - For C shell (.csh):

     ```
     setenv ORACLE_HOME
     /../example.com/vol/dbclient/oracle/SUN64/11gR2/11.2.0.3
     ```
   - For Bourne shell or Korn shell (.sh:)

     ```
     ORACLE_HOME=/../example.com/vol/dbclient/oracle/SUN64/11gR2/11.2.0.3
     export ORACLE_HOME
     ```

   NOTE: If you are using Siebel Business Applications with an Oracle Database, and if you have a previous Oracle Database Client installation, change the value of ORACLE_HOME to specify the location of the Oracle Database Client you have just installed.
6. Add the directory path of the Oracle Database Client libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) script file. For information on this task, see "Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client" on page 119.

7 Unzip the operating system-specific patch for the Oracle Database Client that you downloaded in Step 3 on page 118, then apply the patch using the Oracle OPatch utility.

8 Change the value of the Security Adapter Dll Name parameter to libsscforacleldap.so or libsscforacleldap.sl, depending on the UNIX operating system you are using.

For information on the Security Adapter Dll Name parameter, see "Parameters for LDAP or ADSI Authentication" on page 364.

9 Stop and restart the Siebel Server.

Configuring the siebenv.csh and siebenv.sh Scripts for the LDAP Client

After you have installed the Oracle Database Client on your UNIX operating system, you must add the directory path of the Oracle Database Client libraries to the library path environment variable in either the siebenv.csh (C shell) or siebenv.sh (Bourne or Korn shell) shell scripts. When you source these scripts, they set the environment variables for your Siebel implementation.

The siebenv.csh and siebenv.sh scripts are created in the $SIEBEL_ROOT directory during the Siebel Server installation and configuration process. Edit the siebenv.csh or siebenv.sh script, as described in the following topics, where `$ORACLE_HOME/lib` is the installation path of your Oracle Database Client libraries, `$ORACLE_HOME/lib`.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 116.

Linux and Oracle Solaris Operating Systems

On Linux and Oracle Solaris operating systems, the name of the library path environment variable is LD_LIBRARY_PATH. Depending on whether you source the siebenv.csh or the siebenv.sh script, set the LD_LIBRARY_PATH variable as follows:

- siebenv.csh

```
if ($?LD_LIBRARY_PATH) then
setenv LD_LIBRARY_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/lib:${MWHOME}/
lib:${SQLANY}/lib:/usr/lib:${LD_LIBRARY_PATH}
else
setenv LD_LIBRARY_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/lib:${MWHOME}/
lib:${SQLANY}/lib:/usr/lib
endif
```

- siebenv.sh

```
if [ a${LD_LIBRARY_PATH} = ${LD_LIBRARY_PATH}a ]
then
LD_LIBRARY_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/
$ORACLE_HOME/lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
else
LD_LIBRARY_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/
```

```
$ORACLE_HOME/lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${LD_LIBRARY_PATH}
fi
export LD_LIBRARY_PATH
```

AIX Operating System

On the AIX operating system, the name of the library path environment variable is LIBPATH. Depending on whether you source the siebenv.csh or the siebenv.sh script, set the LIBPATH variable as follows:

- siebenv.csh

```
if ($?LIBPATH) then
setenv LIBPATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/lib:${MWHOME}/
lib:${SQLANY}/lib:/usr/lib:${LIBPATH}
else
setenv LIBPATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/lib:${MWHOME}/
lib:${SQLANY}/lib:/usr/lib
endif
```

- siebenv.sh

```
if [ a${LIBPATH} = ${LIBPATH}a ]
then
LIBPATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
else
LIBPATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${LIBPATH}
fi
export LIBPATH
```

HP-UX Operating System

On the HP-UX operating system, the name of the library path environment variable is SHLIB_PATH. Depending on whether you source the siebenv.csh or the siebenv.sh script, set the SHLIB_PATH variable as follows:

- siebenv.csh

```
if ($?SHLIB_PATH) then
setenv SHLIB_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/lib:${MWHOME}/
lib:${SQLANY}/lib:/usr/lib:${SHLIB_PATH}
else
setenv SHLIB_PATH
${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/lib:${MWHOME}/
lib:${SQLANY}/lib:/usr/lib
endif
```

- siebenv.sh

```
if [ a${SHLIB_PATH} = ${SHLIB_PATH}a ]
then
SHLIB_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib
else
SHLIB_PATH=${SIEBEL_ROOT}/lib:${SIEBEL_ROOT}/lib/odbc/merant:/$ORACLE_HOME/
lib:${MWHOME}/lib:${SQLANY}/lib:/usr/lib:${SHLIB_PATH}
fi
export SHLIB_PATH
```

Creating a Wallet for Certificate Files When Using LDAP Authentication with SSL

If you are using LDAP authentication with SSL, then you must use Oracle Wallet Manager to create a wallet to store the certificates required for SSL communications. This topic describes how to create the wallet, and how to enable SSL for the Siebel LDAP security adapter. For detailed information on using Oracle Wallet Manager, see *Oracle® Database Advanced Security Administrator's Guide*.

By enabling SSL for the Siebel LDAP security adapter, an encrypted connection is established between the Siebel application and the LDAP server. For information on enabling SSL for an LDAP server, refer to your third-party LDAP server administration documentation. This topic assumes that the LDAP server is already SSL-enabled, that is, it accepts SSL connections.

NOTE: The SSL encryption standard is not secure. It is recommended that you implement additional methods of securing connections between the LDAP security adapter and directory servers.

This task is a step in "Process of Installing and Configuring LDAP Client Software" on page 116.

Generating an Oracle Wallet

To enable SSL for the Siebel LDAP security adapter, an Oracle wallet must be created on the Siebel Server computer which runs the Application Object Managers or other components that must support LDAP authentication through the LDAP security adapter. The Oracle wallet must contain CA server certificates that have been issued by Certificate Authorities to LDAP servers.

Use the following procedure to create an Oracle wallet.

To create an Oracle wallet

1. Determine which Certificate Authorities issued the server certificate for your LDAP server and obtain this CA certificate.
2. Copy the CA certificate to the computer where you have installed Oracle Wallet Manager.
3. On the Siebel Server computer where you will run the Application Object Manager components that support LDAP authentication, create an Oracle wallet using Oracle Wallet Manager.

   To create the wallet, follow the detailed instructions in *Oracle® Database Advanced Security Administrator's Guide.* Specify the following values:

a. In the New Wallet dialog box, enter a password for the wallet in the Wallet Password field, then reenter the password in the Confirm Password field.

b. From the Wallet Type list, select Standard, then click OK.

   A new empty wallet is created.

c. When prompted to specify whether or not you want to add a certificate request, select No.

   You return to the Oracle Wallet Manager main window.

d. Save the wallet by selecting Wallet, then Save In System Default to save the wallet file to the default directory location:

   - For UNIX the default directory location is `$ORACLE_HOME/bin/owm/wallets/username`.
   - For Windows the default directory location is `ORACLE_HOME\bin\owm\wallets\username`.

   You must specify this directory when configuring SSL for clients and servers. You can save the wallet to a different directory if required.

4. Import the certificate referred to in Step 2 into the wallet you have created.

   You can import as many CA certificates as required. For information on importing certificates, see *Oracle® Database Advanced Security Administrator's Guide.*

   NOTE: For LDAP servers that have their server certificate issued from a new CA, just add the CA certificate to the existing wallet, instead of creating a new wallet for every LDAP server.

Enabling SSL for the Siebel LDAP Security Adapter

Use the procedure below to configure SSL for the Siebel LDAP security adapter. For more information about LDAP security adapter configuration, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123.

To enable SSL for the Siebel LDAP security adapter

1. Copy the wallet you created in "Generating an Oracle Wallet" on page 121 to the Siebel Server computer where you will run the Application Object Manager components that support LDAP authentication.
2. (Windows Only) If you are using Windows, do one of the following:
   - Copy the contents of the wallet directory `ORACLE_HOME\bin\owm\wallets\username` into a location that the Siebel Server service owner can access, for example `c:\wallet`.
   - Alternatively, change the Siebel Server service owner account log on values so that they are the same as the account used to create the wallet described in "Generating an Oracle Wallet" on page 121. To change the Siebel Server service account owner log on values:
     - From the Windows Start menu, choose Settings, Control Panel, Administrative Tools, and then the Services item.
     - Right-click on the Siebel Server System Service, then select Properties.
     - In the Properties dialog box for this service, click the Log On tab.

- Select the This Account option, then enter the name and password of the account used to create the wallet.

3 Modify the LDAP security adapter configuration parameters using values similar to those shown in the following table.

Parameter	Value
port	*port_number* The SSL port is configurable for the LDAP server. Verify the actual port number the LDAP server is using for SSL and specify that value. The default value is 636.
ssldatabase	*wallet_directory_path* Specify the absolute path to the wallet directory using a format similar to the following: `file:`*`sslwallet`* where: ■ `file` is the wallet resource locator type ■ *`sslwallet`* is the directory containing the wallet, for example, `$ORACLE_HOME/bin/owm/wallets/`*`username`* **NOTE:** (Windows only) If you copied the contents of the wallet directory into another location, for example `c:\wallet` (see Step 2 on page 122), then specify the wallet directory path as follows: file:*`c:\wallet`*.
WalletPassword	*wallet_password* Specify the password you assigned to the wallet in Step a on page 122.

For information on configuring parameters for the LDAP security adapter, see "Parameters for LDAP or ADSI Authentication" on page 364.

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

Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard

This topic describes how to configure the Siebel LDAP or ADSI security adapters using the Siebel Configuration Wizard after you have installed Siebel Business Applications. Alternatively, you can configure the security adapter settings by setting Gateway Name Server parameters directly using Server Manager. For information on installing and configuring Siebel Business Applications, see *Siebel Installation Guide* for the operating system you are using.

You use the Siebel Configuration Wizard to configure the Siebel Gateway Name Server parameters that set security adapter values. You can also use the Siebel Configuration Wizard to configure security adapter settings for Gateway Name Server access authentication; these parameters are stored in the Gateway Name Server configuration file (gateway.cfg). When configuring a Siebel Developer Web Client, you configure authentication parameters stored in the Siebel application configuration file. When you configure Siebel Gateway Name Server parameters, the Siebel Gateway Name Server must be running.

NOTE: The Siebel Enterprise and Gateway Name Server are configured to use database authentication by default. If you specify LDAP or ADSI authentication using the Siebel Configuration Wizard, then the parameter values you specify for the security adapter are only implemented when you manually change the SecAdptName and SecAdptMode parameters using Server Manager to enable LDAP or ADSI authentication.

When you specify LDAP or ADSI as the security adapter type using the Configuration Wizard, the setting you make provides the value for the Security Adapter Mode (SecAdptMode) parameter. The Security Adapter Mode and Security Adapter Name parameters can be set for the Siebel Gateway Name Server, the Siebel Enterprise Server, for a particular Siebel Server, for an individual Application Object Manager component, or for the Synchronization Manager component (for Siebel Remote).

CAUTION: If you want to configure a server component or a Siebel Server to use different LDAP or ADSI authentication settings than those already configured at a higher level (that is, configured for the Siebel Enterprise or Siebel Server), then you must create a new LDAP or ADSI security adapter. Otherwise, the settings you make reconfigure the existing security adapter wherever it is used.

When you specify LDAP or ADSI as the security adapter mode, additional configuration parameters are defined for the particular LDAP or ADSI security adapter. For example, the Security Adapter DLL Name (SecAdptDllName) parameter is automatically set when you specify LDAP or ADSI as the security adapter mode.

The Siebel Configuration Wizard sets authentication-related configuration parameters for Siebel Business Applications and Gateway Name Server authentication, but does not make changes to the LDAP directory or to Active Directory. Make sure the configuration information you enter is compatible with your directory server.

The following procedure describes how to run the Siebel Configuration Wizard to configure the LDAP or ADSI security adapters provided with Siebel Business Applications.

To configure your LDAP or ADSI security adapter

1. Start the Siebel Enterprise Configuration Wizard.
2. Choose the Create New Configuration option, then Configure a New Enterprise in a Gateway Name Server.

   For details about launching the wizard, see *Siebel Installation Guide* for the operating system you are using.
3. Navigate to the Enterprise Security Authentication Profile screen.
4. Choose the authentication type that corresponds to the security adapter you want to implement, and click Next.

- Select Lightweight Directory Access Protocol (LDAP) Authentication to implement the LDAP security adapter.
- Select Active Directory (ADSI) Authentication (Windows only) to implement the ADSI security adapter.

Enter values for the various parameters that the Configuration Wizard presents to you as described in the following steps. The screens that the Configuration Wizard presents depends on the authentication type you select.

5 **Security Adapter Name (named subsystem).** Specify the name of the security adapter. The setting you make provides a value for the Security Adapter Name parameter. You can accept the default name, or specify a nondefault name. If an enterprise profile (named subsystem) does not already exist with the name you specify, then the Siebel Configuration Wizard creates a new enterprise profile using that name. The default names are:

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

6 **Security Authentication Library CRC Checksum.** Specify whether you want to use checksum validation for the security adapter DLL file. Corresponds to the CRC parameter.

If you do not want to use checksum validation, enter 0. Otherwise, enter the value that you generate. For information, see "Configuring Checksum Validation" on page 149.

7 **Directory Server Domain Name.** Corresponds to the ServerName parameter.

Specifies the name of the computer on which the LDAP or Active Directory server runs.

- **LDAP.** You must specify the fully qualified domain name of the LDAP server, not just the domain name. For example, specify ldapserver.example.com, not example.com.
- **ADSI.** For Active Directory, if TLS is configured between the Siebel Server computer and the Active Directory server computer, then you must specify the fully qualified domain name of the directory server. If the Siebel Server and directory server are in the same domain, then you can specify the complete computer name of the Active Directory server.

  Do not specify the IP address of the Active Directory server for the Server Name parameter.

8 **LDAP Port Configuration** (*LDAP only*)**.** The port number used by the LDAP directory server. Corresponds to the Port parameter. Select the appropriate option according to whether LDAP is configured to use a standard port (389) or a secure transmission port (636). Proceed to Step 10.

If you configured LDAP to use a transmission port other than one of those listed, then check the Use a different transmission port (non-default) option and proceed to Step 9.

The Active Directory server port is set as part of the directory installation, not as a configuration parameter.

9 **Network TCP/IP Port Number.** Enter the TCP/IP port number used by your LDAP implementation to authenticate the Siebel application.

10 Enter configuration information pertaining to attribute mapping:

- **Siebel Username Attribute.** The Siebel user ID attribute used by the directory. An example entry for an LDAP directory is uid. An example entry for Active Directory is sAMAccountName (maximum length 20 characters). If your directory uses a different attribute for the Siebel user ID, then enter that attribute instead. Corresponds to the UsernameAttributeType parameter.
- **Siebel Password Attribute.** The password for the Siebel user ID attribute used by the directory (*LDAP only*). Corresponds to the PasswordAttributeType parameter.
- **Credentials Attribute.** The database credentials attribute type used by the directory. For LDAP and Active Directory, an example entry is dbaccount.

11 Enter values for the following:

- **LDAP Roles Attribute.** The attribute type for roles stored in the directory. This setting is required only if you use roles in your directory. Corresponds to the RolesAttributeType parameter. For more information, see "Configuring Roles Defined in the Directory" on page 157.
- **Shared Database Account Distinguished Name (DN).** If you are implementing a shared database account for users, then specify the full DN of the directory object containing the shared database account values. Corresponds to the SharedCredentialsDN parameter. Configuring the shared database account also uses the database account attribute you defined in Credentials Attribute.

  You can, as an alternative, specify the database credentials as profile parameters. For more information on this option, see Step 12.

12 **Store shared database user credentials as parameters.** Choose the appropriate action:

- Select the check box Store Shared Database User Credentials as Parameters if you want to store the database credentials for the shared database account as parameter values for the LDAP Security Adapter profile or the ADSI Security Adapter profile instead of as directory attributes. Proceed to Step 13.
- Leave the check box clear if you want to store each user's database account credentials in an attribute of that user's record in the directory. Proceed to Step 14.

13 Configure the shared database account:

- **Shared Database Account.** Specify the shared database account user name.
- **Shared Database Account Password.** Specify the shared database account password.

For more information on the shared database account, see "Configuring the Shared Database Account" on page 151.

14 Configure the application user:

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

  In addition to defining the application user here, you must also create the application user in the LDAP directory or in Active Directory. For more information, see "Configuring the Application User" on page 147.

  NOTE: If you are configuring an ADSI security adapter, then the application user must either be a domain user or have access to the directory server. If the application user cannot access the directory server, then the authentication process fails.

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

15 **Configure Web Single Sign-On (Web SSO).** To configure Web SSO, select the check box. Corresponds to the SingleSignOn parameter.

- If you selected the check box, then go to Step 16.
- If you did not select the check box, then go to Step 17.

16 Enter configuration information pertaining to Web SSO:

- **Credentials Attribute.** Enter the database credentials attribute type used by the directory.
- **User Specification.** The Web server variable which stores the user's identity key. Corresponds to the UserSpec parameter.
- **Shared Secret.** Specify the trust token to use for Web SSO. Corresponds to the TrustToken parameter. The value also corresponds to the TrustToken parameter in the eapps.cfg file on the SWSE.

17 **SSL Database Certificate File.** To enable SSL with the LDAP security adapter, provide the directory path to the Oracle wallet. For more information, see "Enabling SSL for the Siebel LDAP Security Adapter" on page 122.

18 Enter values for pass word hashing:

- **Hash User Passwords.** Specify whether or not you want to use password hashing for user passwords. Corresponds to the HashUserPwd parameter.
- **Hash Database Passwords.** Specify whether or not you want to use password hashing for database credentials passwords. Corresponds to the HashDBPwd parameter.

For more information, see "About Password Hashing" on page 158.

19 **Salt User Passwords.** Specify whether you want to add a salt value to user passwords before they are hashed. Corresponds to the SaltUserPwd parameter. This option is available only if you have chosen to hash user passwords.

NOTE: You cannot add salt values to user passwords if you enable Web Single Sign-On.

For more information on the salt value feature, see "About Password Hashing" on page 158.

20 **Salt Attribute.** If you have chosen to add salt values to user passwords, then specify the attribute that is to store the salt value. The default attribute is title. Corresponds to the SaltAttributeType parameter.

21 **Security Adapter Mapped User Name.** Specify whether you want to implement the adapter-defined user name. Corresponds to the UseAdapterUserName parameter. For more information, see "Configuring Adapter-Defined User Name" on page 154.

- If you check this option, then you must specify the Siebel User ID attribute. Go to Step 22 on page 127.
- If you do not check this option, then go to Step 23 on page 128.

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

23 **Base Distinguished Name (DN).** Specify the base distinguished name (DN) in the directory under which Siebel users are stored. Corresponds to the BaseDN parameter.

24 **Propagate Change.** Specify whether you want to configure the ability to propagate changes to the LDAP directory or to Active Directory from a Siebel Developer Web Client or a Siebel Mobile Web Client. Corresponds to the PropagateChange parameter.

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

25 **Propagate Authentication Settings to the Gateway Name Server.** Select the check box to apply the Enterprise authentication settings you have just configured to the Gateway Name Server. The values you have specified are written to the gateway.cfg file.

Selecting this option also sets the ConnectString parameter in the gateway.cfg file to the ODBC data source name used to connect to the Siebel database.

NOTE: If this is the first time the Enterprise is being configured on the Gateway Name Server, then you must select this option for the configuration to complete. Subsequently, select this option only when changing existing settings.

For further information on the gateway.cfg file, see "About Authentication for Gateway Name Server Access" on page 165 and "Parameters in the Gateway.cfg File" on page 372.

26 Perform any of the additional tasks listed on the Additional Tasks for Configuring the Enterprise screen as required.

27 Review the settings you have specified on the Summary screen, then execute the configuration.

28 When the Siebel Enterprise Configuration Wizard has executed successfully, enable LDAP or ADSI authentication and implement the security adapter settings you have just configured by changing the SecAdptName and SecAdptMode parameters to specify either LDAP or ADSI.

For the Enterprise, change the SecAdptName and SecAdptMode parameters using Siebel Server Manager (see "Configuring Security Adapter Gateway Name Server Parameters" on page 137). For the Gateway Name Server, edit the SecAdptName and SecAdptMode parameters in the gateway.cfg file (see "Parameters in the Gateway.cfg File" on page 372).

Process of Implementing LDAP or ADSI Security Adapter Authentication

This topic describes the tasks involved in implementing LDAP or ADSI security adapter authentication. Implement your authentication architecture in a development environment before deploying it in a production environment.

The process outlined in this topic provides instructions for implementing and testing security adapter authentication for a single Siebel application using either an LDAP or ADSI security adapter with one of the supported directory servers. The security adapter authenticates a user's credentials against the directory and retrieves login credentials from the directory. A user is authenticated by the user's Siebel user ID and a password.

You can repeat the appropriate tasks listed in this topic to provide security adapter authentication for additional Siebel Business Applications. You can also implement components and options that are not included in this process. For additional information about security adapter authentication options, see "Security Adapter Deployment Options" on page 146. For information about special considerations in implementing user authentication, see "Troubleshooting User Authentication Issues" on page 346.

NOTE: If you use a security adapter that is not provided by Siebel Business Applications, then it must support the Siebel Security Adapter Software Developers Kit, which is described in "Security Adapter SDK" on page 23. You must adapt the applicable parts of the following task instructions to your security adapter.

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

1. Verify that all requirements are met. For information on the requirements, see "Requirements for Implementing an LDAP or ADSI Authentication Environment" on page 130.
2. Review "About Creating a Database Login for Externally Authenticated Users" on page 131.
3. Set up the attributes for users in the directory. See "Setting Up the LDAP Directory or Active Directory" on page 131.
4. Create users in the directory: a regular user, the anonymous user, and the application user. See "Creating Users in the LDAP Directory or Active Directory" on page 132.
5. Add user records in the Siebel database corresponding to the users in the directory. See "Adding User Records in the Siebel Database" on page 134.
6. Edit security adapter parameters in the eapps.cfg file. See "Setting Security Adapter Parameters in the SWSE Configuration File (eapps.cfg)" on page 135.
7. Select the security adapter you want to use (LDAP, ADSI, Custom), and configure parameters for the selected security adapter, using one of the following methods:

   - Using the Siebel Configuration Wizard

     Configure values for the security adapter parameters by running the Siebel Configuration Wizard. Then select the security adapter you want to use (LDAP, ADSI, Custom) by specifying the appropriate values for the SecAdptName and SecAdptMode Siebel Gateway Name Server parameters using either Siebel Server Manager or by running the Siebel Configuration Wizard again. For information on running the Siebel Configuration Wizard, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123.

   - Editing Siebel Gateway Name Server parameters directly

     You can select the security adapter you want to use, and configure Gateway Name Server parameters for the security adapter, by editing Siebel Gateway Name Server parameters directly using Siebel Server Manager. For further information, see "Configuring Security Adapter Gateway Name Server Parameters" on page 137.

- (Developer Web Clients only) Editing the application configuration file

  For Developer Web Clients only, you configure parameters for the security adapter in the application configuration file. For additional information, see "Configuring Security Adapter Parameters for Developer Web Clients" on page 142.

8 (Developer Web Clients only) "Setting a System Preference for Developer Web Clients" on page 143.

9 "Restarting Servers" on page 143.

10 "Testing the LDAP or ADSI Authentication System" on page 143.

Requirements for Implementing an LDAP or ADSI Authentication Environment

This topic describes the requirements for implementing an LDAP or ADSI authentication environment. The Siebel default authentication method is database authentication; if you want to implement LDAP or ADSI authentication instead, verify that the requirements outlined in this topic are in place.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

You must complete the following tasks before you can configure an LDAP or ADSI security adapter for your environment:

- Install the Web server.
- Install the LDAP directory or Active Directory.
- Install the Siebel Enterprise Server components (Gateway Name Server, Siebel Server, and Database Configuration Utilities).

  For information on this task, see *Siebel Installation Guide* for the operating system you are using.
- Review "Requirements for the LDAP Directory or Active Directory" on page 111.

  To implement LDAP or ADSI authentication, you must be experienced with administering the directory. That is, you must be able to perform tasks such as creating and modifying user storage subdirectories, creating attributes, creating users, and providing privileges to users.
- (LDAP only) Install the LDAP or ADSI client software. For information on this task, see "Process of Installing and Configuring LDAP Client Software" on page 116.
- Have available a URL or hyperlink with which users can access the login form for the Siebel application you are configuring.

About Creating a Database Login for Externally Authenticated Users

A database login must exist for all users who log in to Siebel Business Applications through an external authentication system. If you are implementing LDAP or ADSI security adapter authentication, then verify that this login name is present; if it does not exist, then create it. This database login must not be assigned to any individual user.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

A database login is created for externally authenticated users during the Siebel installation process. If you are using an Oracle or Microsoft SQL Server database, then the account is created when you run the grantusr.sql script. If you are using a DB2 database, then the database administrator manually creates this account. For additional information, see *Siebel Installation Guide* for the operating system you are using.

The default user ID of the database login account for externally authenticated users is LDAPUSER. A password is assigned to this database account when the account is created. A Siebel application user account corresponding to the LDAPUSER database account is not provided in the seed data and is not required.

Setting Up the LDAP Directory or Active Directory

When you implement LDAP or ADSI authentication, users are authenticated through a directory. This topic describes how to set up the directory to do the following:

- Authenticate users through the directory.
- Allow self-registration.
- Use the Siebel user ID as the user name.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

The following procedure describes how to set up the LDAP directory or Active Directory. For more information about setting up the directory, review "About Setting Up the LDAP Directory or Active Directory" on page 112.

To set up the LDAP directory or Active Directory

1. Determine the Base Distinguished Name, that is, the location in the directory in which to store users. For details, see the BaseDN parameter description in "Siebel Gateway Name Server Parameters" on page 361.

   You cannot distribute the users of a single Siebel application in more than one base DN. However, you can store multiple Siebel Business Applications' users in one base DN or in substructures such as organization units (OU), which are used for LDAP. For example, store users in the People base DN under the domain level for LDAP directories, or in the Users base DN under the domain level for ADSI directories.

2 Define the attributes to use for the following user data. Create new attributes if you do not want to use existing attributes. Suggested attributes to use are as follows:

- **Siebel user ID.** Suggested attribute: uid for LDAP, or sAMAccountName for ADSI.
- **Database account.** Suggested attribute: dbaccount.
- **Password.** Suggested attribute (for LDAP only): userPassword. However, if you use the LDAP security adapter to authenticate against Microsoft Active Directory, then use either the unicodePWD or userPassword attribute, depending on the code page used by the directory server. ADSI directories do not use an attribute to store a user's password.

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

Creating Users in the LDAP Directory or Active Directory

This topic describes the users you must create in the LDAP directory or Active Directory to implement LDAP or ADSI security adapter authentication.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

When you use LDAP or ADSI authentication, you must create the following users in the directory:

- Application user

  Make sure the application user has write privileges to the directory because the security adapter uses application user credentials when using the self-registration component. The application user must also have search privileges for all user records. For additional information, see "Configuring the Application User" on page 147.

- Anonymous user

  You must define an anonymous user even if your application does not allow access by unregistered users. For more information, see "Configuring the Anonymous User" on page 155.

- Records for each user of the Siebel application

  Initially, create a test user to verify the authentication system.

- (Optional) A shared credentials user account

  You can also store credentials for the shared database account as profile parameters for the LDAP or ADSI security adapter profiles. For more information, see "Configuring the Shared Database Account" on page 151.

Create users in the directory using values similar to those shown in Table 11. Store information for users in the directory attributes indicated in "Setting Up the LDAP Directory or Active Directory" on page 131. Optionally, complete other attribute entries for each user.

Table 11. Records in the LDAP Directory or Active Directory

Type of User	Siebel User ID	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 for a Siebel customer or partner application. For example, if you implement Siebel eService, enter GUESTCST. ■ You can create a new user record or adapt a seed anonymous user record for a Siebel employee application.	GUESTPW or a password of your choice.	A database account is not required for the anonymous user if a shared database credentials account is implemented; the database credentials for the anonymous user are read from the shared database account user record or the relevant profile parameter of the LDAP or ADSI security adapter.
Application user	APPUSER or a name of your choice.	APPUSERPW or a password of your choice.	A database account is not used for the application user.
A test user	TESTUSER or a name of your choice.	TESTPW or a password of your choice.	Database account is not required for any user record, except the anonymous user or the shared credentials user account.
Shared database credentials account user	SharedDBUser or a name of your choice. The user name and password you specify for the shared database account must be a valid Siebel user name and password.	SharedDBPW or a password of your choice.	username=SHAREDDBUSER password=*P* For information about formatting requirements for the database account attribute entry, see "About Setting Up the LDAP Directory or Active Directory" on page 112.

The example directory entries in Table 11 implement a shared credential. The database account for all users is stored in one object in the directory. In this example, the shared database account is stored in the SharedDBUser record. The database account must match the database account you reserve for externally authenticated users which is described in "About Creating a Database Login for Externally Authenticated Users" on page 131. The *P* symbol represents the password for that database account. For additional information, see "Configuring the Shared Database Account" on page 151.

Adding User Records in the Siebel Database

This topic describes how to create a record in the Siebel database that corresponds to the test user record you created in "Creating Users in the LDAP Directory or Active Directory" on page 132.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in Appendix B, "Seed Data." This record must also match the anonymous user you created in "Creating Users in the LDAP Directory or Active Directory" on page 132.

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, then see the instructions for adding such users in "Internal Administration of Users" on page 241.

The following procedure describes how to add user records to the Siebel database.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
2. Navigate to the Administration - User screen, then the Users view.
3. In the Users list, create a new record.
4. Complete the following fields for the test user using values similar to those shown in the following table, then save the record. You can complete other fields, but they are not required.

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

Field	Guideline
User ID Example: *TESTUSER*	Required. This entry must match the uid (LDAP) or sAMAccountName (ADSI) attribute value for the test user in the directory. If you used another attribute, then it must match that value.
Responsibility	Required. Enter the seed data responsibility provided for registered users of the Siebel application that you implement. For example, enter Web Registered User for eService. If an appropriate seed responsibility does not exist, such as for a Siebel employee application, then 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. If the record is not present, then create it using the field values in "Seed Users" on page 384. You can complete other fields, but they are not required.

Setting Security Adapter Parameters in the SWSE Configuration File (eapps.cfg)

This topic describes the parameter values you must enter in the SWSE configuration file (eapps.cfg) when you implement LDAP or ADSI security adapter authentication. For information about editing eapps.cfg parameters and about the purposes of the parameters, see "About Parameters in the eapps.cfg File" on page 353.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

Enter values for eapps.cfg file parameters using values similar to those shown in Table 12 on page 136. Specify values for AnonUserName and AnonPassword in the defaults section of the eapps.cfg file if you are configuring LDAP or ADSI authentication for all your Siebel Business Applications. If you are implementing LDAP or ADSI authentication for a single application, as in this example, then specify these parameters in the application-specific section of the eapps.cfg file.

Table 12. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
[defaults]	SingleSignOn TrustToken UserSpec UserSpecSource	If these parameters are present, then comment out each with a semicolon at the beginning of the line. Do the same if these parameters are present in any other sections.
The section that is specific to your application, such as one of the following: [/eservice_enu] [/callcenter_enu] where *_enu* is the language code for U.S. English.	AnonUserName	Enter the user ID of the seed data user record provided for the application that you implement, or of the user record you create for the anonymous user. This entry also matches the uid (LDAP) or sAMAccountName (ADSI) entry for the anonymous user record in the directory. For example, enter GUESTCST for Siebel eService.
	AnonPassword	Enter the password you created in the directory for the anonymous user. Whether or not you have to encrypt the password depends on the value specified for the EncryptedPassword parameter. For information on this parameter, see "Encrypted Passwords in the eapps.cfg File" on page 46. Typically, password encryption applies to the eapps.cfg file. In this case, you must specify the encrypted password, unless you provide the password through the Siebel Configuration Wizard.
	ProtectedVirtualDirectory	If this parameter is present, then comment it out with a semicolon at the beginning of the line.

Configuring Security Adapter Gateway Name Server Parameters

This topic describes the security-related configuration parameters you use for configuring an LDAP or ADSI security adapter that are defined in the Siebel Gateway Name Server. You can modify Gateway Name Server configuration parameters using Siebel Server Manager, or you can do so using the Siebel Configuration Wizard.

For information on editing Gateway Name Server parameters using the Siebel Configuration Wizard, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123. For information on using Siebel Server Manager to edit Gateway Name Server parameters, see *Siebel System Administration Guide*.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

You can set Gateway Name Server security adapter parameters for the following:

- "Parameters for Enterprise, Siebel Servers, or Components" on page 137
- "Parameters for Application Object Manager Components" on page 138
- "Parameters for Security Adapter (Profile/Named Subsystem)" on page 139

Set security adapter parameters as described in each of these topics. For more information about these parameters, see "Siebel Gateway Name Server Parameters" on page 361.

Parameters for Enterprise, Siebel Servers, or Components

This topic lists security adapter parameters you can set at the Gateway Name Server level, at the Enterprise level, at the Siebel Server level, or at the component level. Applicable components for which you can set these parameters include all Application Object Manager components and the Synchronization Manager component (for Siebel Remote).

To implement LDAP or ADSI authentication for a single Siebel application, set the parameters for the applicable Application Object Manager component, such as for Siebel Call Center or Siebel eService, using values similar to those in Table 13.

Table 13. Siebel Gateway Name Server Parameters (for Enterprise, Server, or Component)

Subsystem	Parameter	Guideline
Security Manager	Security Adapter Mode (SecAdptMode)	The security adapter mode to operate in: ■ For LDAP, specify LDAP. ■ For ADSI, specify ADSI.
	Security Adapter Name (SecAdptName)	The name of the security adapter. ■ For LDAP, specify LDAPSecAdpt or another name of your choice. ■ For ADSI, specify ADSISecAdpt or another name of your choice. The name represents the alias for the enterprise profile (named subsystem) for the specified security adapter.

Parameters for Application Object Manager Components

This topic lists parameters you set for the Application Object Manager component when implementing LDAP or ADSI authentication for a single Siebel application.

To implement LDAP or ADSI authentication for a single Siebel application, set the parameters for the applicable Application Object Manager component, such as for Siebel Call Center or Siebel eService, using values similar to those shown in Table 14.

Table 14. Siebel Gateway Name Server Parameters (for Application Object Manager)

Subsystem	Parameter	Guideline
InfraUIFramework	AllowAnonUsers	Enter TRUE for LDAP or ADSI. Set this parameter to FALSE if your Siebel application does not use functionality that requires anonymous browsing, such as anonymous catalog browsing or user self-registration.
Object Manager	OM - Proxy Employee (ProxyName)	Enter PROXYE.
	OM - Username BC Field (UsernameBCField)	You can leave this parameter empty.

Parameters for Security Adapter (Profile / Named Subsystem)

This topic lists parameters you set for the enterprise profile (named subsystem) for the specific security adapter you are configuring.

To implement LDAP or ADSI authentication for a single Siebel application, configure parameters for one of the following (defined as enterprise profile or named subsystem):

- **LDAP Security Adapter.** Typically, the alias for this adapter is LDAPSecAdpt.
- **ADSI Security Adapter.** Typically, the alias for this adapter is ADSISecAdpt.

Set the security adapter parameters using values similar to those shown in Table 15 on page 139.

Table 15. Siebel Gateway Name Server Parameters (for Enterprise Profile/Named Subsystem)

Parameter	Guideline
Security Adapter Dll Name (SecAdptDllName)	■ For LDAP, enter sscforacleldap.dll. ■ For ADSI, enter sscfadsi. Do not include the file extension (for example, do not specify sscforacleldap.dll for LDAP). The specified value is converted internally to the actual filename for your operating system.
Server Name (ServerName)	Enter the name of the computer on which the LDAP directory or Active Directory server runs. Do not specify the IP address of the Active Directory server for the Server Name parameter.
Port (Port)	■ For LDAP, an example entry is 389. Typically, use port 389 for standard transmission or port 636 for secure transmission. ■ For Active Directory, you set the port at the Active Directory level, not as a configuration parameter.

Table 15. Siebel Gateway Name Server Parameters (for Enterprise Profile/Named Subsystem)

Parameter	Guideline
Base DN (BaseDN)	The Base Distinguished Name is the root of the tree under which users are stored. Users can be added directly or indirectly below this directory. You cannot distribute the users of a single Siebel application in more than one base DN. However, you can distribute them in multiple subdirectories, such as organization units (OU), which are used for LDAP. LDAP example entry: `ou=people, o=`*`domainname`* In the example, “o” denotes “organization” and is the domain name system (DNS) name for this server, such as *`computer.example.com`*. “ou” denotes “organization unit” and is the name of a subdirectory in which users are stored. ADSI example entry: `ou=people, DC=`*`domainname`*`, DC=com` Domain Controller (DC) entries are the nested domains that locate this server. Therefore, adjust the number of DC entries to represent your architecture.
Username Attribute Type (UsernameAttributeType)	LDAP example entry is uid ADSI example entry is sAMAccountName If you use a different attribute in the directory for the Siebel user ID, then enter that attribute name.
Password Attribute Type (PasswordAttributeType)	The LDAP entry must be userPassword. However, if you use the LDAP security adapter to authenticate against Microsoft Active Directory, then set the value of this parameter to unicodePWD. Active Directory does not store the password in an attribute so this parameter is not used by the ADSI security adapter. You must, however, specify a value for the Password Attribute Type parameter even if you are using the ADSI security adapter. Specify a value of unicodePWD.
Credentials Attribute Type (CredentialsAttributeType)	If you are using an LDAP security adapter, an example entry is mail. If you are using an ADSI security adapter, an example entry is physicalDeliveryOfficeName. If you used a different attribute in the directory for the database account, then enter that attribute name.

Table 15. Siebel Gateway Name Server Parameters (for Enterprise Profile/Named Subsystem)

Parameter	Guideline

Application User (ApplicationUser)	LDAP example entry:
	`uid=APPUSER, ou=people, o=`*`domainname`*
	ADSI example entry:
	`CN=APPUSER, ou=people, DC=`*`computername`*`,`
	`DC=`*`domainname`*`, DC=com`
	Adjust your entry if your implementation uses a different attribute for the user name, a different user name for the application user, or a different base DN.

Application Password (ApplicationPassword)	For LDAP and ADSI, enter APPUSERPW or the password assigned to the application user.

Shared Credentials DN (SharedCredentialsDN)	■ LDAP example entry:
	`uid=shared database account user User ID,`
	`ou=people, o=`*`domainname`*
	For example:
	`uid=SharedDBUser, ou=people, o=example.com`
	■ ADSI example entry:
	`CN=shared database account user User ID,`
	`ou=people, DC=`*`computername`*`, DC=`*`domainname`*`, DC=com`
	For example:
	`CN=SharedDBUser, ou=people, DC=qa1, DC=example,`
	`DC=com`

Configuring LDAP or ADSI Authentication for Developer Web Clients

This topic describes the tasks you must perform if you want to implement LDAP or ADSI security adapter authentication for Developer Web Clients.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

To configure LDAP or ADSI authentication for Developer Web Clients, perform the following tasks:

- "Configuring Security Adapter Parameters for Developer Web Clients" on page 142
- "Setting a System Preference for Developer Web Clients" on page 143

Configuring Security Adapter Parameters for Developer Web Clients

For Developer Web Clients, security adapter parameters are configured in the configuration file of the application for which you are implementing LDAP or ADSI security adapter authentication rather than in the Gateway Name Server.

Parameters in sections of the application configuration file that directly pertain to security adapters apply, in this context, only to the Siebel Developer Web Client. These parameters are counterparts to the Siebel Gateway Name Server parameters listed in Table 13 on page 138, Table 14 on page 138, and Table 15 on page 139.

To configure a security adapter for the Developer Web Client, provide parameter values, as indicated by the guidelines in Table 16 on page 142, in the configuration file for the Siebel application for which you are implementing LDAP or ADSI security adapter authentication.

You can use a text editor to make changes to an application configuration file, or you can do so using the Siebel Configuration Wizard. For more information about editing an application's configuration file and about the purposes for the parameters, see "Siebel Application Configuration File Parameters" on page 376. For a list of Siebel application configuration files, see *Siebel System Administration Guide*.

Table 16. Siebel Application Configuration File Parameters

Section	Parameter
[InfraUIFramework]	AllowAnonUsers For the AllowAnonUsers parameter, enter TRUE for LDAP or ADSI. **NOTE:** Set this parameter to FALSE if your Siebel application does not use functionality that requires anonymous browsing, such as anonymous catalog browsing or user self-registration.
[InfraSecMgr]	SecAdptMode For the SecAdptMode parameter: ■ For LDAP, specify LDAP. ■ For ADSI, specify ADSI.
	SecAdptName For the SecAdptName parameter: ■ For LDAP, specify LDAPSecAdpt or another name of your choice. ■ For ADSI, specify ADSISecAdpt or another name of your choice.
[LDAPSecAdpt]	For parameters, see "Configuring Security Adapter Gateway Name Server Parameters" on page 137 or Appendix A, "Configuration Parameters Related to Authentication."
[ADSISecAdpt]	For parameters, see "Configuring Security Adapter Gateway Name Server Parameters" on page 137 or Appendix A, "Configuration Parameters Related to Authentication."

Setting a System Preference for Developer Web Clients

If you are configuring LDAP or ADSI authentication for the Siebel Developer Web Client, then you must set the SecThickClientExtAuthent. system preference to True, as described in this topic.

Setting the SecThickClientExtAuthent. parameter to True allows security adapter authentication for users who log in through the Siebel Developer Web Client. System preferences are enterprise-wide settings, however, the SecThickClientExtAuthent. system preference has no effect on security adapter authentication for users who log in through the Siebel Web Client.

Use the following procedure to specify a value for the SecThickClientExtAuthent. parameter.

To set the SecThickClientExtAuthent parameter

1. Log in as an administrator to a Siebel employee application.
2. Navigate to the Administration - Application screen, then the System Preferences view.
3. In the System Preferences list, select the SecThickClientExtAuthent system preference.
4. In the System Preference Value column, enter TRUE.
5. Restart the Siebel Server.

Restarting Servers

This topic describes the Windows services on the Web server computer that you must restart to activate the changes you make during the process of configuring LDAP or ADSI security adapter authentication.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

Stop and restart the following services:

- **IIS Admin service and Worldwide Web Publishing service.** Stop the IIS Admin service, and then restart the Worldwide Web Publishing service. The IIS Admin service also starts, because the Worldwide Web Publishing service is a subservice of the IIS Admin service.
- **Siebel Server system service.** Stop and restart the Siebel Server. For details, see *Siebel System Administration Guide*.
- **Siebel Gateway Name Server system service.** Stop and restart the Siebel Gateway Name Server. For details, see *Siebel System Administration Guide*.

Testing the LDAP or ADSI Authentication System

After performing all the tasks required to implement LDAP or ADSI security adapter authentication, you can verify your implementation using the procedure in this topic.

This task is a step in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128.

The tests outlined in this topic allow you to confirm that the security adapter provided with Siebel Business Applications, your LDAP directory or Active Directory, and the Siebel application you are implementing work together to:

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

To test your LDAP or ADSI authentication implementation, perform the following procedure.

To test your LDAP or ADSI authentication system

1. In a Web browser, enter the URL to your Siebel application, for example:

   ```
   http://www.example.com/eservice_enu
   ```

   If the authentication system has been configured correctly, then a Web page with a login form appears, confirming that the anonymous user can successfully access the login page.

2. Various links provide access to views intended for anonymous browsing. Some other links will require you to log in first.

   NOTE: Employee applications, such as Siebel Call Center, typically do not allow anonymous browsing, while customer applications such as Siebel eService do.

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

   More screen tabs or other application features might appear, indicating that the test user has authenticated successfully. The user record in the database provides views through the expanded responsibility of this registered user.

4. Click the Log Out link.

5. Repeat Step 1 on page 144 to access the login page. If a New User button is present, then click it.

   If a New User button is not present, then your Siebel application, without additional configuration, does not allow users to self-register.

6. In the Personal Information form, complete the required fields, as shown below, and then submit the form. You can complete other fields, but they are not required.

Field	Description
Last Name	Required. Enter any name.
First Name	Required. Enter any name.

Field	Description
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Verify Password	Required when Password is required.
Challenge Question	Required. Enter a phrase for which there is an “answer.” If you later click Forgot Your Password?, then 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 144.

If the authentication system has been configured correctly, then you can log in successfully and can navigate in the screens provided for registered users.

About Migrating from Database to LDAP or ADSI Authentication

When you install Siebel Business Applications, three security adapters are provided for user authentication: a database security adapter, an ADSI security adapter, and an LDAP security adapter. The database security adapter is enabled by default. If you want to implement LDAP or ADSI security adapter authentication for a Siebel application that was previously configured to use database authentication, then review the information in this topic.

Considerations in Migrating to LDAP or ADSI Authentication

There are a number of issues that you have to consider in deciding the most appropriate authentication method for your Siebel implementation, for example, some features, such as user self-registration, are unavailable with database authentication while some components, such as batch and system management components, must use database authentication. For information on the benefits and limitations of different security adapter authentication options, review the following topics:

- "Comparison of Authentication Strategies" on page 99
- "About Siebel Security Adapters" on page 100
- "Features Not Available for Database Authentication" on page 102
- "About LDAP or ADSI Security Adapter Authentication" on page 106

Migrating from Database to LDAP or ADSI Authentication

To migrate a Siebel application from database authentication to LDAP or ADSI authentication involves the same steps as those outlined in "Process of Implementing LDAP or ADSI Security Adapter Authentication" on page 128. In addition, you must perform the following steps:

1. Migrate your users from the Siebel database to the external directory server; create an entry in the external directory for each user to be authenticated.
2. (Optional) Archive any Siebel user database accounts that are not required for LDAP or ADSI authentication from the Siebel database. Do not archive the following database accounts:
   - The default Siebel administrator account, SADMIN.
   - The default database account, for example, LDAPUSER, that is used by Siebel LDAP and ADSI security adapters to connect to the Siebel database.

Security Adapter Deployment Options

This topic describes security adapter options that can be implemented in a security adapter authentication environment or in a Web SSO environment. Unless noted otherwise, these options are supported by the Siebel LDAP and ADSI security adapters and by adapters that comply with the *Siebel Security Adapter Software Developer's Kit (SDK) version 3.0.* For more information, see 476962.1 (Article ID) on My Oracle Support.

Depending on your security adapter or Web SSO implementation, you might have to configure the following:

- "Configuring the Application User" on page 147
- "Configuring Checksum Validation" on page 149
- "Configuring Secure Communications for Security Adapters" on page 150
- "Configuring the Shared Database Account" on page 151
- "Configuring Adapter-Defined User Name" on page 154
- "Configuring the Anonymous User" on page 155
- "Configuring Roles Defined in the Directory" on page 157

Configuring the Application User

This topic describes how to configure the directory application user. The application user is not an actual user who logs into an application; it is a special user defined to handle access to the directory. The application user is defined as the only user with search, read and write privileges to the LDAP directory or Active Directory. This minimizes the level of access of all other users to the directory and the administration required to provide such access.

The application user must be defined in the following authentication strategies that implement a Siebel security adapter:

- Security adapter authentication: LDAP, ADSI, some custom security adapter implementations

  You do not have to define an application user if you implement a database security adapter.

- Web SSO authentication

  Whether or not an application user must be defined depends on how you have implemented the Web SSO solution.

About Application User Permissions

The application user is the only user who can read or write user information in the directory. Therefore, it is critical that the application user has appropriate privileges to the directory. The application user must be defined in the directory with the following qualities:

- The application user provides the initial binding of the LDAP or Active Directory server with the Application Object Manager when a user requests the login page. Otherwise, binding defaults to the anonymous user.
- Assign the application user sufficient permissions to read any user's information in the directory and do any necessary administration:
  - In a Siebel security adapter implementation, the application user must have search and write privileges for all user records in the directory. In a Web SSO implementation, the application user must have, at least, search privileges.
  - For ADSI authentication, it is recommended that you use the Active Directory Delegation of Control Wizard to define privileges for users in Active Directory.

    If you are using a Microsoft Active Directory server, then you *must* use the Delegation of Control Wizard to assign the following permissions to the application user on the Users base DN:

    - Create, delete, and manage user accounts
    - Reset passwords on user accounts
    - Read all user information
- If you are configuring an ADSI security adapter, then the application user must either be a domain user or have access to the directory server. If the application user cannot access the directory server, then the authentication process fails.
- Permissions for the application user must be defined at the organization level (for example, OU for LDAP).

Defining the Application User

The following procedure describes how to define the application user.

To define the application user

1 Define a user in the directory, using the same attributes as for other users.

Assign values in appropriate attributes that contain the following information:

- **Username.** Assign a name of your choice. If you implement an adapter-defined user name, then use that attribute (for further information, see "Configuring Adapter-Defined User Name" on page 154). Otherwise, use the attribute in which you store the Siebel user ID, although the application user does not have a Siebel user ID.
- **Password.** Assign a password of your choice. Enter the password in unencrypted form. If you are using an Active Directory, then you specify the password using Active Directory user management tools, not as an attribute.

  You maintain an unencrypted password for the application user in the directory, while an encrypted version of the password is used in other phases of the authentication process. An encryption algorithm is applied to the application user password before it is sent to the database. The application user login must also be set up with the encrypted version of the password.

2 Assign appropriate permissions to the application user in the directory as described in "About Application User Permissions" on page 147.

3 For your Siebel security adapter, define the following parameter values for the security adapter's enterprise profile (such as LDAPSecAdpt or ADSISecAdpt) on the Siebel Gateway Name Server.

- **ApplicationUser.** Enter the application user's full distinguished name (DN) in the directory.

  For example, ApplicationUser can be set as in the following example:

  ```
  ApplicationUser = "uid=APPUSER, ou=people, o=example.com"
  ```

- **ApplicationPassword.** Enter the application user password (unencrypted).

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 361. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center. For Gateway Name Server authentication, define these parameters in the gateway.cfg file.

Application User and Password Expiration Policies

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

If you implement a password expiration policy in the directory, then exempt the application user from the policy so the application user's password will not expire. To do this, set the application user's password policy explicitly after the application user sets the password policy for the whole directory. For more information about account policies and password expiration, see "Login Security Features" on page 202.

Configuring Checksum Validation

The checksum validation option verifies that the security adapter loaded by the authentication manager is the correct version. It is recommended that you use checksum validation to make sure that the appropriate security adapter provides user credentials to the authentication manager for all users who request access.

Checksum validation for security adapters can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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

Checksum validation supports the following principles:

- A CRC (cyclical redundancy check) checksum value for the security adapter library file (such as the DLL file on Windows) is stored as a configuration parameter value for the security adapter.
- When a security adapter provides a user identity and database account to the Application Object Manager, a checksum value is calculated for that security adapter.
- The user is granted access if the two checksum values are equal.

The following procedure outlines the steps in implementing checksum validation.

To configure checksum validation

1. Enter and run the following command at a command prompt, using the required security adapter library file name (such as the DLL file on Windows) as the argument:

   ```
   checksum -f filename
   ```

   The utility returns the checksum value.

   For example, if you are using an LDAP security adapter, then the following command:

   ```
   checksum -f sscforacleldap.dll
   ```

   returns something similar to:

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

   NOTE: You must specify a different DLL file if you are using an ADSI security adapter or a custom security adapter.

2 For the security adapter you are using, set the CRC configuration parameter to the checksum value that is calculated in Step 1 on page 149.

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 361. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center. For Gateway Name Server authentication, define these parameters in the gateway.cfg file.

In previous Siebel CRM releases, the CRC checksum value was set using the Security Adapter CRC system preference, rather than a configuration parameter.

NOTE: The checksum value in this procedure is an example only. You must run the checksum utility as described to generate the value that is valid for your implementation. In addition, you must recalculate the CRC checksum value and update the CRC parameter value each time you upgrade your Siebel Business Applications, including each time you apply a Siebel Patchset.

Configuring Secure Communications for Security Adapters

This topic describes how to use SSL or TLS to transmit data between a security adapter provided with Siebel Business Applications and an LDAP directory or Active Directory. Secure communications for the Siebel security adapter can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

The setup you must do to implement SSL or TLS differs depending on whether you implement the LDAP or ADSI security adapter. If you use the LDAP security adapter to authenticate against Active Directory, then you must configure SSL between the LDAP security adapter and the Active Directory server if you want to manage user passwords or create new users in the Active Directory. Implementing SSL in these circumstances is a requirement of Microsoft Windows and Active Directory.

NOTE: SSL encryption is supported with the LDAP security adapter. TLS encryption is supported with the ADSI security adapter. The SSL encryption standard is not secure. It is recommended that you implement additional methods of securing connections between the LDAP security adapter and directory servers.

Configuring SSL for the LDAP Security Adapter

The following procedure describes how to configure SSL for the LDAP security adapter.

To configure SSL for the LDAP security adapter

1. Set the SslDatabase parameter value for the security adapter (LDAPSecAdpt) to the absolute directory path of the Oracle wallet.

   The Oracle wallet, generated using Oracle Wallet Manager, contains a certificate for the certificate authority that is used by the directory server. For information, see "Creating a Wallet for Certificate Files When Using LDAP Authentication with SSL" on page 121.

2. Set the WalletPassword parameter for the LDAP security adapter (LDAPSecAdpt) to the password assigned to the Oracle wallet.

Configuring TLS for the ADSI Security Adapter

The following procedure describes how to configure TLS for the ADSI security adapter.

To configure TLS for the ADSI security adapter

1. Set up an enterprise certificate authority in your domain.
2. Set up the public key policy so that the Active Directory server automatically demands a certificate from that certificate authority.
3. Set the profile parameter UseSsl to True for the ADSI Security Adapter profile (alias ADSISecAdpt).

   For information about setting Siebel Gateway Name Server parameters, see "Siebel Gateway Name Server Parameters" on page 361.

Configuring the Shared Database Account

You can configure your authentication system so that a designated directory entry contains a database account that is shared by many users; this is the shared database account. The shared database account option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

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

The shared database account option can be specified for the LDAP and ADSI security adapters as follows:

- The shared database account credentials can be specified in an attributes of the shared database account record in the directory. Database credentials are retrieved from the shared database account if they are available to be extracted. If database credentials are not available from the shared database account, then they are instead retrieved from the user. For information, see "Storing Shared Database Account Credentials as Directory Attributes" on page 152.

- The shared database account credentials can be specified as profile parameters (SharedDBUsername and SharedDBPassword) for the LDAP or ADSI Security Adapter profiles. If you want to implement a shared database account, then it is recommended that you specify database credentials as profile parameters. For information, see "Storing Shared Database Account Credentials as Profile Parameters" on page 153.

When storing database credentials in a directory attribute, both the user name and password are stored as plain text, even if you implement database credentials password hashing (in this case the hashed password is maintained in the database, while an unhashed version of the password is stored in the directory). Specifying database credentials as profile parameters avoids having to store database credentials as plain text in the directory.

Shared Database Accounts and Administrative Users

Even if you implement a shared database account with external directory authentication, the shared database account cannot be used for any user who requires administrator access to Siebel Business Applications functionality, for example, any user who has to perform Siebel Server management and configuration tasks. For these users, you must either:

- Create a separate database account.

  The database account user ID and password you create for the user must match the user ID and password specified for the user in the external directory.

- Do the following:
  - Implement LDAP or ADSI authentication for the Gateway Name Server.
  - Create a user account record in the directory for the user requiring administrator access.
  - In the attribute of the record that is used to store role information, specify the user role that is required to access the Gateway Name Server: Siebel Administrator is the default role.

The following topics describe in more detail how the LDAP and Active Directory servers use the shared database account option.

Storing Shared Database Account Credentials as Directory Attributes

This topic describes how to implement a shared database account and store the database credentials as attributes of the directory entry you create for the shared database account. This option is available to you when you use either the LDAP or ADSI security adapters.

To store shared database credentials in an attribute of the directory entry

1. Create a database account to be shared by all users who log into a given Siebel application; the account must have administrator privileges.

2 Create a designated entry in the directory, and enter the user name and password parameters for the shared database account in one of that entry's attributes, such as the dbaccount attribute. You might have to create this attribute.

NOTE: The user name and password you specify for the shared database account must be a valid Siebel user name and password and must have administrator privileges.

For information about formatting a directory attribute that contains the database account, see "Requirements for the LDAP Directory or Active Directory" on page 111.

3 For each security adapter that implements this shared database account, specify values for the parameters shown in the following table.

Parameter	Value
CredentialsAttributeType	Enter the attribute in which the database account is stored in the directory, for example, dbaccount.
SharedCredentialsDN	Enter the distinguished name (including quotes) for the designated entry, such as: `"uid=SHAREDENTRY, ou=people, o=example.com"`

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 361. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center. For Gateway Name Server authentication, define these parameters in the gateway.cfg file.

Storing Shared Database Account Credentials as Profile Parameters

This topic describes how to configure a shared database account for an LDAP directory or Active Directory and how to store the database credentials for the account as parameters of either the LDAP or the ADSI Security Adapter profile.

It is recommended that you store shared database account credentials as profile parameters unless you have to store more than one set of database credentials, as only one set of database credentials can be stored as profile parameters.

To store shared database credentials as profile parameters

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

2 Select either the LDAPSecAdpt profile or the ADSISecAdpt profile.

3 Specify values for the following parameters for the LDAPSecAdpt or ADSISecAdpt profile.

Parameter	Value
SharedDBUsername	Enter the user name to connect to the Siebel database.
SharedDBPassword	Enter the password to connect to the Siebel database

NOTE: You must specify a valid Siebel user name and password for the SharedDBUsername and SharedDBPassword parameters.

Configuring Adapter-Defined User Name

You can configure your authentication system so that the user name presented by the user and passed to the directory to retrieve a user's database account is not the Siebel user ID. For example, you might want users to enter an adapter-defined user name, such as their Social Security number, phone number, email address, or account number. The security adapter returns the Siebel user ID of the authenticated user and a database account from the directory to the authentication manager.

The adapter-defined user name option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

The adapter-defined user name must be stored in one attribute in your directory, while the Siebel user ID is stored in another attribute. For example, users can 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 (alias UsernameBCField) parameter for the Application Object Manager defines the field of the User business component that underlies the attribute specified by UsernameAttributeType.

Even if other requirements to administer user attributes in the directory through the Siebel client are met, you must also set the UsernameAttributeType parameter for the security adapter, and set the OM - Username BC Field parameter. If you do not define these parameters appropriately, then changes through the Siebel client to the underlying field are not propagated to the directory.

For example, for users to log in with their work phone number, you must specify UsernameAttributeType to be the directory attribute in which the phone number is stored, for example, telephonenumber, and you must define OM - Username BC Field to be Phone #, the field in the User business component for the work phone number.

The following procedure outlines how to configure an adapter-defined user name.

To configure an adapter-defined user name

1 For each security adapter (such as LDAPSecAdpt) that implements an adapter-defined user name, define the following parameter values:

Parameter	Value
UseAdapterUsername	TRUE
SiebelUserNameAttributeType	The attribute in which you store the Siebel user ID, such as uid (LDAP) or sAMAccountName (ADSI).
UsernameAttributeType	The attribute in which you store the adapter-defined user name, such as `telephonenumber`.

For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 361. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center. For Gateway Name Server authentication, define these parameters in the gateway.cfg file.

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

The Application Object Manager parameter to be populated is OM - Username BC Field.

For information about working with Siebel business components, see *Configuring Siebel Business Applications*. For information about working with configuration parameters, see *Siebel System Administration Guide*.

3 Using Siebel Server Manager, specify the User business component field name as the value for the OM - Username BC Field parameter. You can provide this value at the Enterprise, Siebel Server, or component level. If this parameter is not present in the parameters list, then add it.

NOTE: The OM - Username BC Field parameter is case sensitive. The value you specify for this parameter must match the value specified for the parameter in Siebel Tools.

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

Configuring the Anonymous User

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

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

Anonymous Browsing and the Anonymous User

If you implement security adapter or database authentication, then you can allow or disallow unregistered users to browse a subset of an application's views. Unregistered users access Siebel application views and the database through the anonymous user record.

If you allow anonymous browsing, then users can browse views that are not flagged for explicit login. If you disallow anonymous browsing, then unregistered users have no access to any of the application's views but do still have access to an application's login page. For additional information on enabling anonymous browsing, see "Process of Implementing Anonymous Browsing" on page 215.

The following procedure describes how to configure the anonymous user.

To configure the anonymous user

1. If you are using database security adapter authentication, then create a database account for the anonymous user.
2. If you are using LDAP or ADSI security adapter authentication, then define a user in the directory using the same attributes as used for other users. Assign values in appropriate attributes that contain the following information:
   - **Siebel user ID.** Enter the user ID of the anonymous user record for the Siebel application you are implementing in the attribute in which you store the Siebel user ID, for example, GUESTCST.
   - **Password.** Assign a password of your choice. Enter the password in unencrypted form. If you have implemented Active Directory, then you specify the password using Active Directory user management tools, not as an attribute.
3. Specify values for the following parameters, either when configuring the SWSE logical profile (recommended), or by editing the eapps.cfg file manually:
   - **AnonUserName.** Enter the user name required for anonymous browsing and initial access to the login pages of the application you are implementing, in this example, GUESTCST.
   - **AnonPassword.** Enter the password associated with the anonymous user. If necessary, you can manually encrypt this password using the encryptstring.exe utility. For additional information, see "Encrypting Passwords Using the encryptstring Utility" on page 47.

   You can define an anonymous user for a single application or as the default for all the Siebel Business Applications you deploy. Even if the anonymous user is specified as the default, any single application can override the default.

   If you use one anonymous user for most or all of your applications, then define the anonymous user in the [defaults] section of the eapps.cfg file. To override the default value for an individual application, list the AnonUserName and AnonPassword parameters in the application's section of the eapps.cfg file, for example, the [/eservice] section.

Configuring Roles Defined in the Directory

Responsibilities assigned to each user in Siebel Business Applications provide users with access to particular views in the application. Responsibilities are created in the Siebel application and are stored in the Siebel database. One or more responsibilities are typically associated with each user in the Administration - Application screen.

Creating roles in the LDAP directory or Active Directory is another means of associating Siebel responsibilities with users. Roles are useful for managing large collections of responsibilities. A user has access to all the views associated with all the responsibilities that are directly or indirectly associated with the user.

You can choose to store users' Siebel responsibilities as roles in a directory attribute instead of in the Siebel database in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

NOTE: You can store Siebel user responsibilities as roles in a directory attribute but you cannot store Siebel user positions as roles in a directory attribute.

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, then leave the attribute empty. If you use roles to administer user responsibilities, then create responsibilities in the Siebel application, but do not assign responsibilities to users through the Siebel application interface.

To configure roles defined in the directory

1. In the directory, define a directory attribute for roles.

   To make sure that you can assign more than one responsibility to any user, define the roles directory attribute as a multivalue attribute. The security adapters supported by Siebel Business Applications cannot read more than one responsibility from a single-value attribute.

2. For each user, in the directory attribute for roles, enter the names of the Siebel responsibilities that you want the user to have. Enter one responsibility name, such as Web Registered User, in each element of the multivalue field. Role names are case-sensitive.

3. Configure the security adapters provided with Siebel Business Applications to retrieve roles for a user from the directory by setting the RolesAttributeType parameter for the LDAP or ADSI security adapter. For example, for the LDAP security adapter, define the following parameter:

   `RolesAttributeType= attribute_in_which_roles_are_stored`

   For information about setting Siebel Gateway Name Server configuration parameters, see "Siebel Gateway Name Server Parameters" on page 361. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center. For Gateway Name Server authentication, define these parameters in the gateway.cfg file.

About Password Hashing

This topic describes the password hashing options available with Siebel Business Applications. User passwords and database credentials passwords can be hashed for greater security. Hashing passwords is recommended.

Unlike encryption that involves two-way algorithms (encryption and decryption), hashing uses a one-way algorithm. A clear-text version of a password is hashed using a Siebel utility, then stored in the database or in an external directory such as LDAP or ADSI. During login, a clear-text version of a password is provided (such as by a user), which is then hashed and compared to the stored hashed password.

The password hashing options available with Siebel Business Applications are as follows:

- **User password hashing.** When you are using security adapter authentication (including database, LDAP or ADSI, or custom security adapters), user passwords can be hashed.

  A hashed password is maintained for each user, while the user logs in with an unhashed (clear-text) version of the password. This password is hashed during login.

  Password hashing is a critical tool for preventing unauthorized users from bypassing Siebel Business Applications and logging directly into the Siebel database using an RDBMS tool such as SQL*Plus. It also prevents passwords intercepted over the network from being used to access the applications, because an intercepted hashed password will itself be hashed when login is attempted, leading to a failed login.

- **Adding salt values to user passwords.** In the current release, if you are using an LDAP, ADSI, or a custom security adapter you can choose to prefix a user's password with a salt value (a random string) before the password is hashed. The result of the hash function and the salt value are then stored in the security adapter directory. During authentication, the user password supplied is prefixed with the stored salt value and hashing is applied. If this computed value matches the hash value in the directory, then the user is authenticated.

  NOTE: Adding salt values to user passwords is not supported if you are using Web Single Sign-On or database authentication. The SaltUserPwd parameter is ignored if the SingleSignOn parameter is set to TRUE.

  Adding salt values to user passwords provides protection against dictionary attacks on the hashed passwords. By making passwords longer and more random, salt values lessen the likelihood that the hashed passwords can be deciphered. For additional information on the SaltUserPwd parameter, see "Parameters for LDAP or ADSI Authentication" on page 364.

- **Database credentials password hashing.** When you are using security adapter authentication other than database authentication (LDAP, ADSI, or custom security adapters), or if you are using Web SSO authentication, database credentials passwords can be hashed.

  A hashed password for a database account is maintained in the database, while an unhashed (clear-text) version of the password is stored in the external directory. This password is hashed and compared during database login.

  Credentials password hashing prevents users from being able to log into the Siebel database directly using a password obtained through unauthorized access to the external directory because the unhashed password in the directory will not match the hashed version stored in the database.

- **Password hashing utility.** Siebel Business Applications provide a password hashing utility called hashpwd.exe which uses the RSA SHA-1 hashing algorithm by default. For existing customers, the Siebel proprietary hashing algorithm (the mangle algorithm) is also available as an option for the hashpwd.exe utility.

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

For information about managing encrypted passwords in the eapps.cfg file, see "Encrypted Passwords in the eapps.cfg File" on page 46. The password encryption mechanism described there is unrelated to the password hashing mechanism described in this topic.

Login Scenario for Password Hashing

This topic describes the login process for a Siebel application user when password hashing has been implemented. A user is logged into the Siebel application by the following process:

1. The user logs in with user credentials that include the unhashed password.
2. The Application Object Manager receives the user credentials, and passes them to the authentication manager.
3. If user password salting is enabled, then the authentication manager retrieves the salt value associated with the user password from the LDAP, ADSI, or custom security adapter directory and prefixes it to the user provided password.
4. The authentication manager hashes the password, according to the configuration of the security adapter.
   - In a database authentication environment:
     - The authentication manager passes the user credentials (user ID and hashed password) to the database security adapter.
     - The database security adapter verifies that the hashed password matches the hashed password stored in the database for the user. It validates the credential by trying to connect to the database server. The security adapter confirms to the Application Object Manager, through the authentication manager, that the credentials are valid.
   - In an LDAP or ADSI authentication environment:
     - The authentication manager passes the user credentials, including the hashed password, to the LDAP or ADSI security adapter.
     - The LDAP or ADSI security adapter verifies that the hashed password matches the hashed password stored in the directory for the user, and then returns the database account and the Siebel user ID to the Application Object Manager through the authentication manager.
5. The Application Object Manager initiates a Siebel application session for the user.

Related Topics

"Process of Configuring User and Credentials Password Hashing" on page 160

"Running the Password Hashing Utility" on page 163

Process of Configuring User and Credentials Password Hashing

This topic describes how to implement password hashing for user passwords or for database credentials, how to implement the use of salt values for user passwords, and how to specify the default hashing algorithm.

Configuration parameters for all security adapters provided with Siebel Business Applications, and for custom security adapters you implement, specify the password hashing settings in effect. For LDAP or ADSI authentication, parameters are specified for the security adapter. For database authentication, the relevant parameters are specified for a data source referenced from the database security adapter, rather than specified directly for the security adapter.

To configure password hashing, perform the following tasks:

1. Review "Guidelines for Password Hashing" on page 160
2. Perform either or both of the following tasks, as appropriate:
   - "Configuring User Password Hashing" on page 161
   - "Configuring Password Hashing of Database Credentials" on page 162

   NOTE: Some steps in these procedures, such as those for setting configuration parameter values using Siebel Server Manager, can alternatively be accomplished by using the Siebel Configuration Wizard.

Guidelines for Password Hashing

This topic describes the factors to consider if you choose to implement password hashing with Siebel Business Applications.

This task is a step in "Process of Configuring User and Credentials Password Hashing" on page 160.

Guidelines for using password hashing with Siebel Business Applications include the following:

- The password hashing utility, hashpwd.exe, does not automatically store hashed passwords or salt values in the Siebel database, LDAP directory, or Active Directory. The administrator is responsible for defining and storing the hashed passwords and salt values. A hashed password is stored in one of the following locations:
  - In a database authentication environment, the hashed password is set as the valid password for the database account.
  - In an LDAP or Active Directory authentication environment, the hashed password is stored in the attribute specified for the user's password. The password salt value is stored in the attribute specified for the salt value.
- The unhashed version of the password is given to a user to use when logging in.
- Stored passwords must first be hashed (after salt values are added, if applicable) with the same hashing algorithm (typically, RSA SHA-1) that is applied to the passwords in the authentication process.

- Database credentials passwords stored outside of the Siebel database must be stored in unhashed form, because such passwords are hashed during the authentication process. For additional information, see "About Password Hashing" on page 158.
- With database authentication, the Siebel Server components that log in to the database must use the hashed password value stored in the Siebel database. Otherwise, the component login will fail.

  For example, when you run the Generate Triggers (GenTrig) component, the value provided for the PrivUserPass parameter (used along with the PrivUser parameter) must be the hashed password value.

  To determine if a Siebel Server component uses a hashed password, select the component from the Enterprise Component Definition View and query for the component parameter OM - Data Source. If the value that OM - Data Source references has DSHashAlgorithm set to a hashing algorithm and DSHashUserPwd set to TRUE, then it means that the component can accept an unhashed password and hash it using the specified parameters.
- Password hashing and use of salt values must be specified consistently for all Siebel Enterprise components that will work together. For example, all Siebel Servers subject to Application Object Manager load balancing must use the same security adapter settings, including those for password hashing, or component login will fail.
- For the Siebel Mobile Web Client, password hashing for the local database password has the following requirements:
  - The parameter Encrypt client Db password (alias EncryptLocalDbPwd) must have been set to TRUE for the server component Database Extract (alias DbXtract) at the time the user's local database was extracted. See *Siebel Remote and Replication Manager Administration Guide* for details.
  - The database security adapter must be in effect for the Mobile Web Client, and the DSHashUserPwd and DSHashAlgorithm parameters must be set appropriately for the data source specified for the security adapter. For more information, see "About Database Authentication" on page 102 and "Siebel Application Configuration File Parameters" on page 376.

Configuring User Password Hashing

The procedure in this topic describes how to configure user password hashing with Siebel Business Applications.

This task is a step in "Process of Configuring User and Credentials Password Hashing" on page 160

To implement user password hashing

1. For each user, create and record a user name and a password.
2. To hash one or more passwords, run the hashpwd.exe utility at a command prompt. For command syntax options, see "Running the Password Hashing Utility" on page 163.

3 For each user, do one of the following:

- In a database authentication environment, set the credentials for a database account to the user name and the hashed password. For information about setting credentials for database accounts, see your RDBMS documentation.
- In an LDAP or ADSI authentication environment, set the values in the directory attributes for user name, password, and salt to the user name, hashed password, and salt value returned by the hashpwd.exe utility.

4 Using Siebel Server Manager, configure the security adapter for user password hashing as follows:

- For the database security adapter (typically, DBSecAdpt):
  - Set the DataSourceName parameter to the name of the applicable data source (for example, ServerDataSrc).
  - For the applicable data source, set the DSHashUserPwd parameter to TRUE.
  - For the applicable data source, set the DSHashAlgorithm parameter to RSASHA1 (this is the default value) or SIEBELHASH (the Siebel proprietary algorithm).
- For the LDAP or ADSI security adapter (typically, LDAPSecAdpt or ADSISecAdpt):
  - Set the HashUserPwd parameter to TRUE.
  - Set the HashAlgorithm parameter to RSASHA1 (this is the default value) or SIEBELHASH (the Siebel proprietary algorithm).
  - (Optional) Set the SaltUserPwd parameter to TRUE to specify that salt values can be added to user passwords.
  - (Optional) Set the SaltAttributeType parameter to specify the attribute that is to store the salt value.

5 Provide each user with the user name and the clear-text password for logging in.

Related Topics

"About Password Hashing" on page 158

"Configuring Password Hashing of Database Credentials" on page 162

Configuring Password Hashing of Database Credentials

The procedure in this topic describes how to configure database credentials password hashing with Siebel Business Applications.

This task is a step in "Process of Configuring User and Credentials Password Hashing" on page 160.

To implement database credentials password hashing

1 For each applicable database account, create and record a login name and a password.

2 To hash one or more passwords, run the hashpwd.exe utility at a command prompt. For command syntax options, see "Running the Password Hashing Utility" on page 163.

3 For each database account, assign the hashed passwords to their corresponding database accounts.

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

4 In the LDAP directory or Active Directory, specify the unhashed version of the password for the attribute that contains the database account.

   The database credentials password must be stored in unhashed form in the directory because the password is hashed during the authentication process. Users cannot log into the Siebel database using a password obtained through unauthorized access to the directory because the unhashed password in the directory will not match the hashed version stored in the database.

   As an additional security measure, however, you can define an access control list (ACL) to restrict access to the directory attribute containing the unhashed version of the password or, if you are implementing a shared database account, the shared database login name and hashed password can be specified as profile parameters for the LDAP or ADSI Security Adapter profiles.

   For information about required attributes in the directory, see "Requirements for the LDAP Directory or Active Directory" on page 111. For information on setting up directory ACLs, see your directory vendor documentation.

5 Using Siebel Server Manager, configure the security adapter for credentials password hashing. For the LDAP or ADSI security adapter:

   - Set the HashDBPwd parameter to TRUE.
   - The hash algorithm is based on the setting you previously made for the HashAlgorithm parameter when you configured user password hashing.

Related Topics

"About Password Hashing" on page 158

"Configuring User Password Hashing" on page 161

Running the Password Hashing Utility

This topic describes how to hash user passwords and generate salt values using the hashpwd.exe utility. The hashpwd.exe utility is located in *SIEBSRVR_ROOT*\bin (Siebel Server installation directory) or *SIEBEL_CLIENT_ROOT*\bin (Siebel Mobile or Developer Web Client installation directory).

You can hash passwords using the RSA SHA-1 hashing algorithm or the siebelhash algorithm. The procedures in this topic describe how to hash passwords using both algorithms.

When you have hashed user passwords using hashpwd.exe, store the hashed passwords and salt values in the directory or database, as appropriate. For information on storing hashed passwords, see "Guidelines for Password Hashing" on page 160. For information about the password hashing options mentioned in the procedures in this topic, see "About Password Hashing" on page 158.

Hashing Passwords Using the RSA SHA-1 Algorithm

The following procedure describes how to run the hashpwd.exe utility using the default password hashing algorithm, RSA SHA-1.

To hash passwords using the RSA SHA-1 algorithm

- To hash a password using the RSA SHA-1 algorithm, run the hashpwd.exe utility using one of the following syntaxes:
  - To hash individual passwords, use the following syntax:

    ```
    hashpwd password1 password2 ...
    ```

    ```
    hashpwd -a rsasha1 password1 password2 ...
    ```

  - To hash individual passwords and generate salt values for each password, use the following syntax:

    ```
    hashpwd -a rsasha1 -s salt_length password1 password2 ...
    ```

    where *salt_length* specifies the length, in bytes, of the salt value. Enter a value between 1 and 16. For example, for the clear text password, PassWord02, the hash values generated by the hashpwd.exe utility using the default rsasha1 option are as follows:

    ```
    Salt : HyviRlb2yP
    ```

    ```
    Password: UctMxQ+DoRlQZgiHIl7ghDy1bJM=
    ```

  - To hash multiple passwords using a batch file, enter the passwords into a batch file (for example, the file might be named passwords.txt), and then specify the filename using the following syntax:

    ```
    hashpwd @password_file_name
    ```

Hashing Passwords Using the Siebelhash Algorithm

The following procedure describes how to run the hashpwd.exe utility using the Siebel proprietary password hashing algorithm.

To hash passwords using the siebelhash algorithm

- To hash passwords using the Siebel proprietary password hashing algorithm, run the hashpwd.exe utility using one of the following syntaxes:
  - To hash individual passwords, use the following syntax:

    ```
    hashpwd -a siebelhash password1 password2 ...
    ```

  - To hash individual passwords and generate salt values for each password, use the following syntax:

    ```
    hashpwd -a siebelhash -s salt_length password1 password2 ...
    ```

    where *salt_length* specifies the length, in bytes, of the salt value. Enter a value between 1 and 16.

- To hash multiple passwords using a batch file, enter the passwords into a batch file (for example, the file might be named passwords.txt), and then specify the filename using the following syntax:

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

Related Topic
"About Password Hashing" on page 158

About Authentication for Gateway Name Server Access

The Siebel Gateway Name Server serves as the dynamic registry for Siebel servers and components. The Gateway Name Server provides startup information to the application servers and, if compromised, could propagate changes throughout the server environment. To prevent unauthorized changes to the enterprise configuration parameters on the Gateway Name Server, user access to the Gateway Name Server is authenticated. (Authentication is not implemented for starting the Gateway Name Server, only for connecting to it.)

Gateway Name Server authorization is required whether you use the Siebel Configuration Wizard, Siebel Server Manager, or other utilities to access the Gateway Name Server. In each case, you must specify a valid Gateway Name Server authentication user name and password. For information on the Gateway Name Server authentication credentials, see "About the Gateway Name Server Authentication Password" on page 44.

Authentication Mechanisms

You can choose to use database authentication, LDAP authentication, or Active Directory authentication for the Gateway Name Server.

When you configure the Siebel Enterprise Server using the Siebel Configuration Wizard, you choose the type of authentication provider to use by specifying values for the SecAdptName and SecAdptMode parameters (see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123 for further information). These, and the other security-related configuration values you specify, apply to both the Siebel Enterprise and the Gateway Name Server; these values are used to populate information in various different configurations including the Gateway Name Server configuration file, gateway.cfg.

The Siebel Enterprise and Gateway Name Server are configured to use database authentication by default. If you choose to implement database authentication in your Siebel deployment, then after configuring the Siebel Enterprise Server, no additional steps are required.

If you configure the Enterprise and the Gateway Name Server to use LDAP, ADSI or a custom security adapter using the Siebel Configuration Wizard, then the configuration is not implemented until it is changed manually after configuration. For the Gateway Name Server, this requires editing the gateway.cfg file. For information on implementing LDAP or ADSI authentication for the Gateway Name Server, see "Implementing LDAP or ADSI Authentication for the Gateway Name Server" on page 166.

About the gateway.cfg File

The Gateway Name Server authentication configuration is stored in the gateway.cfg file, which is located in the *SIEBEL_ROOT*\gtwysrvr\bin (Windows) or *SIEBEL_ROOT*/gtwysrvr/bin (UNIX) directory. Parameters for the authentication type as well as parameters for the authentication subsystems are stored in this file.

When a user attempts to log in to the name server, the user's credentials are passed by the name server to the authentication provider specified in the gateway.cfg file, which checks that the user has the required administrator privileges to access the name server. If it has, the Gateway Name Server starts to process service requests. For detailed information on the Gateway Name Server authentication configuration parameters, see "Parameters in the Gateway.cfg File" on page 372.

Implementing LDAP or ADSI Authentication for the Gateway Name Server

This topic describes how to implement LDAP or ADSI authentication for the Gateway Name Server. This involves configuring the Siebel Enterprise Server for LDAP or ADSI authentication using the Siebel Configuration Wizard, then adding parameters to the Gateway Name Server configuration file (gateway.cfg) and the LDAP directory or Active Directory. These tasks are described in the following procedure.

To implement LDAP or ADSI authentication for the Gateway Name Server

1. Using the Siebel Configuration Wizard, configure your Siebel Enterprise to use either the LDAP or ADSI security adapter provided with Siebel Business Applications.

   For information on this task, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123.

2. Add parameters to the gateway.cfg file to specify the security adapter you want to implement.

   For information on the gateway.cfg file, see "About Authentication for Gateway Name Server Access" on page 165. Specify values similar to the following:

Section	Parameter	Value
[InfraSecMgr]	Security Adapter Mode (SecAdptMode)	The security adapter mode to operate in: ■ For LDAP, specify LDAP. ■ For ADSI, specify ADSI.

Section	Parameter	Value
[InfraSecMgr]	Security Adapter Name (SecAdptName)	The name of the security adapter. ■ For LDAP, specify LDAPSecAdpt or another name of your choice. ■ For ADSI, specify ADSISecAdpt or another name of your choice.
[LDAPSecAdpt] or [ADSISecAdpt]	Roles Attribute Type (RolesAttributeType)	The name of the directory attribute that is used to store role information, for example, roles.

3 Add the following information to the LDAP directory or Active Directory:

- Gateway Name Server authentication user name and password.
- For the Gateway Name Server user, in the directory attribute that is used to store role information (for example, the roles attribute), specify the user role that is required to access the Gateway Name Server. Specify Siebel Administrator as the default role.

Security Adapters and the Siebel Developer Web Client

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

- Application Object Manager (through the siebel.exe program)
- Application configuration file
- Authentication manager and security adapter
- Oracle Database Client (where applicable)

NOTE: Siebel Business Applications support for the Siebel Developer Web Client is restricted to administration, development, and troubleshooting usage scenarios only. Siebel Business Applications does not support the deployment of this client to end users.

When you implement security adapter authentication for Siebel Developer Web Clients, observe the following principles:

- It is recommended to use the remote configuration option, which can help you make sure that all clients use the same configuration settings. This option is described later in this topic.
- Authentication-related configuration parameters stored in application configuration files on client computers, or stored in remote configuration files, must generally contain the same values as the corresponding parameters in the Siebel Gateway Name Server (for Siebel Web Client users). Distribute the appropriate configuration files to all Siebel Developer Web Client users. For information about setting parameters in Siebel application configuration files on the Siebel Developer Web Client, see "Siebel Application Configuration File Parameters" on page 376.

- It is recommended that you use checksum validation to make sure that the appropriate security adapter provides user credentials to the authentication manager for all users who request access. For information about checksum validation, see "Configuring Checksum Validation" on page 149.
- In a security adapter authentication implementation, you must set the security adapter configuration parameter PropagateChange to TRUE, and set the Siebel system preference SecThickClientExtAuthent to TRUE, if you want to implement:
  - Security adapter authentication of Siebel Developer Web Client users.
  - Propagation of user administration changes from the Siebel Developer Web Client to an external directory such as LDAP or ADSI. (For example, if a user changes his or her password in the Developer Web Client, then the password change is also propagated to the directory.)

  For more information, see "Siebel Application Configuration File Parameters" on page 376 and "Configuring LDAP or ADSI Authentication for Developer Web Clients" on page 141.
- In some environments, you might want to rely on the data server itself to determine whether to allow Siebel Developer Web Client users to access the Siebel database and run the application. In the application configuration file on the local client, you can optionally define the parameter IntegratedSecurity for the server data source (typically, in the [ServerDataSrc] section of the configuration file).

  This parameter can be set to TRUE or FALSE. The default value is FALSE. When TRUE, the Siebel client is prevented from prompting the user for a user name and password when the user logs in. Facilities provided in your existing data server infrastructure determine if the user is allowed to log into the database.

  You can set the IntegratedSecurity parameter to TRUE with the database security adapter. See also "About Database Authentication" on page 102.

  NOTE: Integrated Security is only supported for Siebel Developer Web clients that access Oracle and Microsoft SQL Server databases. This functionality is *not* available for Siebel Web Clients or Siebel Mobile Web clients.

For additional information on integrated authentication, refer to your third-party documentation. For Oracle, refer to the OPS$ and REMOTE_OS_AUTHENT features. For Microsoft SQL Server, refer to Integrated Security. For more information about the Siebel Developer Web Client, see the *Siebel Installation Guide* for the operating system you are using and the *Siebel System Administration Guide*.

Sample LDAP Section in Configuration File

The following sample is an example of LDAP configuration information generated by the Siebel Configuration Wizard when you configure an LDAP security adapter for Developer Web Clients. For more information, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123. For information about setting Siebel configuration parameters, see "Siebel Application Configuration File Parameters" on page 376.

```
[LDAPSecAdpt]
SecAdptDllName = sscforacleldap
ServerName = ldapserver.example.com
Port = 636
BaseDN = "ou=people, o=example.com"
```

```
SharedCredentialsDN = "uid=HKIM, ou=people, o=example.com"
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = mail
RolesAttributeType = roles
SslDatabase =file:c:\sslSLwallet
ApplicationUser = "uid=APPUSER, ou=people, o=example.com"
ApplicationPassword = APPUSERPW
HashDBPwd = TRUE
PropagateChange = TRUE
CRC =
SingleSignOn = TRUE
TrustToken = mydog
UseAdapterUsername = TRUE
SiebelUsernameAttributeType = PHONE
HashUserPwd = TRUE
HashAlgorithm = RSASHA1
```

Remote Configuration Option for Developer Web Client

This option applies to the Siebel Developer Web Client only. The remote configuration option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, custom (not database authentication)
- Web SSO authentication

With this approach, you create a separate text file that defines any parameter values that configure a security adapter. You configure all security adapter parameters, such as those in a section like [LDAPSecAdpt] or [ADSISecAdpt], in the remote file, not in the application configuration file.

Storing configuration parameters in a centralized location can help you reduce administration overhead. All Developer Web Clients can read the authentication-related parameters stored in the same file at a centralized remote location.

The examples below show how a remote configuration file can be used to provide parameters for a security adapter that is implemented by Siebel eService in a Web SSO environment. The following example is from the configuration file uagent.cfg for Siebel Call Center:

```
[InfraSecMgr]
SecAdptMode = LDAP
SecAdptName = LDAPSecAdpt
UseRemoteConfig = \\it_3\vol_1\private\ldap_remote.cfg
```

In this case, the configuration file ldap_remote.cfg would contain an [LDAPSecAdpt] section. It could be defined similarly to the example earlier in this topic, and would contain no other content. The application configuration file would contain the [InfraSecMgr] section as defined above. It would not contain an [LDAPSecAdpt] section and, even if it did, it would be ignored.

To implement remote security configuration for Siebel Developer Web Clients, follow these guidelines:

- The [InfraSecMgr] section in the Siebel configuration file must include the UseRemoteConfig parameter, which provides the path to a remote configuration file. The path is specified in universal naming convention format, for example, `\\server\vol\path\ldap_remote.cfg`.

- The remote security configuration file contains only a section for configuring the security adapter, such as the [LDAPSecAdpt] section.
- Each Developer Web Client user must have read privileges on the remote configuration file and the disk directory where it resides.

About Authentication for Mobile Web Client Synchronization

This topic describes some of the processing that occurs to authenticate a remote user during synchronization. For detailed information about the synchronization process, see *Siebel Remote and Replication Manager Administration Guide*.

The following facts apply to Siebel Remote and remote users:

- Remote users do not connect to the Web server.

  When remote users synchronize, they connect directly from the Siebel Mobile Web Client to the Siebel Remote server, that is, the Siebel Server designated to support synchronization with remote users.
- Only one user ID and password can be used to access a local database. Local databases cannot belong to more than one user.
- A single user can have multiple Mobile Web Clients, such as two clients on two separate computers.

About the Synchronization Process for Remote Users

The Siebel remote user connects to a local database on their client computer, makes transaction modifications, and then synchronizes theses changes to the Siebel Remote server. This involves the following steps:

1. Launch the Siebel icon on the client computer, then enter a user ID and password.
2. In the Connect To parameter, choose Local.

   The user ID and password are validated by the local database residing on the client computer.
3. The Siebel application appears in the Web browser and the user navigates through the application and modifies data, as appropriate (insert, update, or delete operations).
4. Later, the user decides to synchronize the local database changes and download updates from the Siebel Remote server. This involves the following steps:
   a. Connect to the Siebel Remote server using a dial-up modem or LAN, WAN, or VPN connection.
   b. Launch the Siebel icon on the client computer, then enter a user ID and password.
   c. In the Connect To parameter, choose Local.

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

d When the Siebel application appears in the Web browser, the user chooses File, and then Synchronize Database.

   The user is now accessing the Siebel Remote server for synchronization, and is subject to authentication.

e Once the remote user is authenticated, synchronization begins.

Authentication Options for Synchronization Manager

The Synchronization Manager server component for Siebel Remote validates each incoming Mobile Web Client request. Synchronization Manager validates the mobile user's user ID against the list of valid Mobile Web Clients in the server database and validates that the effective end date is valid or NULL.

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

Synchronization Manager authenticates the Mobile Web Client's password by using the method specified using the Authentication Method configuration parameter (alias Authentication). Set this parameter for Synchronization Manager using Siebel Server Manager. For details, see *Siebel Remote and Replication Manager Administration Guide*.

Authentication Method can be set to one of the following values:

- **None.** Does not authenticate the Mobile Web Client's password. This is the default setting.
- **Database.** Uses the Mobile Web Client's user name and password to connect to the server database. Uses the database security adapter to do this (typically, DBSecAdpt).
- **SecurityAdapter.** Uses the security adapter specified using the parameters Security Adapter Mode and Security Adapter Name to authenticate the user. Depending on the security adapter in effect, the user can be authenticated against the database or against an LDAP directory or Active Directory. Password hashing is subject to the configuration of this security adapter.

  The Security Adapter Mode and Security Adapter Name parameters can be set at the Enterprise or Siebel Server level, or set for the Synchronization Manager component. Database authentication is the default security adapter. You can use the same security adapter across the Siebel Enterprise, or use a different security adapter for Synchronization Manager than you do for the rest of the Enterprise. For more information, see "About Siebel Security Adapters" on page 100 and subsequent topics, earlier in this chapter.
- **Siebel.** Validates the Mobile Web Client's password against the password stored in the Mobile Web Client's screen. (This option uses the mangle encryption algorithm, which is generally no longer recommended.)
- **AppServer.** Verifies that the password is the same as the user's operating system password on the Siebel Server computer. (This option is generally no longer recommended.)

About Securing Access to Siebel Reports

Siebel Business Applications use Oracle Business Intelligence Publisher (BI Publisher) to generate Siebel reports, to modify the preconfigured Siebel reports and report templates, and to create custom Siebel reports. Siebel Reports supports two environments: a Siebel Reports disconnected environment, for mobile or disconnected clients, and a Siebel Reports connected environment, for connected clients.

In a disconnected Siebel Reports environment, the Siebel BI Publisher Server is a logical component that uses the local XMLP Report business service and the BI Publisher Engine to manage report generation. The XMLP Report business service and the BI Publisher core libraries are available as part of the Siebel Mobile Web Client and Developer Web Client installations. User authentication mechanisms are not required in a disconnected environment.

In the Siebel Reports connected environment, the BI Publisher is installed separately to Siebel Business Applications. Siebel Web Clients and other connected clients are supported in a Siebel Reports connected environment, but access to the BI Publisher Server is authenticated. For information on the methods available to authenticate user access to the BI Publisher Server in a Siebel Reports connected environment, see *Siebel Reports Guide* and 1501378.1 (Article ID) on My Oracle Support.

6 Web Single Sign-On Authentication

This chapter describes how to implement Web Single Sign-On (Web SSO) for user authentication. It includes the following topics:

- About Web Single Sign-On on page 173
- About Implementing Web Single Sign-On on page 174
- Web Single Sign-On Authentication Process on page 176
- Requirements for Standards-Based Web Single Sign-On on page 177
- Set Up Tasks for Standards-Based Web Single Sign-On on page 178
- Requirements for Microsoft Windows Integrated Authentication on page 179
- Process of Implementing Windows Integrated Authentication on page 180
- About Digital Certificate Authentication on page 191
- Configuring the User Specification Source on page 192
- Configuring the Session Timeout on page 193
- Configuring Siebel CRM and Oracle BI Publisher for Web Single Sign-On on page 194

NOTE: If you are using the Siebel Self-Service Applications available with Siebel CRM Release 8.1, then see *Siebel Self-Service Application Deployment Guide* for additional information on Web Single Sign-On user authentication.

About Web Single Sign-On

In a Web SSO implementation, users are authenticated by a third-party authentication system at the Web-site level. Siebel Business Applications do not provide Web SSO authentication capabilities; they do, however, support this mode of authentication by providing an interface that allows a third-party Web SSO system 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 Business Applications into existing Web sites or portals. Web SSO architecture is appropriate for Web sites on which only approved registered users can gain access to sensitive data, such as a Web site on which you share data with your channel partners.

Web SSO authentication does not apply to the Siebel Mobile Web Client. When connecting to the local database using Siebel Mobile Web Client, mobile users must use local database authentication. For a particular Siebel application, when users connect from the Siebel Developer Web Client to the server database, the authentication mechanism must be the same as that used for Siebel Web Client users. For information about authentication options for local database synchronization for mobile users, see *Siebel Remote and Replication Manager Administration Guide*.

If you are using Oracle's Siebel CRM Desktop applications, then you can implement CRM Desktop Single Sign-On. CRM Desktop SSO allows you to implement Single Sign-On for the CRM Desktop client, and can be customized to support your existing Web Single Sign-On implementation. For information, see *Siebel CRM Desktop for IBM Lotus Notes Administration Guide* and *Siebel CRM Desktop for Microsoft Outlook Administration Guide*.

Web Single Sign-On Limitations

In Web SSO deployments, user authentication and user management are the responsibility of the third-party security infrastructure. As a result, certain capabilities are not available, as Siebel Business Applications features, in a Web SSO environment.

In a Web SSO environment, the following features are not available:

- User self-registration
- Delegated administration of users
- Login forms
- Logout links or the Log Out menu item in the File application-level menu
- Change password feature (in Profile view of User Preferences screen)
- Anonymous browsing

Access to Siebel administration and configuration views is also not available with an Application Object Manager configured for Web SSO authentication.

Verify that functionality you require does not rely on the capabilities in the previous list before you attempt to deploy such functionality in a Web SSO environment. For example, the Siebel eSales - Checkout Process workflow and user registration both make use of login forms.

Your Siebel Business Applications might require configuration changes to hide the capabilities in the previous list. For information on hiding or disabling the capabilities listed, see *Configuring Siebel Business Applications*. For information about logging out of a Web SSO environment, see "Logging Out of a Siebel Application" on page 203.

About Implementing Web Single Sign-On

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

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

In a Web SSO environment, you must provide your authentication service and any required components, such as an authentication client component.

Web Single Sign-On Implementation Considerations

The following are some implementation considerations for a Web SSO strategy:

- Users are authenticated independently of Siebel Business Applications, such as through a third-party authentication service or through the Web server.
- You must synchronize users in the authentication system and users in the Siebel database at the Web site level.
- You must configure user administration functionality, such as self-registration, at the Web site level.
- A delegated administrator can add users to the Siebel database, but not to the authentication system.
- Siebel Business Applications support the following types of Web SSO solutions:
  - Windows Integrated Authentication (WIA) SSO

    To implement Windows Integrated Authentication SSO solutions, the Siebel application and the Siebel Web server must run on Windows operating systems.
  - Standards-based Web SSO solutions that meet the requirements listed in "Requirements for Standards-Based Web Single Sign-On" on page 177.
- Siebel Business Applications do not support Web SSO solutions that are based on Security Assertion Markup Language or that are cookie based.

NOTE: Implement Web SSO in a development environment before deploying it in a production environment.

Web Single Sign-On Options

You can implement the following options in a Web SSO environment that uses a Siebel-compliant security adapter:

- **User specification source.** You must specify the source from which the Siebel Web Engine derives the user's identity key: a Web server environment variable or an HTTP request header variable. For details, see "Configuring the User Specification Source" on page 192.
- **Digital certificate authentication.** Siebel Business Applications support X.509 digital certificate authentication by the Web server. For information on implementing digital certificate authentication for Web SSO, see "About Digital Certificate Authentication" on page 191.
- In addition, many options identified in "Security Adapter Deployment Options" on page 146 can be implemented for Web SSO.

Related Topics

"Requirements for Standards-Based Web Single Sign-On" on page 177

"Requirements for Microsoft Windows Integrated Authentication" on page 179

Web Single Sign-On Authentication Process

The user authentication process in a Web SSO environment is illustrated in Figure 4 on page 177. The steps in the Web SSO authentication process are as follows:

1. A user attempts to access the Siebel client. (A)
2. The SSO authentication service intercepts the user request and determines if the Siebel resource is protected. (B)
   a. If the resource is protected, the SSO authentication service checks for the user's session cookie.
   b. If a valid session does not exist, the user is prompted to enter a username and password.
3. The user enters credentials at the client that are passed to the Web server. (C)
4. The third-party authentication client on the Web server (C) passes the user credentials to the third-party authentication service. (B)
5. The authentication service verifies the user credentials, sets an HTTP header variable that maps to the Siebel user ID, and passes the authenticated user's user name in the header variable to the Siebel Web Server Extension (SWSE) on the Web server. (C)

   NOTE: For LDAP standards-based Web SSO, a header variable must be used.
6. The SWSE passes the authenticated user's user name and the value for the TrustToken parameter to the security adapter. The user name can be the Siebel user ID or another attribute. (E)
7. The security adapter provides the authenticated user's user name to a directory, from which the user's Siebel user ID, a database account, and, optionally, roles are returned to the security adapter. (F)

   In addition, the security adapter compares the TrustToken value provided in the request with the value stored in the Application Object Manager's configuration file (D). If the values match, then the Application Object Manager accepts that the request has come from the SWSE; that is, from a trusted Web server.
8. The Application Object Manager (D) uses the returned credentials to retrieve the user's data based on their roles and visibility. (G)

   If the user is not authorized, the user is denied access and redirected to another URL as determined by the organization's administrator.

Figure 4 on page 177 illustrates the Web SSO authentication process.

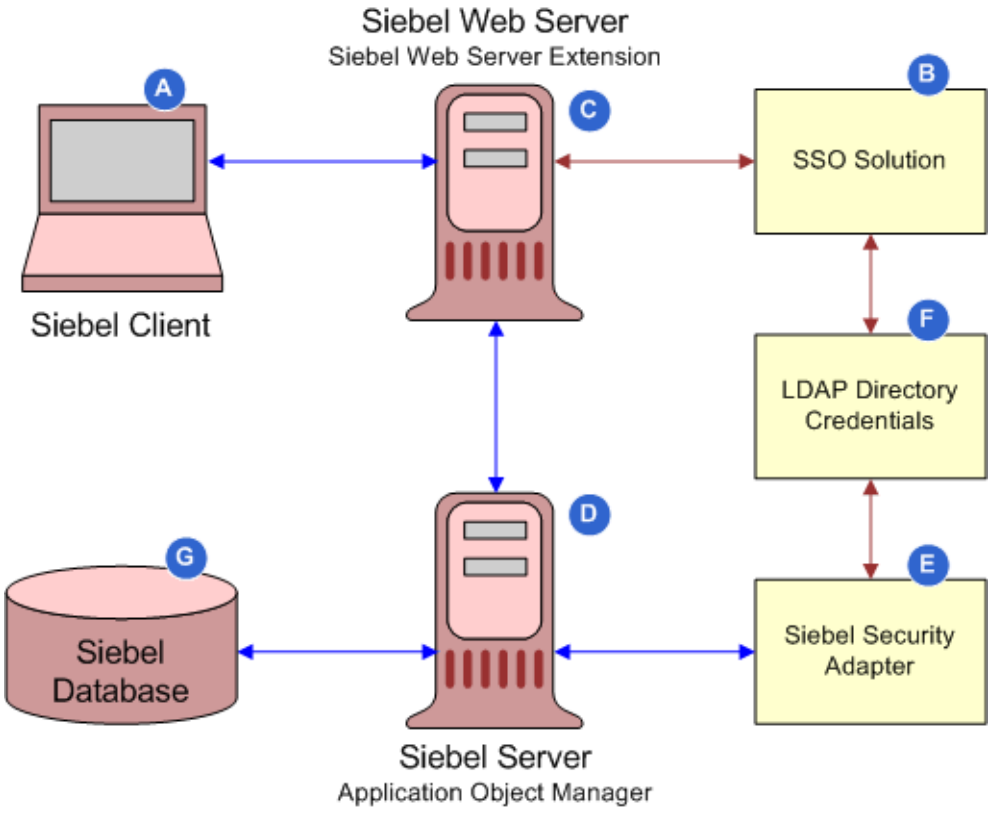

Figure 4. Web Single Sign-On Authentication Process

Related Topic

"About Web Single Sign-On" on page 173

Requirements for Standards-Based Web Single Sign-On

In this guide, the term *standards-based Web SSO* refers to Web SSO systems that support the LDAP standards described in this topic. Standards-based Web SSO is contrasted with Windows Integrated Authentication Web SSO, which uses Microsoft Active Directory or other Windows accounts to identify users. This topic outlines the requirements for integrating Siebel CRM with a standards-based Web SSO system.

To integrate a standards-based Web SSO authentication system with Siebel Business Applications, the following are the minimum requirements that must be met:

- The Web SSO authentication system can send the identity of each Siebel user to be authenticated in an HTTP header variable using HTTP1.1 standard W3C HTTP 1.1 RFC-2616+.

  In a standards-based Web SSO implementation, the SWSE derives the user's user name from the HTTP request header variable. The recommended method is to use a header variable populated with an attribute value that is stored in the directory.
- Siebel Web Single Sign-On is configured for the Siebel Web Server Extension (SWSE).
- The Siebel LDAP security adapter is implemented to provide authentication functionality.
- The Web SSO authentication system uses a static trust token in the HTTP header.
- The Web SSO authentication system supports the following:
  - LDAP 3.0 standard based on compliance with IETF LDAP RFC 2256 and later
  - IEFT Password Policy for LDAP Directories (09)
- In the eapps.cfg file, the fully qualified domain name of the SWSE host and the port number of the SWSE host are specified. For additional information, see *Siebel System Administration Guide*.

Set Up Tasks for Standards-Based Web Single Sign-On

This topic describes the tasks that must be completed for a standards-based Web SSO authentication solution so that it can integrate with Siebel CRM. For detailed information on configuring your authentication service, see the vendor documentation.

To set up the third-party Web SSO authentication service, you must perform the following tasks:

- Install all the components required for the Web SSO authentication service as detailed by the vendor.
- Synchronize the time on all servers hosting the Siebel application and the Web SSO authentication service.
- Configure the authentication service to map an SSO header variable uid to the Siebel uid directory attribute.

  The Header variable set in the Web SSO policy must be equal to the value of the UserSpec parameter in the eapps.cfg file. For information, see "Configuring the User Specification Source" on page 192. In the following example, the uid is mapped to the SSO_SIEBEL_USER HTTP header variable:

  ```
  Type: HeaderVar

  Name: SSO_SIEBEL_USER

  Attribute: uid
  ```
- Grant access to resources that are protected by the policy domain to all Siebel users.
- Remove default no-cache HTTP pragma header fields for your Web SSO solution. No cache should be created by Web SSO.

Requirements for Microsoft Windows Integrated Authentication

This topic outlines the requirements for integrating Siebel CRM with a Microsoft Windows Integrated Authentication (WIA) SSO solution.

To deploy Microsoft Windows Integrated Authentication as your Web SSO solution, the following requirements must be met:

- Make sure that your client and Web server meet one of the following conditions:
  - Are in the same Windows domain.
  - Are in a trusted Windows domain where a user's account can be granted access to resources on the computer hosting Microsoft IIS.

  NOTE: Siebel Business Applications can support Web SSO in a multiple domain Active Directory implementation provided that all Siebel user IDs exist in the Active Directory that the Siebel application connects to, and provided that multiple domain authentication is supported by the Web SSO system. In a multiple domain implementation, each Siebel user who uses Internet Explorer as a Web browser must perform the steps in "Configuring Internet Explorer for Windows Integrated Authentication" on page 179.
- Use a version of Microsoft IIS Web Server that is supported by Siebel Business Applications.
  - For information on supported servers, see the Certifications tab on My Oracle Support.
  - For information on configuring the IIS Web server for Integrated Authentication go to the Microsoft MSDN Web site at

    http://msdn.microsoft.com/
- In the [SWE] section of the eapps.cfg file, set the parameter IntegratedDomainAuth to a value of TRUE, and set the SingleSignOn parameter to TRUE.
- In a Web SSO implementation using Microsoft Windows Integrated Authentication, the SWSE can derive the user's user name from either a Web server environment variable or an HTTP request header variable. For additional information, see "Configuring the User Specification Source" on page 192.

  If you are using header variables to store the user's user name, configure the Web SSO authentication service to map an SSO header variable uid to the Siebel uid directory attribute.
- Siebel users must run Siebel Business Applications on a Microsoft Internet Explorer Web browser.

Configuring Internet Explorer for Windows Integrated Authentication

In a multiple domain implementation of Windows Integrated Authentication, each Siebel user who uses Internet Explorer as a Web browser must perform the steps in the following procedure to suppress authentication challenges when logging into Siebel Business Applications.

To configure Internet Explorer for Windows Integrated Authentication

1. From the Tools menu, select Internet Options, then the Security tab.

2 Select a zone, for example, Trusted sites, then click the Custom level.. button.

3 Navigate to User Authentication, and then Logon.

4 Select the Automatic logon with current user name and password option, then click OK.

Process of Implementing Windows Integrated Authentication

This topic describes the tasks involved in implementing a Windows Integrated Authentication Single Sign-On authentication system.

The process outlined in this topic provides instructions for implementing and testing Web SSO authentication for a single Siebel application, using Microsoft Windows Integrated Authentication as your Web SSO solution. You can repeat the appropriate instructions in this process to provide Web SSO access to additional Siebel Business Applications. For details on the environment setup for the solution outlined in the process, see "Requirements for the Example Windows Integrated Authentication Environment" on page 181.

Perform the following tasks to implement and test Windows Integrated Authentication SSO:

1 Verify that all requirements are met. For information, see:

- "Requirements for Microsoft Windows Integrated Authentication" on page 179
- "Requirements for the Example Windows Integrated Authentication Environment" on page 181.

2 Set up third-party Web SSO authentication.

3 Review "About Creating a Database Login for Externally Authenticated Users" on page 131.

4 "Setting Up Active Directory to Store Siebel User Credentials for Windows Integrated Authentication" on page 181.

5 "Configuring the Microsoft IIS Web Server for Windows Integrated Authentication" on page 182

6 "Creating Users in the Directory (Windows Integrated Authentication)" on page 184.

7 "Adding User Records in the Siebel Database" on page 185.

8 "Setting Web Single Sign-On Authentication Parameters in the SWSE Configuration File" on page 187.

9 Configure authentication parameters, using one of the following methods:

- Edit Siebel Gateway Name Server parameters. See "Setting Web Single Sign-On Authentication Parameters for the Gateway Name Server" on page 188.
- (Developer Web Clients only). Edit the Siebel application's configuration file parameters.

  For Developer Web Clients only, configure authentication parameters in the application configuration file. For additional information, see "Editing Web Single Sign-On Parameters in the Application Configuration File" on page 189.

10 "Restarting Servers" on page 190.

11 "Testing Web Single Sign-On Authentication" on page 190.

Requirements for the Example Windows Integrated Authentication Environment

This topic outlines the requirements for implementing the Web SSO authentication environment described in "Process of Implementing Windows Integrated Authentication" on page 180.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

The following requirements must be met before setting up the example Windows Integrated Authentication environment:

- Microsoft IIS Web Server is deployed on Microsoft Windows. The Microsoft IIS Web Server functions as the authentication service.
- The Active Directory server and the Web server are installed on different computers. The Active Directory functions as a directory of users for the following functions:
  - Authenticates Web server users.
  - Provides the Siebel user ID and the database account for authenticated Web server users.
- The ADSI security adapter communicates between the authentication manager and the Active Directory.
- Siebel Business Applications, including the Siebel Gateway Name Server and the Siebel Server, are installed. The Siebel Server, including affected Application Object Managers, is installed on the Web server computer.

  NOTE: These instructions are for a minimal, baseline configuration. In a production environment, it is not recommended to install the Siebel Server on the same computer as the Web server.
- If you use a non-Siebel security adapter, it must support the Siebel Security Adapter Software Developers Kit, described in "Security Adapter SDK" on page 23. You must adapt the applicable parts of the implementation to your security adapter.
- You are experienced with administering Active Directory and can perform tasks such as creating and modifying user storage subdirectories, creating attributes, and creating and providing privileges to users.

Setting Up Active Directory to Store Siebel User Credentials for Windows Integrated Authentication

This topic describes how to set up Active Directory for Windows Integrated Authentication. In this example, the Active Directory performs two functions that might be handled by two separate entities in other Web SSO implementations:

- Users are authenticated through the Active Directory performing its function as the Microsoft IIS Web Server directory.
- The Active Directory functions as the directory from which an authenticated user's Siebel user ID and database account are retrieved.

This topic describes how to configure the Active Directory as the directory which provides the user IDs and the Siebel database account for authenticated users. For information about configuring the Microsoft IIS Web Server, see "Configuring the Microsoft IIS Web Server for Windows Integrated Authentication" on page 182.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

To set up Active Directory to store Siebel user credentials

1. Select a subdirectory in the Active Directory to store users, for example, the Users subdirectory under the domain-level directory.

   You cannot distribute the users of a single Siebel application in more than one subdirectory. However, you can store multiple Siebel Business Applications' users in one subdirectory.

2. Define the attributes to use for the following user data (create new attributes if you do not want to use existing attributes):

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

3. **Password.** Assign a user password to each user using the ADSI user management tools. The user password is not stored as an attribute.

   NOTE: A user password is required for the Active Directory for its role as the Microsoft IIS Web Server directory, which is the authentication service in this configuration. A user password attribute is not required for Active Directory 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.

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

Configuring the Microsoft IIS Web Server for Windows Integrated Authentication

This topic describes the configuration tasks you must perform on the IIS Web Server for Windows Integrated Authentication.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Configuring the IIS Web Server to Authenticate against Active Directory

Configure the Microsoft IIS Web Server to authenticate against the Active Directory. Select the type of authentication that is most appropriate for your deployment.

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.

Configuring Authentication for Siebel Virtual Directories

During configuration of the Siebel Web Server Extension, Siebel virtual directories are created on the IIS Web server for the installed Siebel Business Applications. For example, the virtual directory eservice_enu is for Siebel eService using U.S. English (ENU). You must set the authentication mode for these virtual directories to Windows Authentication or Integrated Windows Authentication, depending on the version of IIS Web Server that you are using.

For information about configuring authentication modes for the Microsoft IIS Web Server, go to the Microsoft MSDN Web site at

http://msdn.microsoft.com

(Optional) Creating Protected Virtual Directories

This topic describes how to create virtual directories in a Web SSO implementation. Creating virtual directories allows users to access a Siebel application and anonymously browse specific views while requiring Web SSO authentication to access other views in the application.

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

Perform the steps in the following procedure to create a custom protected virtual directory, and to enable Windows Authentication for the virtual directory.

To create a protected virtual directory

1. Make a copy of the appropriate eapps_virdirs batch file provided in the SWSE logical profile directory.

   The eapps_virdirs batch files are used to create Siebel virtual directories. For additional information, see *Siebel Installation Guide* for the operating system you are using.

2. Edit the copied eapps_virdirs file to specify the name and other details of the virtual directory you want to create for the Siebel application.

   For example, enter p_eservice as a virtual directory name for Siebel eService.

3. Run the eapps_virdirs batch file, and a Siebel virtual directory with the name you specified is created.

   It is recommended that you save the edited eapps_virdirs file so that it can be used if you need to restore or migrate your virtual directory environments.

4. Set the Authentication setting for the virtual directory you created to Windows Authentication as follows:

   a. In the Internet Service Manager explorer, right-click the virtual directory you created in the previous steps, then choose Properties.

      The Properties dialog box appears.

b Click the Directory Security tab.

c Click Edit in the Anonymous Access and Authentication Control section.

d The Authentication Methods dialog box appears.

e Check the Integrated Windows Authentication check box, and uncheck all others. Make sure that the Allow Anonymous Access box is unchecked.

NOTE: On some versions of the IIS Web Server, an Integrated Authentication check box is not displayed. In this case, make sure that the Allow Anonymous Access box is unchecked and enable Windows Authentication.

f 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.

g Click Apply, and then click OK.

Creating Users in the Directory (Windows Integrated Authentication)

To implement Web SSO using Windows Integrated Authentication, you must create users in the Active Directory, as described in this topic.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Create three users in the Active Directory, using values similar to those shown in Table 17 on page 185. The attribute names, sAMAccountName and Password, are suggestions; your entries might vary depending on how you make attribute assignments in "Setting Up Active Directory to Store Siebel User Credentials for Windows Integrated Authentication" on page 181. Complete other attribute fields for each user, as needed.

Table 17. Active 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 383, for a Siebel customer or partner application. For example, for Siebel eService, enter GUESTCST. ■ You can create a new user record or adapt a seed anonymous user record for a Siebel employee application.	GUESTPW or a password of your choice.	username=LDAPUSER password=*P*.
Application user	APPUSER or a name of your choice.	APPUSERPW or a password of your choice.	A database account is not used for the application user.
A test user	TESTUSER or a name of your choice.	TESTPW or a password of your choice.	username=LDAPUSER password=*P*.

The database account for all users is the same, and must match the database account reserved for externally-authenticated users described in "Setting Up Active Directory to Store Siebel User Credentials for Windows Integrated Authentication" on page 181. *P* represents the password in that database account. For information about formatting the database account attribute entry, see "Requirements for the LDAP Directory or Active Directory" on page 111.

NOTE: Make sure the application user has privileges to search and write to all records in the directory.

Adding User Records in the Siebel Database

This topic describes how to create a record in the Siebel database that corresponds to the test user you created in "Creating Users in the Directory (Windows Integrated Authentication)" on page 184.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

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, then see the instructions for adding such users in "Internal Administration of Users" on page 241.

To add user records to the database

1. Log in as an administrator to a Siebel employee application, such as Siebel Call Center.
2. Navigate to the Administration - User screen, then the Users view.
3. In the Users list, create a new record.
4. Complete the following fields for the test user, then save the record. Use the indicated guidelines. Suggested entries are for this example. You can complete other fields, but they are not required.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID For example, 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, then 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, then 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. 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, then create it using the field values in Table 47 on page 384. You can complete other fields, but they are not required.

   This record must also match the anonymous user you create in "Creating Users in the Directory (Windows Integrated Authentication)" on page 184. You can adapt a seed data anonymous user or create a new anonymous user for a Siebel employee application.

Setting Web Single Sign-On Authentication Parameters in the SWSE Configuration File

To implement Web Single Sign-On authentication, you must specify values for parameters in the SWSE configuration file, eapps.cfg, as indicted in this topic.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Provide parameter values in the eapps.cfg file, as indicated by the guidelines in Table 18. For information about editing eapps.cfg parameters and about the purposes of the parameters, see "About Parameters in the eapps.cfg File" on page 353.

Table 18. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
[defaults]	Various	The values of the parameters in this section are overridden by the parameter values you set in the sections for individual applications. For this scenario, set Web SSO and related parameters in application-specific sections.
The section particular to your application, such as one of these: [/eservice_enu] [/callcenter_enu] where _enu is the language code for U.S. English.	AnonUserName	Enter the user ID of the seed data user record provided for the application that you implement or of the user record you create for the anonymous user. This entry also matches the sAMAccountName entry for the anonymous user record in the directory. For example, enter GUESTCST for Siebel eService.
	AnonPassword	Enter the password you created in the directory for the anonymous user. **NOTE:** Typically, password encryption applies to the eapps.cfg file. In this case, you must specify the encrypted password. See "Encrypted Passwords in the eapps.cfg File" on page 46.
	SingleSignOn	Enter TRUE to implement Web SSO.
	TrustToken	Enter HELLO, or a contiguous string of your choice. In Web SSO mode when used with a custom security adapter, the specified value is passed as the password parameter to a custom security adapter if the value corresponds to the value of the Trust Token parameter defined for the custom security adapter. **NOTE:** Typically, password encryption applies to the eapps.cfg file. In this case, you must specify the encrypted value. See "Encrypted Passwords in the eapps.cfg File" on page 46.

Table 18. Parameter Values in eapps.cfg File

Section	Parameter	Guideline
	UserSpec	Example entry: REMOTE_USER REMOTE_USER is the default Web server variable in which the user's identity key is placed for retrieval by the authentication manager. For additional information, see "Configuring the User Specification Source" on page 192.
	UserSpecSource	Example entry: Server
	ProtectedVirtual Directory	If you created a protected virtual directory, as described in "(Optional) Creating Protected Virtual Directories" on page 183, enter the name of the directory. Alternatively, if anonymous browsing is not implemented, you can enter the name of the existing virtual directory created for your Siebel application. **NOTE:** It is recommended that this parameter is always used in a Web SSO implementation.
[swe]	Integrated DomainAuth	Set to TRUE for Windows Integrated Authentication. This parameter is set to FALSE by default.

Setting Web Single Sign-On Authentication Parameters for the Gateway Name Server

To implement Web SSO authentication, you must specify values for the Gateway Name Server parameters listed in this topic.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Set each Siebel Gateway Name Server parameter listed in Table 19 on page 188 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 additional information about Siebel Gateway Name Server parameters, see "Siebel Gateway Name Server Parameters" on page 361.

Table 19. Siebel Gateway Name Server Parameters

Subsystem	Parameter	Guideline
InfraUIFramework	AllowAnonUsers	Enter TRUE.
	SecureLogin	Enter TRUE or FALSE. If TRUE, the login form completed by the user is transmitted over TLS. For information about other requirements for secure login, see "Login Security Features" on page 202.

Table 19. Siebel Gateway Name Server Parameters

Subsystem	Parameter	Guideline
Object Manager	OM - Proxy Employee	Enter PROXYE.
	OM - Username BC Field	Leave empty.
Security Manager	Security Adapter Mode	The mode for the security adapter. Values are DB, LDAP, ADSI, or CUSTOM. This parameter is set at the Enterprise, Siebel Server, or component level. For information, see Chapter 5, "Security Adapter Authentication."
	Security Adapter Name	The name of the security adapter. The default names are: ■ DBSecAdpt ■ LDAPSecAdpt ■ ADSISecAdpt This parameter is set at the Enterprise, Siebel Server, or component level. For more information, see Chapter 5, "Security Adapter Authentication."
The enterprise profile or named subsystem for the security adapter you are using. For example: ■ LDAPSecAdpt (LDAP security adapter) ■ ADSISecAdpt (ADSI security adapter)	SingleSignOn	Enter TRUE to indicate the security adapter is used in Web SSO mode.
	TrustToken	Enter a contiguous string of your choice, for example, HELLO. The value you enter must be the same as the value you specify for the TrustToken parameter in the eapps.cfg file (see Table 18 on page 187).
	For more information about configuring parameters for each security adapter, see Chapter 5, "Security Adapter Authentication." See also Appendix A, "Configuration Parameters Related to Authentication."	

Editing Web Single Sign-On Parameters in the Application Configuration File

If you are implementing Web SSO authentication for the Developer Web Client, then you must specify the parameter shown in Table 20 in the configuration file for the Siebel application you are implementing. For information about editing an application's configuration file, see "Siebel Application Configuration File Parameters" on page 376.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Table 20. Siebel Application Configuration File Parameter Values

Section	Parameter	Guidelines for ADSI Security Adapter
[InfraUIFramework]	AllowAnonUsers	Enter TRUE.

The AllowAnonUsers parameter in the InfraUIFramework section of the application configuration file applies to Developer Web Clients only. The corresponding Application Object Manager parameter, which applies to Web Clients, is set using Siebel Server Manager and is listed in Table 19 on page 188.

Restarting Servers

You must stop and restart Windows services on the Web server computer to activate the changes you make to the Application Object Manager configuration parameters when implementing Web SSO.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Stop and restart the following services:

- **Microsoft IIS Admin service and Worldwide Web Publishing service.** Stop the Microsoft IIS Admin service, and then restart the Worldwide Web Publishing Service. The Microsoft IIS Admin service also starts because the Worldwide Web Publishing Service is a subservice of the Microsoft IIS Admin service.
- **Siebel Server system service.** Stop and restart the Siebel Server. For details, see *Siebel System Administration Guide*.

Testing Web Single Sign-On Authentication

After performing all the tasks required to implement Web SSO authentication, you can verify your implementation using the procedure in this topic.

This task is a step in "Process of Implementing Windows Integrated Authentication" on page 180.

Perform the following procedure to confirm that the Web SSO components work together to:

- Allow a user to log into the Web site.
- Allow a user who is authenticated at the Web site level to gain access to 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.example.com
```

If the authentication system has been configured correctly, then a Web page with a login form for the Web site appears.

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.

If the authentication system has been configured correctly, then you gain access to the Web site.

3 On a Web browser, enter the URL to your Siebel application, for example:

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

Alternatively, if you provide a link on the Web site, click it.

If the authentication system has been configured correctly, then you gain access to the Siebel application as a registered user without having to log in.

About Digital Certificate Authentication

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

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

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

For customers who have an existing PKI (Public Key Infrastructure) with client certificates, Siebel Business Applications support the use of X.509 certificates to authenticate the users of an application. This authentication is accomplished using TLS 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 "Set Up Tasks for Standards-Based Web Single Sign-On" on page 178, with the following specific guidelines:

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

Parameter	Value	Comment
SingleSignOn	TRUE	None
TrustToken	HELLO	None
ClientCertificate	TRUE	None
UserSpec	CERT_SUBJECT or REMOTE_USER	For client authentication on Windows and AIX, use CERT_SUBJECT. For other UNIX operating systems, use REMOTE_USER.
SubUserSpec	CN	This parameter value tells the application to extract the user name from the certificate name. For the Oracle iPlanet Web Server (formerly known as the Sun Java System Web Server), this setting is ignored.
UserSpecSource	Server	None

- Set the SecureBrowse parameter to True for the Application Object Manager component for which Digital Certificate Authentication is implemented, such as Call Center Object Manager.
- For each security adapter (such as LDAPSecAdpt) that is to support certificate-based authentication, define the following parameter values:

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

Configuring the User Specification Source

The User Specification Source option can be implemented in a Web SSO authentication strategy. In a Web SSO implementation, the SWSE derives the user's user name from either a Web server environment variable or an HTTP request header variable. You must specify one source or the other.

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

The following procedure describes how to specify the source of a user name: either a Web server environment variable or an HTTP request header variable.

To specify the source of the user name

- 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, then the value of UserSpec is the variable that is passed into the HTTP header; the name of the variable must not be prefaced with HTTP_.
  - UserSpecSource = Server, if you use a Web server environment variable.
  - UserSpecSource = Header, if you use an HTTP request header variable.

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

  For information about setting parameters in the eapps.cfg file, see "About Parameters in the eapps.cfg File" on page 353.

Configuring the Session Timeout

You can configure an expiration period for a Siebel session by setting a session timeout value in both Siebel Business Applications and many Web SSO authentication service providers. The timeout values must be the same for both applications. If you configure a timeout value for your Siebel application that is shorter than the one you configure for your Web SSO authentication service, users can re-establish their Siebel session after it times out without providing login credentials.

The procedures in this topic describe how to configure the session timeout. To make sure that users must re-authenticate after the timeout limit is reached, you must also configure the same timeout value for your Web SSO authentication service. For information on the Siebel SessionTimeout parameter, see "About the SessionTimeout Parameter" on page 359.

Configuring the Session Timeout

To configure the session timeout for your Siebel application and for the Web SSO authentication service, perform the steps in the following procedure.

To configure the session timeout

1. To configure the session timeout for the Siebel application:
   a. Navigate to the eapps.cfg file located in the *SWSE_ROOT*\BIN directory.
   b. Set the value of the SessionTimeout parameter as required.
   c. Restart the Siebel Web server.
2. To configure the session timeout for the Web SSO authentication service, follow your Web SSO vendor's procedure for setting session timeout values. Specify the following values:

a Change the value of the Maximum user session time (seconds) field.

Set this value to be just longer than the session timeout value you specified for the Siebel application.

b Change the value of the Idle session time (seconds) field.

Set this value to be the same as the value you set for the Siebel application.

Testing the Web Single Sign-On Session Timeout Configuration

After configuring the session timeout values for your Siebel application and Web SSO authentication service, verify that the session timeout values work correctly by performing the steps in the following procedure.

To test the Web SSO session timeout configuration

1 Configure the Web SSO session timeout to be five minutes and restart the Web servers.

2 Open a Web browser and access the Web server's main page (http://*hostname*).

The main page is displayed; user authentication should not be required.

3 Access the Siebel URL for the Web server from the same browser used in Step 2 on page 194.

Basic authentication should be required.

4 Enter valid Siebel user credentials.

The Siebel application should be displayed.

5 Leave the browser window open and idle for more than five minutes.

6 Refresh the browser window using the Refresh button.

You should be prompted to enter user credentials.

7 Enter valid Siebel user credentials.

The Siebel application should be displayed.

8 Repeat Step 2 on page 194 to Step 5 on page 194 for the Web server you have implemented.

Configuring Siebel CRM and Oracle BI Publisher for Web Single Sign-On

This topic describes the configuration tasks you must perform to configure Siebel CRM and Oracle Business Intelligence Publisher (Oracle BI Publisher) in a Web Single Sign-On environment. Oracle BI Publisher is the reporting module for Siebel CRM. Siebel Reports integrates with Oracle BI Publisher to run and administer reports.

For information on configuring Siebel CRM and Oracle BI Publisher for Web Single Sign-On authentication, see the following topics:

- "Configuring Siebel CRM for Integration with Oracle BI Publisher with Web Single Sign-On" on page 195
- "Configuring Oracle BI Publisher for Integration with Siebel CRM with Web Single Sign-On" on page 197
- "Enabling Reports Scheduling with Web Single Sign-On" on page 197

Configuring Siebel CRM for Integration with Oracle BI Publisher with Web Single Sign-On

This topic describes the configuration tasks you must perform for your Siebel application so that it can integrate with Oracle BI Publisher when Web Single Sign-On authentication is implemented.

To configure Siebel CRM for BI Publisher integration in a Web SSO environment

1 For the Security Adapter Profile (either the LDAP Security Adapter profile or the ADSI Security Adapter profile) that is used for authentication and Web SSO, specify parameter values similar to those shown in the following table.

Parameter Name	Value
Single Sign On	True
Trust Token	*password* This is the value of the TrustToken parameter (in encrypted format) this is specified in the eapps.cfg file.

2 For the server components listed in the following table, specify values for the parameters shown. Specify values either for the LDAP or for the ADSI security adapter, depending upon the security adapter you have implemented.

Server Component	Parameter	Value
Application Object Manager and EAI Object Manager	Security Adapter Name	Either LDAPSecAdpt or ADSISecAdpt
	Security Adapter Mode	LDAP or ADSI
	Username	*LDAP_USER_ID* or *AD_USER_ID*
	Password	*password* The password associated with the *LDAP_USER_ID* or *AD_USER_ID*
XMLP Report Server	Security Adapter Name	LDAPSecAdpt or ADSISecAdpt
	Security Adapter Mode	LDAP or ADSI
	Username	*LDAP_USER_ID* or *AD_USER_ID*
	Password	*password* This is the value of the TrustToken parameter (in encrypted format) specified in the eapps.cfg file.

NOTE: The *LDAP_USER_ID* or *AD_USER_ID* values you specify must be an LDAP or Active Directory user who has a Siebel employee record, for example, AnonUserName, in the eapps.cfg file.

3 Enable Single Sign-On for the EAI Object Manager by adding the parameters in the following table to the [/eai_*lang*] section of the eapps.cfg file.

Parameter	Value
SingleSignOn	True
TrustToken	*TrustToken_Value*
UserSpec	*HTTP Header Variable*
UserSpecSource	Header

4 Restart the Siebel Server, Siebel Gateway Name Server, and the Siebel Web Server services.

5 When the services are started, verify that the Application Object Manager, EAI Object Manager, and XMLP Report Server components are online.

   If any of these services are unavailable, create a service request (SR) on My Oracle Support. Alternatively, you can phone Oracle Global Customer Support directly to create a service request or get a status update on your current SR. Support phone numbers are listed on My Oracle Support.

Configuring Oracle BI Publisher for Integration with Siebel CRM with Web Single Sign-On

This topic describes how to configure Oracle BI Publisher to integrate with Siebel CRM when Web Single Sign-On authentication is implemented.

To configure Oracle BI Publisher for Siebel CRM integration in a Web SSO environment

1 Log into the Oracle BI Publisher Server with administrator credentials.

2 Click the Admin tab, then select Security Configuration in the Security Center section.

3 Change the value of the Administrator Password parameter for the Siebel Security Model to specify the value of the Trust Token (in clear text) specified for Web SSO in the eapps.cfg file.

4 Restart the Oracle BI Publisher OC4J instance.

   NOTE: After the Administrator Password parameter is set to specify the value of the Trust Token, any Siebel user who wants to log into the Oracle BI Publisher Server must enter the Trust Token value as the password.

Enabling Reports Scheduling with Web Single Sign-On

This topic describes how to enable Siebel Reports scheduling when Web Single Sign-On authentication is implemented for Siebel CRM and when the Siebel Security Model is implemented for Siebel Reports.

Oracle BI Publisher issues an inbound Web service call (BIPDataService) to retrieve data from the Siebel application when reports are scheduled and executed. During this process, report users are authenticated against the EAI Application Object Manager. You must, therefore, use a non-SSO security adapter for reports scheduling.

To enable Siebel Reports scheduling when Web SSO is implemented

1 Create a new custom Siebel Server component based on the EAI Object Manager component, and name the new component BIP EAI Object Manager.

   For information about creating custom Siebel Server component definitions, see *Siebel System Administration Guide*.

2 Create a new Siebel enterprise profile (named subsystem) by copying the security adapter profile used by the Application Object Manager.

- If the Siebel application is using the LDAPSecAdpt security adapter profile, create a copy of the profile and name it LDAPSecAdpt_NoSSO.
- If the Siebel application is using the ADSISecAdpt security adapter profile, create a copy of the profile and name it ADSISecAdpt_NoSSO.

For information about creating Siebel Enterprise Server named subsystems, see *Siebel System Administration Guide*.

3 Set the Single Sign On profile parameter for the new security adapter profile you created in Step 2 on page 198 to False.

4 For the BIP EAI Object Manager component you created in Step 1 on page 197, specify values for the parameters shown in the following table.

Parameter	Value (LDAP Authentication)	Value (AD Authentication)
Security Adapter Name	LDAPSecAdpt_NoSSO	ADSISecAdpt_NoSSO
Security Adapter Mode	LDAP	ADSI

5 Synchronize the new component definitions, then restart the Siebel Server and the Siebel Gateway Name Server services.

For information about synchronizing components on a Siebel Enterprise Server, see *Siebel System Administration Guide*.

6 Create a new virtual directory in the Siebel Web server and name it bipeai_*lang*.

Refer to the Siebel Web server product documentation for information on creating a virtual directory and making it accessible. Configure the new virtual directory in exactly the same way as the existing eai_*lang* virtual directory.

7 Edit the eapps.cfg file to add a section for the [/bipeai_*lang*] virtual directory, and add parameters similar to the following:

```
[/bipeai_lang]
ConnectString = ConnectString
EnableExtServiceOnly = TRUE
WebPublicRootDir = SWSE_Installation_Directory\PUBLIC\language
SiebEntSecToken = security_token
```

NOTE: Do not add Web SSO-related parameters to this section.

For additional information, see "About Parameters in the eapps.cfg File" on page 353.

8 Restart the Siebel Web server service for the changes to take effect.

9 Launch the Siebel Web Client and log into the Siebel application as a Siebel administrator.

10 Navigate to the Administration - Web Services screen, then the Inbound Web Services view.

11 In the Name field of the Inbound Web Services list, query for BIPDataService.

12 In the address URL for the BIPDataService, change the value eai_*lang* to bipeai_*lang*. For example:

```
http://SiebelWebServerName/bipeai_lang/
start.swe?SWEExtSource=WebService&SWEExtCmd=Execute&WSSOAP=1
```

13 Click the Generate WSDL button to generate a WSDL file, then save the file with the name dataservice.wsdl.

14 Copy the dataservice.wsdl file to the Oracle BI Publisher home directory. By default, this is the `OraHome_X\oc4j_bi\bin` directory on the Oracle BI Publisher server.

15 Restart the Oracle BI Publisher OC4J instance.

7 Security Features of Siebel Web Server Extension

This chapter describes several options that relate to security issues and the Siebel Web Server Extension (SWSE). It includes the following topics:

- Configuring a Siebel Web Client to Use HTTPS on page 201
- Login Security Features on page 202
- About Using Cookies with Siebel Business Applications on page 206

Configuring a Siebel Web Client to Use HTTPS

You can configure Siebel Business Applications to specify whether or not URLs must use TLS over HTTP (HTTPS protocol) to access views in a Siebel application. You can specify that HTTPS must be used to access specific views, to access all views, or is not required to access views.

If you use the HTTPS protocol, then be aware of the following issues:

- You can switch between secure and nonsecure views in Siebel customer applications, but not in employee applications (such as Siebel Call Center). For employee applications, if any views are to be secure, then all views must be secure.
- Your Web server must be configured to support HTTPS.

  You must install a certificate file on the Web server with which you want to secure communication. For more information, see "About Certificates and Key Files Used for SSL or TLS Authentication" on page 57.

Two factors determine whether or not the Siebel Web Engine verifies that requests for a view use the HTTPS protocol:

- The value (True or False) of the view's Secure attribute

  You can set the Secure property of a specific view to indicate whether or not the HTTPS protocol must be used to access the view. The ability to selectively secure individual views applies to standard-interactivity applications. For information about specifying the Secure attribute for an individual view, see *Configuring Siebel Business Applications*.
- The value (True or False) of the SecureBrowse component parameter

  You can specify a value for the SecureBrowse parameter to indicate whether or not the HTTPS protocol must be used to access all the views in an application.

The following procedure describes how to configure your application to use HTTPS or HTTP for all views in an application.

To configure your application to use HTTPS or HTTP for all views

- Using Siebel Server Manager, specify one of the following values for the SecureBrowse component parameter:
  - **SecureBrowse is set to TRUE.** If SecureBrowse is set to TRUE, then HTTPS is required for all views in the application, regardless of how the Secure attribute is set for individual views.
  - **SecureBrowse is set to FALSE.** If SecureBrowse is set to FALSE, then HTTP is required for all views in the application, except for views for which the Secure attribute is set to TRUE. Secure views require HTTPS.

  NOTE: In previous releases of Siebel Business Applications, values for the SecureLogin and SecureBrowse parameters for Siebel Web Clients were specified in the Siebel application configuration file. Since Siebel version 8.0, SecureLogin and SecureBrowse are Application Object Manager (AOM) parameters which are set using Siebel Server Manager. For information on setting parameters using Siebel Server Manager, see *Siebel System Administration Guide*.

You can also specify that user credentials entered at login must be transmitted from the Web client to the Web server using the HTTPS protocol by setting values for the SecureLogin parameter. For information on this parameter, see "Implementing Secure Login" on page 203.

Login Security Features

This topic describes features and considerations associated with the user login process for Siebel Business Applications. A login page or a login form embedded in a Siebel application page collects user credentials.

NOTE: You cannot log into a Siebel application by presenting user credentials as parameters in a URL.

A user must log in, thereby identifying himself or herself as a registered user, to access protected views in Siebel Business Applications. Protected views are designated for explicit login. Views that are not designated for explicit login are available for anonymous browsing, if the Siebel application allows anonymous browsing. For information about anonymous browsing, see "Configuring the Anonymous User" on page 155.

Siebel Business Applications also provide other features on a login form besides user credentials collection, such as remembering a username and providing forgotten password support. For information on these features, see the following topics:

- "Implementing Secure Login" on page 203
- "Logging Out of a Siebel Application" on page 203
- "Login User Names and Passwords" on page 204
- "Account Policies and Password Expiration" on page 205

Implementing Secure Login

This topic describes how to implement secure login. With secure login, the Siebel Web Engine transmits user credentials entered in a login form from the browser to the Web server using TLS, that is, over HTTPS.

Secure login can be implemented in the following authentication strategies:

- Security adapter authentication: database authentication
- Security adapter authentication: Lightweight Directory Access Protocol (LDAP), Active Directory Service Interfaces (ADSI), or custom
- Web SSO authentication

For each Siebel application where you want to implement secure login, you set the value of the SecureLogin component parameter to TRUE. The following procedure demonstrates how to set this parameter for the Siebel Call Center application. To implement secure login, you must also have a certificate from a certificate authority on the Web server where you installed SWSE.

To implement secure login

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. Select the Siebel Server of interest.
3. Click the Components view and select the component of interest. For example, select Call Center Object Manager (ENU) in a U.S. English deployment if you want to set secure login for the Siebel Call Center application.
4. Click the Parameters view and select the record for SecureLogin.
5. In the Value on Restart field, enter TRUE.
6. Restart the component to apply the change.

   For information about administering Siebel Server components, see *Siebel System Administration Guide*.

Related Topic

"Login Security Features" on page 202

Logging Out of a Siebel Application

Siebel application users can end a Siebel session by using the Siebel application log out features or by closing the browser window.

If you select the Siebel application Log Out menu option, you are logged out of the Siebel application and the user session is ended immediately. Alternatively, you can close the browser window to end the Siebel session. The effect of closing the browser window differs depending on the mode in which your Siebel application runs:

- If you are using Siebel Business Applications with a Siebel Open UI client or with a standard-interactivity client, clicking the X box in the top-right corner of the application window closes the window but does not terminate the Siebel user session until the session timeout is reached.

  The value of the session timeout is determined by the SessionTimeout parameter in the eapps.cfg file on the SWSE. For more information about this parameter, see "About Parameters in the eapps.cfg File" on page 353.

- If you are using Siebel Business Applications with a high-interactivity client, closing the browser window by clicking the X box in the top-right corner of the application window causes the Siebel user to be logged out of the Siebel application and ends the user session.

Related Topic

"Login Security Features" on page 202

Login User Names and Passwords

Siebel Business Applications provide two features on the Siebel login dialog box to assist users. These features are:

- The Remember My User ID check box
- The Forgot Your Password? link

  For information on retrieving forgotten passwords, see "Retrieving a Forgotten Password (Users)" on page 233.

Remember My User ID

A user can check the Remember My User ID check box when logging into a Siebel application. By doing so, whenever the user logs in to the same Siebel application in the future, the Username field is prefilled with the user's user name; the user simply has to enter the associated password to access the Siebel application.

The Remember My User ID functionality can be used by the same user on a number of different Siebel Business Applications simultaneously, provided the user checks the Remember My User ID check box when logging in to each application. This is particularly useful to users, for example, system administrators, who regularly log in to a number of different Siebel application environments.

Remember My User ID uses the auto-login credential cookie that the Siebel Web Engine provides when a session is started. This functionality requires that cookies be enabled. For information about the auto-login credential cookie, see "Auto-Login Credential Cookie" on page 210.

Related Topic

"Login Security Features" on page 202

Account Policies and Password Expiration

For enhanced security, you might want to implement the following account policies. Account policies are functions of your authentication service. If you want to implement account policies, then you are responsible for setting them up through administration features provided by the authentication service vendor.

- Password syntax rules, such as minimum password length.

  When creating or changing passwords, minimum length requirements and other syntax rules defined in the external directory are enforced by the Siebel application.

- An account lockout after a specified number of failed attempts to log in.

  Account lockout protects against password guessing attacks. Siebel Business Applications support lockout conditions for accounts that have been disabled by the external directory.

- Password expiration after a specified period of time.

  The external directory can be configured to expire passwords and warn users that passwords are about to expire. Password expiration warnings issued by the external directory are recognized by Siebel Business Applications and users are notified to change their passwords.

About Password Expiration

Password expiration can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, ADSI, or applicable custom security adapter
- Database authentication where supported by the RDBMS

If you are using an LDAP or ADSI security adapter, then password expiration is handled by the external LDAP directory or Active Directory, and is subject to the configuration of this behavior for the third-party directory product.

For example, when a password is about to expire, the directory might provide warning messages to the Siebel application to display when the user logs in. Such a warning would indicate the user's password is about to expire and must be changed. If the user ignores such warnings and allows the password to expire, then the user might be required to change the password before logging into the application. Or, the user might be locked out of the application once the password has expired.

Password expiration configuration steps for each directory vendor will vary. For more information, see the documentation provided with your directory product. More information about password expiration for use with Active Directory is provided below.

Password Expiration on Active Directory

On Active Directory, factors that affect the password state include the following attributes and parameters:

- Password Never Expires (attribute for user object)
- User Must Change Password At Next Logon (attribute for user object)
- Last Time User Set Password (attribute for user object)

- Maximum Password Age (attribute for domain)
- Password Expire Warn Days (parameter for ADSI security adapter)

When you configure password expiration for Active Directory, you add the parameter Password Expire Warn Days (alias PasswordExpireWarnDays) to the ADSI security adapter. Set the value to the number of days you want to provide a warning message before a user's password expires.

NOTE: The attributes Password Never Expires and User Must Change Password at Next Logon are mutually exclusive, and cannot both be checked for a user.

The state of each user's password is determined by the following logic:

- If Password Never Expires is checked for a user, then this user never gets a password expired error, regardless of the settings of other attributes.
- If User Must Change Password At Next Logon is checked for a user, then this user gets a password expired error, regardless of the settings of other attributes.
- If neither of the above attributes are checked for a user, then the following behavior applies:
  - If Maximum Password Age is set to 0 for the domain, then a user will not get a password-expired error. No password will expire in the domain.
  - If a value is specified for Maximum Password Age, then the following behavior applies:
    - If the difference between the current time and the last time a user has set the password (the value of the Last Time User Set Password attribute for the user) is larger than the value of Maximum Password Age, then this user gets a password-expired error.
    - If the difference between current time and the last time a user has set the password is smaller than Password Expire Warn Days (set for the ADSI security adapter), then this user gets a password-expiring warning message.
    - If the difference between current time and the last time a user has set the password is smaller than Maximum Password Age, and larger than Password Expire Warn Days, then this user will log in successfully and will not get any error or warning message.

NOTE: Confirm all third-party directory product behavior and configuration with your third-party documentation.

About Using Cookies with Siebel Business Applications

Siebel Business Applications running in the Web browser can use cookies for a variety of purposes. This topic describes the types of cookies used and provides instructions for enabling cookies for Siebel Business Applications.

Unless otherwise noted, all of the cookies used by Siebel Business Applications apply to both high interactivity and standard interactivity applications and to Siebel Open UI. All cookies used by Siebel Business Applications are encrypted using standard encryption algorithms provided by RSA. Siebel Business Applications use the following kinds of cookies:

- **Session cookie.** Manages user sessions for Siebel Web Client users. For details, see "Session Cookie" on page 207.

- **Auto-login credential cookie.** Stores user credentials for Siebel Web Client users. For details, see "Auto-Login Credential Cookie" on page 210.
- **Siebel QuickStart cookie.** Used by the Mobile Web Client when Siebel QuickStart is used. For details, see "Siebel QuickStart Cookie" on page 211.

Session Cookie

The session cookie consists of the session ID generated for a user's session. This cookie is used to manage the state of the user's session. The session cookie applies to the Siebel Web Client only.

Cookie modes are determined on the Siebel Web Server Extension (SWSE) by the setting of the SessionTracking parameter in the eapps.cfg file. For information about setting parameters in the eapps.cfg file, see Appendix A, "Configuration Parameters Related to Authentication."

The SessionTracking parameter settings are:

- Automatic

  Using the default SessionTracking setting of Automatic, the SWSE runs in cookie-based mode and session information is maintained through cookies. However, if a browser does not support cookies or if a user's browser is configured to not allow cookies, then the SWSE will function in cookieless mode and use URLs instead. A cookieless session is invoked when the browser does not send back a session cookie to the SWSE.

- Cookie

  To force the SWSE to always use cookie-based mode, set the following parameters in the eapps.cfg file to the values shown:

  ```
  SessionTracking = Cookie
  URLSession = FALSE
  CookieSession = TRUE
  ```

  If you want to implement cookie-based mode, be aware of the following:

  - If you set SessionTracking to Cookie, Web browsers with cookie handling disabled cannot maintain a Siebel user session.
  - If you use the Internet Explorer Web browser, make sure that the Web server host name does not include special characters. Internet Explorer does not support session cookies if the Web server host name contains characters such as the underscore (_) or hyphen (-).

  NOTE: Siebel Open UI requires cookie-based mode. If you implement Siebel Open UI, set the SessionTracking parameter in the eapps.cfg file to Cookie.

- URL

  Siebel Open UI clients do not support cookieless mode. However, if you are using a Siebel high-interactivity client or a Siebel standard-interactivity client, you can force the SWSE to always use cookieless mode by setting the SessionTracking parameter to URL. Session information is passed through the URL.

  You might have to implement cookieless mode if security requirements in an organization do not permit the use of cookies. However, this option is not secure and is not recommended for customer-facing deployments of Siebel Business Applications.

  NOTE: In cookieless mode, Siebel URLs reference an internal Siebel parameter, the SRN parameter. The SRN parameter is used in securing client requests during an authenticated user session. Do not change or use this parameter when customizing your Siebel application.

Some Siebel application requirements relating to the settings of the SessionTracking parameter are as follows:

- The Quick Print feature requires that you set SessionTracking to either Automatic (the default) or URL. For information about using this printing feature, see *Siebel Fundamentals*. For information about browser requirements for this feature, see *Siebel System Administration Guide*.
- Inbound EAI HTTP Transport requires cookie-based mode. You can omit the SessionTracking parameter, or set it to either Automatic (the default) or Cookie, in each eapps.cfg file section whose name starts with *eai*. For more information about inbound EAI HTTP Transport, see *Transports and Interfaces: Siebel Enterprise Application Integration* and other relevant Siebel EAI documentation.
- The Remember My User ID functionality requires that you set SessionTracking to either Automatic (the default) or Cookie. Make sure that cookies are enabled in the browser. See also the description of the auto-login credential cookie in "Auto-Login Credential Cookie" on page 210.

If you have implemented Web Single Sign-On as your method of user authentication, then, for security reasons, it is recommended that you implement cookie mode by setting the SessionTracking parameter to Cookie.

Cookie-Based Mode and Cookieless Mode

This topic describes how session IDs are generated and processed in cookie-based and cookieless mode. The mode employed is determined as follows:

- Cookie-based mode applies when SessionTracking is set to Cookie, or when SessionTracking is set to Automatic and the user's browser accepts cookies.
- Cookieless mode applies when SessionTracking is set to URL or when SessionTracking is set to Automatic and the user's browser does not accept cookies.

When a Siebel Web Client user successfully logs into Siebel Business Applications, a unique session ID is generated for that user. The steps involved in a user session are as follows:

1. The components of the session ID are generated in the Siebel Server and sent to the Session Manager running in the SWSE.

2 The session ID is passed to the client either in the URL or in a cookie as determined by the value of the SessionTracking parameter. Depending on the mode implemented, the following occurs:

- In cookie-based mode:
  - The session ID is passed to the user's browser in the form of a nonpersistent cookie which is stored in memory. It stays in the browser for the duration of the session, and is deleted when the user logs out or is timed out.
  - For every application request that the user makes during the session, the cookie is passed to the Web server in an HTTP header as part of the request.
  - The SWSE parses the incoming cookie to obtain the session ID and, if the ID is valid, processes the request. If the HTTP header does not include a cookie containing a valid session ID, then the Web server does not honor that request.
- In cookieless mode:
  - The session ID is passed to the user's browser as an argument in the SWSE construct of the URL. The browser stores the session ID in memory until the session ends.
  - For every application request that the user makes during the session, the request URL includes the session ID.
  - The SWSE parses the incoming request URL to obtain the session ID and, if it is valid, processes the request. If the session ID is missing or not valid, then the Web server rejects the client request.

Using Secure Cookies

To increase the security of session cookies, Siebel Business Applications assign the Secure attribute to all session cookies by default. Setting the Secure attribute for cookies specifies that the cookies are to be transmitted to Web servers only over HTTPS connections, that is, to Web servers that have enabled TLS.

The EnableSecureCookie parameter is used to configure whether or not the Secure attribute is set for Siebel session cookies. If the parameter is set to True, then the Secure attribute is set for all session cookies. If the parameter is set to False, then the Secure attribute is not assigned to session cookies.

The following procedure describes how to configure secure cookies.

To enable secure cookies

1 Navigate to the eapps.cfg file in the *SWEAPP_ROOT*\bin directory.

2 In the [swe] section of the eapps.cfg file, set the value of the EnableSecureCookie parameter to True, which is the default value.

3 Verify that the Siebel Web server is configured to support HTTPS.

If you set the EnableSecureCookie parameter to True, but the Siebel Web server does not support HTTPS communications, then the Secure attribute is not assigned to Siebel session cookies and the cookies can be sent over HTTP connections between the Siebel Web server and the Siebel client.

Session ID Encryption

The session ID is composed of the applicable server ID, process ID, and task ID, combined with a timestamp. All values are in hexadecimal form, as shown:

server_ID.*process_ID*.*task_ID*.*timestamp*

For example, the session ID might resemble the following:

```
sn=!1.132.6024.3ca46b0a
```

You can optionally choose to encrypt the session ID in the URL (cookieless mode) or in the cookie (cookie-based mode). To encrypt the session ID, set the EncryptSessionId parameter to TRUE in the eapps.cfg file.

The RC2 algorithm encrypts the session ID by using a 56-bit encryption key, however, if you are using cookieless mode, the SWSE can specify a different encryption key length. The result of this encryption is then encoded using Base64 Content-Transfer-Encoding. Encrypting the session ID prevents unauthorized users from capturing it and using it in a malicious attack.

You can increase the encryption key length up to 256-bits for AES. To increase the encryption key length, you must use Siebel Strong Encryption. For more information about Siebel Strong Encryption, see "About Siebel Strong Encryption" on page 87.

NOTE: If the user changes the password during an application session, then the password information in the session ID might no longer allow the user to access Siebel Reports during this session. This is the case when using both database authentication and password hashing. After changing the password, the user must log out and log in again in order to be able to run reports.

Auto-Login Credential Cookie

The auto-login credential cookie underlies the Remember My User ID feature on the login page. This cookie consists of the user name for a given user, and the URL string used to access the application. The auto-login credential cookie is persistent and is stored on the user's browser in encrypted form (it is always encrypted). The RC4 algorithm encrypts this cookie. The result of this encryption is then encoded using base64 Content-Transfer-Encoding. This cookie applies to the Siebel Web Client only.

The auto-login credential cookie is not mandatory. It is an optional way to allow users not to have to enter their user name every time they log in. If the user subsequently accesses the application URL through another browser window, then the user information is provided to the application so the user does not have to provide it again.

The format of the auto-login credential cookie is as follows:

start.swe=*encrypted_user_information*

NOTE: Functionality provided by the auto-login credential cookie is not available in cookieless mode.

Related Topic

"About Using Cookies with Siebel Business Applications" on page 206

Siebel QuickStart Cookie

The Siebel QuickStart cookie is created for the Mobile Web Client when Siebel QuickStart is used. The Siebel QuickStart cookie, named siebel.local.client, is persistent and does not contain Siebel session ID data. For more information about Siebel QuickStart, see *Siebel Installation Guide* for the operating system you are using.

Related Topic

"About Using Cookies with Siebel Business Applications" on page 206

Enabling Cookies for Siebel Business Applications

This topic describes how to enable the Microsoft Internet Explorer Web browser to handle cookies used by Siebel Business Applications. These instructions can vary depending on your supported browser version.

NOTE: If you are using a browser other than Internet Explorer to run Siebel Business Applications, see your browser documentation for information on enabling cookies.

To enable cookies using Internet Explorer

1. Choose Tools, and then Internet Options.
2. Click the Privacy tab.
3. In Privacy settings, click Advanced.
4. Verify that Override automatic cookie handling is checked. Also consider:
   - If First-party Cookies is set to Accept, then all Siebel cookies are enabled.
   - If First-party Cookies are blocked, then you can still enable the session cookie by checking Always allow session cookies.
5. Click OK, then click OK again.

Related Topic

"About Using Cookies with Siebel Business Applications" on page 206

8 User Administration

This chapter provides information about registering and administering users of Siebel employee, partner, and customer applications. It includes the following topics:

- About User Registration on page 213
- About Anonymous Browsing on page 214
- Process of Implementing Anonymous Browsing on page 215
- About Self-Registration on page 218
- User Experience for Self-Registration on page 218
- Process of Implementing Self-Registration on page 220
- Identifying Disruptive Workflows on page 232
- About Managing Forgotten Passwords on page 232
- Internal Administration of Users on page 241
- About Adding a User to the Siebel Database on page 241
- Delegated Administration of Users on page 248
- Maintaining a User Profile on page 253

About User Registration

A user who is not a registered Siebel application user has no authenticated access to the Siebel database. Depending on the Siebel application, unregistered users have various levels of access. Minimally, the user can access a login page. By default, or by your configuration, unregistered users can 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 Business Applications. You can grant different registered users different levels of access to the database and features.

Typically, a user is registered when the following tasks are performed:

- Create a user record in the Siebel database.
- Provide the means for the user to be authenticated at login.

Depending on the Siebel application, a user can be registered in one or more of the following ways:

- **Self-registration.** The user can self-register at the Web site.
- **Internal registration.** An administrator at your company can register users.
- **External registration.** A delegated administrator (a user at a customer or partner company) can register users.

If you implement an external authentication system, then adding a user to the Siebel database, whether by self-registration or by an administrator, might or might not propagate the user's login data to the external authentication system. If the login credentials do not propagate to the authentication system, then you must create the login credentials separately in the authentication system.

If you implement database authentication, then adding the user to the database, with the user ID and password, is enough to allow this user to be authenticated. For more information about authentication and propagation of user data, see Chapter 5, "Security Adapter Authentication."

Requirements for User Registration

You must complete the following implementations before you can register users:

- Install your Siebel Business Applications.
- Set up and configure your user authentication architecture.
- Create database accounts for users, as required by your authentication architecture.

Seed Data for User Registration

When you install your Siebel Business Applications, you are provided seed data that is related to user registration, user authentication, and user access to Siebel Business Applications. The seed data includes users, responsibilities, positions, an organization, and a database login. References to the seed data appear throughout this chapter. For detailed information on seed data and for procedures for viewing and editing seed data, see Appendix B, "Seed Data."

About Anonymous Browsing

This topic provides information about anonymous browsing. Several Siebel Business Applications allow anonymous browsing of views intended for public access as default functionality. Anonymous browsing typically applies to Siebel customer and partner applications, not employee applications. However, you can configure any Siebel application to either allow or disallow anonymous browsing.

Unregistered users gain access to application views and the database through the anonymous user. The anonymous user is a record in the Siebel database that also performs functions during user authentication and user self-registration. If you implement an external authentication system, then the anonymous user has a corresponding record in the user directory.

The anonymous user session caches information so any changes to data, for example, catalogs, is not updated until either the user logs in or the anonymous user session is restarted.

For information about the anonymous user's role in user authentication, see "Configuring the Anonymous User" on page 155. For information on implementing anonymous browsing, see "Process of Implementing Anonymous Browsing" on page 215.

Process of Implementing Anonymous Browsing

To implement anonymous browsing so that Siebel views are accessible to unregistered users, you must perform the following tasks:

- Review "Anonymous Browsing and the Anonymous User Record" on page 215
- "Setting Configuration Parameters for Anonymous Browsing" on page 216
- "Configuring Views for Anonymous Browsing or Explicit Login" on page 217

For Siebel Business Applications for which anonymous browsing is implemented by default, confirm that these tasks have been completed.

Anonymous Browsing and the Anonymous User Record

This topic describes the modifications you might have to make to the anonymous user record when you implement anonymous browsing. For additional information on the anonymous user, see "Configuring the Anonymous User" on page 155.

This task is a step in "Process of Implementing Anonymous Browsing" on page 215.

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.

Before implementing anonymous browsing, check that:

- An anonymous user record exists in your Siebel database and external directory.

  In general, you will have set up your user authentication architecture before configuring an application for user access so the anonymous user will already exist in your Siebel database and in your directory. For information, see "Configuring the Anonymous User" on page 155.

- The anonymous user record is assigned appropriate responsibilities.

  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 used for your Siebel Business Application includes an appropriate responsibility so that unregistered users can see the views you intend them to see.

If you choose to use a seed anonymous user in your authentication setup, then verify that its seed responsibility includes the views you want to provide for anonymous browsing. For example, if you use the GUESTCST seed user for a Siebel customer application, then verify that its responsibility, Web Anonymous User, includes the required views.

If the responsibility does not include your required views, then do one of the following:

- Create one or more additional responsibilities that include missing views, and then add these responsibilities to the existing seed responsibility in the anonymous user's Responsibility field. The user has access to all the views in all the assigned responsibilities. For information about creating a responsibility or adding views to a responsibility, see Chapter 9, "Configuring Access Control."
- 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.

Related Topic

"About Adding a User to the Siebel Database" on page 241

Setting Configuration Parameters for Anonymous Browsing

This topic describes the configuration parameters you must set to enable anonymous browsing.

This task is a step in "Process of Implementing Anonymous Browsing" on page 215.

Perform the steps in the following procedure to implement anonymous browsing.

To set configuration parameters for anonymous browsing

1. For a Siebel Web Client deployment, set the AllowAnonUsers parameter to TRUE for the applicable Application Object Manager component as follows:
   a. Navigate to the Administration - Server Configuration screen, then the Servers view.
   b. In the Siebel Servers applet, select the relevant Siebel Server, then click the Components tab.
   c. Select the applicable component, for example, Call Center Object Manager, then click the Parameters tab.
   d. In the Component Parameters applet, locate the AllowAnonUsers parameter and set the Value to True.

      If this parameter is FALSE, then unregistered users are not allowed access to the Siebel application.
2. In the eapps.cfg file, set the following parameters:

- AnonUserName

  This is the user name for the anonymous user. It 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.

  CAUTION: Specify the name of a restricted user for AnonUserName. Do not specify SADMIN as the AnonUserName; doing so allows anonymous users to access every part of the Siebel system.

- AnonPassword

  This is the authenticated password that is paired with AnonUserName.

For information about setting parameter values in the eapps.cfg file, see "About Parameters in the eapps.cfg File" on page 353.

Configuring Views for Anonymous Browsing or Explicit Login

This topic describes how to configure views for anonymous browsing.

This task is a step in "Process of Implementing Anonymous Browsing" on page 215.

When a view is included in the responsibility for the anonymous user, the view is still 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 outlines the general steps you must perform in Siebel Tools to allow a view to be accessible to anonymous users. For detailed information about modifying view properties in Siebel Tools, see *Configuring Siebel Business Applications*.

To remove the explicit login requirement for a view

1. Open Siebel Tools.
2. Select Tools, and then Lock Project.
3. In Object Explorer, select the View object type.

   The Views list appears.
4. Select a view.
5. For each view, set the Explicit Login property to FALSE to allow the view to be available for anonymous browsing.

   Set the Explicit Login property to TRUE if only registered users are to have access to the view.
6. Recompile the Siebel repository file, and unlock the project.

About Self-Registration

Several Siebel Business Applications allow users to self-register as default functionality. This topic observes the following principles about self-registration functionality that is provided by default with your Siebel Business Applications:

- Self-registration applies to Siebel customer and partner applications.
- Self-registration can be implemented only in Siebel Business Applications whose clients use standard interactivity. It cannot be implemented for Siebel employee applications or for any other Siebel application that uses the high interactivity client.
- You can configure any eligible Siebel application to either allow or disallow self-registration.
- You implement Lightweight Directory Access Protocol (LDAP) or Active Directory Service Interfaces (ADSI) security adapter authentication with Siebel Business Applications for which you allow self-registration.

To implement self-registration for applications that use Web SSO user authentication, you are responsible for configuring the self-registration functionality at the Web site level and for synchronizing the user data with the Siebel database. Configuration guidelines are not provided in Siebel Business Applications documentation. Self-registration is not feasible when you implement database authentication.

NOTE: If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow users' Siebel user IDs stored in the directory to be managed from within Siebel Business Applications, including user self-registration. For information about user authentication, see Chapter 5, "Security Adapter Authentication."

User Experience for Self-Registration

Self-registration functionality is available with several Siebel Business Applications. The self-registration experience for end users varies, depending on the application. Some application-specific capabilities are:

- **Siebel eService.** A user self-registers to gain access to more services.
- **Siebel Sales.** A user self-registers to be allowed to make an online purchase.
- **Siebel Partner Portal.** A user self-registers as an individual to become a partner user with limited access, or a user self-registers as a request for his or her company to be approved as a partner. In either case the user is assigned a limited responsibility that contains views to master data, but not to transactional data. This responsibility differs from that for a partner user in an approved partner company.

  For more information on registering partners and partner users for Siebel Partner Portal, see *Siebel Partner Relationship Management Administration Guide*.

To self-register

1 The user clicks New User on a Siebel application page, for example, the Siebel eService home page.

The Personal Information form appears.

2 The user completes the form, then clicks Next. For example, fields for Siebel eService are shown below.

Field	Guideline
First Name	Required. Enter any name.
Last Name	Required. Enter any name.
Email	Required. Enter any valid email address.
Time Zone	Required. Specify the time zone.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Verify Password	Required when Password is required.
Challenge Question	Required. The user enters a phrase for which there is an answer typically known only to this user. If the user clicks Forgot Your Password?, then this phrase is displayed, and the user must enter the correct answer to receive a new password.
Answer to Challenge Question	Required. The user provides a word or phrase that is considered the correct answer to the challenge question.

The Contact Information form appears. The fields on this form vary depending on the application.

3 The user completes the Contact Information form, and then clicks a button at the bottom of the form to continue. The names and number of buttons vary depending on the application.

4 If the application is Siebel Partner Portal or Siebel Sales, then the user does one of the following:

- A user who self-registers for Siebel Partner Portal chooses to register as an individual or to request that his or her company be approved to become a partner. In either case, the user completes a form requiring company information.

- A user who self-registers for Siebel Sales completes forms to provide some or all of the following: payment information, address information, or wireless access information.

5 On the Usage Terms form, the user must agree to the terms of the license agreement to be registered.

The Registration Confirmation message appears.

Process of Implementing Self-Registration

This topic describes the tasks involved in implementing user self-registration.

Self-registration comprises several components, as follows:

- 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.

Perform the following tasks to implement self-registration:

- Review "Self-Registration and the Anonymous User Record" on page 220
- "Setting the PropagateChange Parameter for Self-Registration" on page 221
- Review "About Activating Workflow Processes for Self-Registration" on page 222
- "(Optional) Modifying Self-Registration Views and Workflows" on page 224
- "(Optional) Managing Duplicate Users" on page 228

Self-Registration and the Anonymous User Record

This topic describes the modifications you might have to make to the anonymous user record when you implement self-registration. For additional information on the anonymous user, see "Configuring the Anonymous User" on page 155.

This task is a step in "Process of Implementing Self-Registration" on page 220.

Before implementing self-registration, verify that:

- An anonymous user record exists in your Siebel database and external directory.
- The New Responsibility field of your anonymous user provides all the views you require for self-registering users.

Different Siebel Business Applications in the same implementation can use different anonymous users. Two Siebel application user records, identified by their user IDs, GUESTCST and GUESTCP, are provided as seed data for use as anonymous users. Appendix B, "Seed Data," describes seed data users, responsibilities, and the Siebel Business Applications for which they are designed.

When a user self-registers, a new record is created in the User Registration business component. The User Registration business component is based on the same tables as the User business component, so a new User record is essentially created.

NOTE: When a user self-registers through partner applications, such as Siebel Partner Portal, data is also written to the Contact business component (or equivalent).

The following key fields are populated automatically from fields in the anonymous user's record in the Siebel database:

- **Responsibility.** The new user's responsibility is inherited from the anonymous user's New Responsibility field. A user's responsibility determines the list of views to which the user has access.
- **New Responsibility.** The new user's New Responsibility field value is also inherited from the anonymous user's New Responsibility field. The New Responsibility field is not used by regular registered users. Several Siebel Business Applications allow customer or partner users to be upgraded to delegated administrators. A delegated administrator can register other users, who inherit their responsibility from the delegated administrator's New Responsibility field.

The New Responsibility field is a single-value field. Therefore, if the seed responsibility in the New Responsibility field of your anonymous user does not provide all the views you require for self-registering users, then do one of the following:

- Replace the New Responsibility value with a responsibility you create.
- Copy the seed responsibility record, add missing views to the copy, and replace the New Responsibility with the modified responsibility.

  NOTE: You cannot directly modify a seed responsibility.

For information about creating a responsibility or adding views to a responsibility, see Chapter 9, "Configuring Access Control."

Setting the PropagateChange Parameter for Self-Registration

This topic describes the Siebel PropagateChange parameter. Setting the PropagateChange parameter to True simplifies user administration when you implement user self-registration.

This task is a step in "Process of Implementing Self-Registration" on page 220.

The user directory can be administered through Siebel Business Applications if you implement security adapter authentication. Changes such as adding a user, or changing a password by an internal administrator, a delegated administrator, or when a user self-registers, are propagated to the user directory.

Set the PropagateChange parameter to True for the security adapter so that user data, including user name and password, propagate to the user directory when users self-register from the Siebel Web Client.

To set the PropagateChange parameter to True

1. In a Siebel employee application, such as Siebel Call Center, navigate to the Administration - Server Configuration screen, then the Profile Configuration view.
2. Select either ADSI Security Adapter or LDAP Security Adapter, as appropriate.
3. In the Profile Parameters applet, set the Propagate Change parameter to True.

For additional information about setting the PropagateChange parameter, see "Siebel Gateway Name Server Parameters" on page 361.

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 when a new user is created in the Siebel database.

About Activating Workflow Processes for Self-Registration

When you install Siebel Business Applications, you are provided with several workflow processes that control self-registration. For the self-registration workflow processes to be invoked, you must set the workflows to have a status of Active. For information about how to activate workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

This task is a step in "Process of Implementing Self-Registration" on page 220.

About the Self-Registration Workflow Processes

The self-registration workflow processes together present a sequence of forms for the user to complete. They perform data validation, and they invoke database operations. The self-registration workflow processes which you must activate are as follows:

- **User Registration Initial Process.** For purposes of self-registration, this process is invoked when a user clicks New User on the login form or clicks Check Out during the buying process in Siebel Sales. This process is also invoked by clicking Forgot Your Password? on the login form. The process branches to one of the following subprocesses:
  - User Registration Process
  - User Registration Forgot Password Process
- **User Registration Process.** This is the main self-registration process. It updates the database, including:
  - Creating a new User record
  - Checking for a duplicate User record
  - Updating the existing User record with new information if a duplicate record is found

- **User Registration SubProcess.** This process is a subprocess to User Registration Process. It performs all of the information gathering and validation. The validated information includes:
  - A duplicate user ID does not exist in the database
  - The Password and Verify Password entries are identical
  - All required fields are completed

The registration workflow processes branch at various stages depending on the following:

- The application is Siebel Partner Portal
- The application is other than Siebel Partner Portal

  This is the default case, and it includes Siebel Sales, Siebel eService, Siebel Customer, Siebel Training, Siebel Events, and Siebel Marketing.

About the Self-Registration Workflow Process Views

Table 21 lists the views specified in the workflow processes that provide interactive forms during self-registration.

Table 21. Self-Registration Workflow Views

View Name	Applications Using This View	Description
VBC User Registration Initial Form View VBC User Registration Password Error Msg View VBC User Registration Missing Info Msg View VBC User Registration Legal Confirmation View VBC User Registration Login Error Msg View VBC User Registration Confirmation Msg View VBC User Registration Declined View VBC User Registration Create User Error Msg View VBC User Registration Security Setup Error Msg View	All	These views, common to all applications that use the User Registration Process, comprise two groups: ■ Personal Information form and messages resulting from flawed entries or a duplicate user ID with an existing user record. ■ Usage Terms form and messages resulting from accepting or declining to agree.

Table 21. Self-Registration Workflow Views

View Name	Applications Using This View	Description
VBC User Registration Contact Information View	Default	This view is the Contact Information form used by default.
VBC User Registration Company Information - Company View (SCW) VBC User Registration Company Information - Individual View (SCW) VBC User Registration Contact Information View (SCW)	Siebel Partner Portal	These views collect contact information and information about the user's company.

(Optional) Modifying Self-Registration Views and Workflows

You can modify existing views in a self-registration workflow process or create new views as required. You can also modify the seed workflow processes that are used for self-registration.

This task is an optional step in "Process of Implementing Self-Registration" on page 220.

You can modify the default self-registration functionality in several ways. See the following topics for additional information:

- "Replacing the License Agreement Text" on page 225
- "About Revising a Workflow Process" on page 225
- "Custom Business Services" on page 225
- "Redefining Required Fields" on page 226
- "Adding or Deleting Fields in an Existing View" on page 227
- "About Changing the Physical Appearance of a View or Applet" on page 228
- "About Creating a New View for Self-Registration" on page 228

Modifying self-registration views, applets, and workflow processes include standard processes common with modifying other views, applets, and workflow processes.

The views used in the self-registration workflow processes are based on the VBC User Registration virtual business component, which collects the user data. The data is written to the User Registration business component and the Siebel database only when all stages of collecting user data are completed. Before you make any modifications, you must understand how these components handle the user data.

The User Registration and User business components are both based on the same database tables: S_PARTY, S_CONTACT, and S_USER. Therefore, writing a record through the User Registration business component is equivalent to writing a record through the User business component. In either case, a new user is created.

The user-registration process provides the following benefits:

- If the self-registration process is terminated before completion, then it is not necessary to perform the time-consuming process of undoing a new, partially written record in the database. This process requires searching several tables.
- User record duplication can be prevented before a record is written.

Replacing the License Agreement Text

You can replace the default license agreement that appears to the self-registering user in the User Registration Legal Confirmation View.

The DotCom Applet License Base 1 Column Web template includes the Web template file with the name DotCom Applet Form Base 1 Column, which is the file of name dCCAppletLicenseBase1Col.swt. The license agreement is contained in the dCCAppletLicenseBase1Col.swt file, following the phrasing: *<!--This is where we include the html license agreement-->.* You can replace the license agreement text. For information about working with Web templates, see *Configuring Siebel Business Applications*.

About Revising a Workflow Process

The self-registration workflow processes for your business scenario might require that you do revisions to the seed self-registration workflow processes, such as:

- Replace or insert a view
- Insert or delete a step
- Modify a step

You cannot directly modify a seed workflow process, such as any of the self-registration processes. Instead, you must create a copy of the process, and then revise the copy.

By convention, to avoid renaming processes, you can use the Revise button to make a copy of the same name, but with an incremented version number. All other processes of the same name are assigned Outdated status, so that the new version can be the only active version. This convention is recommended for revising any workflow process, not just seed processes. For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

Custom Business Services

Siebel Business Applications provides predefined business services that you can use in a step of a workflow process. You can also script your own custom business services and then run them in workflow process steps. For information about predefined business services and creating business services, see *Configuring Siebel Business Applications*. For information about running business services in workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

Redefining Required Fields

As default functionality, a user who is self-registering is required to provide entries in certain fields. These fields might differ depending on the application. A required field is indicated in the user interface by a star icon, where the field appears in a form.

For a view used in the self-registration workflow processes, you can change whether a field is required. Use Siebel Tools to determine the view that includes a self-registration field. For information about how to view, revise, activate, and deploy workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

The CSSSWEFrameUserRegistration frame class is applied to applets that are used in views that appear in the seed self-registration workflow processes. This class allows you to specify required self-registration fields.

To designate a required field in a self-registration form, use Siebel Tools to modify the applet that contains the form. The following procedure is intended to present the main steps in a Siebel Tools task. For detailed information about working with applets and views in Siebel Tools, see *Configuring Siebel Business Applications*.

To designate a required field in a self-registration form

1. Open Siebel Tools.
2. Lock the User Registration project.
3. In Object Explorer, expand the View object type.

   The Views list appears.
4. Select a view that includes a self-registration field.
5. In Object Explorer, expand the View Web Template child object type, and then expand its child, View Web Template Item.

   Self-registration views typically contain a single form applet. It is listed in the View Web Template Items list.
6. In the View Web Template Items list, drill down on the link in the Applet field for the single applet that is listed. If there is more than one applet listed, then 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, and then New Record.

A new user property record appears.

11 Complete the following fields. Use the indicated guidelines.

Field	Guideline
Name	Required. Enter Show Required and a sequence number one greater than the highest existing sequence number. For example, if Show Required 6 is the highest sequenced entry, then enter Show Required 7. This entry is case-sensitive.
Value	Required. The name of the field that you recorded in Step 8 on page 226, 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 a star icon.

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 227, or delete the record.

Adding or Deleting Fields in an Existing View

All the data collected in views used in the seed self-registration workflow processes are written to fields in the User Registration business component. The following process describes how data is collected in the user interface and written to a user's record in the database:

- The user enters data, such as the user's last name, into a text box on a form.
- The text box is mapped to a field in the VBC User Registration virtual business component, such as LastName. Consequently, the data is written to that field.
- Data from the virtual business component VBC User Registration is written to the User Registration business component. The User Registration business component writes to the same database tables as the User business component. Consequently, each field is actually stored as part of a user record.

  NOTE: No data from the VBC User Registration virtual business component is written to the User Registration business component fields until the self-registration process is complete.

To add or delete fields in a view used in a self-registration workflow process, you must perform Siebel Tools tasks and then Siebel Workflow tasks (using Business Process Designer in Siebel Tools).

To add a field to one of the views used in the self-registration workflow processes, you must use Siebel Tools to do one or more steps of the following procedure. This procedure is intended to identify the major tasks required. For detailed information about modifying views and applets, see *Configuring Siebel Business Applications*.

To add a field to a view used in a self-registration workflow process

1 Open Siebel Tools.

2 Lock the User Registration project.

3 Determine the business component and the underlying database table on which the new field is based.

4 If the new field is not based on an existing database table column, then 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, then create a new field in the VBC User Registration virtual business component. Use the exact same field name.

7 Configure the appropriate applet to display the new field in the user interface.

8 If necessary, configure the new field so that a self-registering user is required to complete it.

9 Recompile the Siebel repository file, and unlock the User Registration project.

NOTE: To remove a field from the self-registration user interface, you do not have to delete the field from the applet in which it appears. Instead, configure the applet so that the field is not displayed in the user interface.

About Changing the Physical Appearance of a View or Applet

For information about changing the physical appearance of a view or applet, such as moving fields or changing colors, see *Configuring Siebel Business Applications*.

About Creating a New View for Self-Registration

You create a new view for insertion into one of the self-registration workflow processes in the same way you create a view for any other purpose.

You can include new applets in a view that you create that you include in a self-registration workflow process. You create the new applet and include it in the view in the same way as you would for any other purpose. However, if you base the applet on the User Registration business component, then apply the CSSSWEFrameUserRegistration class to the applet. This allows you to define fields for which a star icon displays in the user interface. By convention, fields that you require users to complete during the self-registration process have a star icon. For information about working with views, see *Configuring Siebel Business Applications*.

(Optional) Managing Duplicate Users

When a user self-registers, the User Registration Process workflow process attempts to determine whether the user already exists in the database. User deduplication is a default feature, and it is configurable.

This task is an optional step in “Process of Implementing Self-Registration” on page 220.

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, then 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, then the existing field is updated with the new data. All other existing field values are left unchanged.

In the User Registration SubProcess workflow process, the duplication comparison is done by the ValidateContact method in the User Registration business service. The comparison is done by the Check User Key step.

Modifying Updated Fields for a Duplicate User

You can specify that certain fields in the User Registration business component are not updated when a duplicate user is determined.

The following procedure is intended to list the major steps you must do. For detailed information about doing any step, see *Configuring Siebel Business Applications*.

To exclude a field from being updated when a duplicate user is determined

1. Open Siebel Tools.
2. Lock the User Registration project.
3. Determine the field in the VBC User Registration virtual business component that you want to exclude from updating.
   a. In the Object Explorer, click Business Component.
   b. In the Business Components list, select the VBC User Registration business component.
   c. In the Object Explorer, expand the Business Component item, then select the Field child item.
   d. In the Fields list, query or scroll to select the field you want to exclude.
4. Add the appropriate business service user property.
   a. In the Object Explorer, click Business Service.
   b. In the Business Services list, select the User Registration business service.
   c. In the Object Explorer, expand the Business Service item, then select the Business Service User Prop child item.
   d. In the Business Service User Props list, create a new record.

e Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter Exclude From Update *number*, where *number* is the next number in the sequence for this particular user property. For example, enter Exclude From Update 3. This entry is case-sensitive.
Value	Enter the field name from the VBC User Registration virtual business component that you noted in Step 3 on page 229.

5 Recompile the Siebel repository file and unlock the User Registration project.

Modifying Fields Used to Determine a Duplicate User

You can change the fields that are used to determine whether a duplicate user exists.

The following procedure is intended to list the major steps you must perform to modify the fields used to determine a duplicate user. For detailed information about performing any step, see *Configuring Siebel Business Applications*.

To modify the fields used to determine a duplicate user

1 Open Siebel Tools.

2 Lock the User Registration project.

3 Determine the fields in the User Registration business component that you want to add or delete from the duplication comparison.

a In the Object Explorer, expand Business Component, and then expand its Field child.

b In the Business Component list, select the User Registration business component.

4 In the Object Explorer, expand Business Service, and then click on its Business Service User Properties child.

The Business Services list and the Business Service User Properties child list appear.

5 In the Business Services list, select User Registration.

6 Delete a field from the duplication comparison:

a In the Business Service User Properties list, select the record with name App User Key: Default *number* or App User Key: Siebel eChannel *number* (for Siebel Partner Portal) whose value is the User Registration business component field you want to delete from the comparison.

b Click to put a check in the Inactive field, and then commit the record.

7 Add a field to the duplication comparison:

a In the Business Service User Properties, create a new record.

b Enter only the fields listed below. Use the indicated guidelines.

Field	Guideline
Name	Enter App User Key: Default *number* or App User Key: *application number*, where *application* is the name of the Siebel application, and *number* is the next number in the sequence for this particular user property. This entry is case-sensitive. For example, you might enter App User Key: Default 2 to add a field for Siebel eService, or App User Key: Siebel eChannel 4 to add a field for Siebel Partner Portal.
Value	Enter the name of the field in the User Registration business component that you want to add to the duplication check.

8 Recompile the Siebel repository file and unlock the User Registration project.

Deactivating the Duplicate User Check

You can deactivate the duplicate user check.The following procedure is intended to show the main steps in deactivating the duplication check. For more detailed information on working with workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

To deactivate the self-registration deduplication check

1 In Siebel Tools, select Workflow Process in the Object Editor.

2 Query or scroll to select User Registration SubProcess.

3 Create a revised copy of User Registration SubProcess.

For information, see "(Optional) Modifying Self-Registration Views and Workflows" on page 224.

4 Right-click and choose Edit Workflow Process to edit the revised copy.

The Process Designer appears, showing the current workflow process.

5 For each process step that applies to your application, record the sources of all connectors to the step and the destination of the single connector from the step. Reroute the connectors to bypass the step. For all Siebel Business Applications, choose the Check User Key step.

6 Delete the bypassed process step, which is no longer the source or destination of any connector.

7 Right-click and choose All Processes.

The Workflow Processes list appears again. The revised process is still selected.

8 Click Deploy.

Identifying Disruptive Workflows

This topic describes how to identify workflows that are interfering with the user registration process. Once identified, these workflows can be deactivated allowing the user registration process to proceed.

This task is part of "Troubleshooting User Registration Issues" on page 348.

If nothing happens when a user clicks Next in a User Registration view, then verify that the workflow processes that control self-registration are activated. For information on this task, see "About Activating Workflow Processes for Self-Registration" on page 222. If the appropriate workflows are activated, then the problem might be caused by a disruptive workflow. The following procedure describes how to identify and locate workflows that are disrupting the user registration process so that they can be deactivated.

To locate a disruptive workflow

1. In the Administration - Runtime Events screen, click the Events view.
2. Query for Object Name is null.

   If there are no disruptive workflows, then only application type events are returned. Take note of any record whose Action Set Name value begins with Workflow. Such a record indicates that the workflow is triggered every time the event specified in the Event field happens. This can be particularly disruptive if the event is common, such as ShowApplet or WriteRecord. The Object Name normally constrains the actions to trigger only when the specified event occurs within the context of the object; for example, a specific business component or applet.
3. If there is a suspicious Event, then drill down on the Action Set Name and note the ID following the string ProcessId in the Business Service Context field.
4. Query against the database to find the suspect workflow. Use a query similar to the following:

   ```
   select NAME from S_WF_STEP where ROW_ID='xxx'
   ```

   where *xxx* is the ID noted in Step 3.

   The workflow returned in the query is the disruptive one. Deactivate it.

About Managing Forgotten Passwords

This topic describes how to manage forgotten passwords. If a user who has previously self-registered on a Siebel customer or partner application forgets his or her password, then the user can get a new password by clicking the Forgot Your Password? link in the login dialog box.

NOTE: Forgot Your Password? is a default feature of Siebel customer and partner applications, but it is available only if you implement LDAP or ADSI security adapter authentication. To implement similar functionality in a Web SSO environment, you are responsible for configuring the functionality in your external authentication application, in your user directory, and in your security adapter. Consult your third-party vendor documentation for information about performing these tasks.

You can optionally configure the Forgot Your Password? feature in a number of ways:

- You can specify the minimum and maximum length of the new password that a user can retrieve as described in "Defining Password Length for Retrieved Passwords" on page 234.
- You can amend the forgotten passwords workflow process to change:
  - The way in which the user identification data is compared with database user records.
  - The identification data requested from users.

  For information on both these tasks, see "Modifying Workflow Process to Request Different Identification Data" on page 238.

For additional information about managing forgotten passwords, see also the following topics:

- "Retrieving a Forgotten Password (Users)" on page 233
- "Architecture for Forgotten Passwords" on page 235
- "About Modifying the Workflow Process for Forgotten Passwords" on page 236

Retrieving a Forgotten Password (Users)

This topic describes how users, who have previously self-registered, can create new passwords if they have forgotten their existing password. On a future login, users can change new passwords in the User Profile view.

The following procedure describes the steps involved in retrieving a new password.

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, then the Challenge Question form appears.
3. The user enters the answer to the challenge question.
4. If the challenge question is answered correctly, then the user is prompted to enter a new password, and then to reenter the password to confirm it.

   Provided that the passwords match and do not violate the requirements for passwords set by the directory server, the new password is set for the user.
5. Click Continue.

Related Topic
"About Managing Forgotten Passwords" on page 232

Defining Password Length for Retrieved Passwords

This topic describes how to configure the length of new passwords retrieved by users who have previously self-registered but who have forgotten their password. For information on the forgotten password feature, see "About Managing Forgotten Passwords" on page 232 and "Retrieving a Forgotten Password (Users)" on page 233.

To make sure that passwords conform to your company's policy on password length, you can specify minimum and maximum character lengths for passwords by adding two user properties to the User Registration business service in Siebel Tools. These user properties are RandPassMinLength and RandPassMaxLength. When a user requests a new password using the Forgot Your Password feature, the User Registration business service invokes the SetPassword method to create the new password after verifying that the password meets the password length requirements defined for these two properties.

To define minimum and maximum values for password length

1. Open Siebel Tools and, in the Object Explorer, click Business Service.

   The Business Services list appears.

2. In the Business Services list, query or scroll to select the User Registration business service.
3. Choose Tools, and then Lock Project.
4. In the Object Explorer, click Business Service User Props.

   The Business Service User Props list appears.

5. Right-click in the Business Service User Props list and select New Record from the displayed context menu.

   A new record field appears.

6. Complete the fields for the new record, as shown in the following table.

In this field...	Enter...
Name	RandPassMinLength
Value	Enter the minimum number of characters that your company's password policy states a password must contain. The default value is 5.

   This defines the minimum number of characters that a password can contain.

7. Step off the record to save changes.

8 Repeat Step 5, Step 6, and Step 7 with modifications for Step 6, as shown in the following table.

In this field...	Enter...
Name	RandPassMaxLength
Value	Enter the maximum number of characters that your company's password policy states a password must contain. The default value is 15.

This defines the maximum number of characters that a password can contain.

9 Recompile the Siebel repository file, and unlock the User Registration project.

Related Topic

"About Managing Forgotten Passwords" on page 232

Architecture for Forgotten Passwords

Forgot Your Password? is implemented in the User Registration Forgot Password Process workflow process. This process is a subprocess in User Registration Initial Process.

As described in "Retrieving a Forgotten Password (Users)" on page 233, to receive a new 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, then the user must answer the challenge question associated with that record. The challenge answer must also return a case-sensitive match.

When a user enters values to the comparison fields in the user interface, the values are written to fields in the User Registration business component. This business component is based on the same tables as the User business component. The virtual field values are not written to the database, but are compared with field values in those underlying tables. The user entries in the following fields in the user interface are compared with field values in the tables indicated:

- The Last Name, First Name, Email, and Work Phone # fields are compared with S_CONTACT field values.
- The Challenge Answer field is compared with an S_USER field value.

The User Registration Forgot Password Process workflow process uses the following views:

- User Registration Forget Pwd Challenge Answer Error View
- User Registration Forgot Pwd Error View
- User Registration Forgot Pwd Invalid Error View
- User Registration Forgot Pwd Reset Confirm View
- User Registration Pwd Info View
- User Registration Pwd Nomatch View
- User Registration Forget Pwd Challenge Ques View

Related Topic
“About Managing Forgotten Passwords” on page 232

About Modifying the Workflow Process for Forgotten Passwords

You can modify the User Registration Forgot Password Process workflow process in the following ways:

- Make a comparison of null fields as well as fields for which the user has provided a value

  For information on this task, see “Modifying Workflow Process to Query Null Fields” on page 237.

- Request different identification data from the user

  For information on this task, see “Modifying Workflow Process to Request Different Identification Data” on page 238.

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, then the user can prove he or she owns the record by answering the challenge question.

Table 22 on page 237 describes the arguments for the FindContact method.

Table 22. FindContact Method Arguments

List	Records	Comments About Values
Input Arguments	EmailAddress FirstName LastName WorkPhoneNum	The Input Argument field values are the field names in the User Registration business component that the FindContact business service queries for a match. The comparison is made with the process property values given in the Property Name field. These process properties collect the entries made by the user.
	Output Field: Id Output Field: Login Name	As given by the Input Argument field values, the FindContact method is requested to return the Id and Login Name field values for each user record whose field values match the entries by the user. A temporary table of values is defined in which the rows are the records returned and the columns are given by the Value field values. One row of the temporary table contains the ID for a returned record in the Id column and the record's Login Name in the Login Name column.
Output Arguments	Login Name Siebel Operation Object Id RegError	■ Each Property Name field value is a process property name. The Login Name and Siebel Operation Object Id process properties receive values if FindContact returns a unique matching record. If a unique record is not determined that matches the criteria, then 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.

Related Topic
"About Managing Forgotten Passwords" on page 232

Modifying Workflow Process to Query Null Fields

By default, if a user completes fewer than all four fields on the User Information form, then 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, then the query does not do any comparisons on the Email or Work Phone # fields.

You can specify that the Query User step (FindContact method in the User Registration business service) must 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. The following procedure describes this task.

To modify the User Registration Forgot Password Process workflow to query null fields

1. Make a copy of the User Registration Forgot Password Process workflow.
2. In the copy of the workflow, modify the Query User step by adding the QueryAllFields input argument with a value of Y. By default, the value of this input argument is N.

   When you create input arguments, enter the fields and values described in the following table.

Field	Value
Input Argument	QueryAllFields
Type	Literal
Value	Y

3. Activate the amended copy of the User Registration Forgot Password Process workflow.

   For detailed information about modifying workflow processes, see *Siebel Business Process Framework: Workflow Guide*.

Related Topics

"About Modifying the Workflow Process for Forgotten Passwords" on page 236

"Modifying Workflow Process to Request Different Identification Data" on page 238

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 input arguments

Modifying the User Interface for User Registration

To add or delete a field in the User Information form, you must use Siebel Tools to modify its underlying applet. The following procedure is intended to list the major steps you must perform to add or delete a field in the User Information form. For detailed information about performing any step, see *Configuring Siebel Business Applications*.

To add or delete a field in the User Information form

1. Open Siebel Tools.
2. Lock the User Registration project.
3. If you are adding a field, then determine what field to add. Add to both the VBC User Registration virtual business component and the User Registration business component the field that corresponds to the field you want to add. Use the same names for these fields.

   For more information, see "(Optional) Modifying Self-Registration Views and Workflows" on page 224.

   a. In the Object Explorer, click Business Component.

   b. In the Business Components list, query or scroll to select the User Registration business component.

   c. In the Object Explorer, expand Business Component, then click its Field child item.

   d. In the Fields list, add the field you need for this business component.

   e. Repeat this process for the VBC User Registration virtual business component.
4. Configure the applet VBC User Registration Initial Form Applet to display or hide the field.

   a. In the Object Explorer, click Applet.

   b. In the Applets list, query or scroll to select the applet VBC User Registration Initial Form Applet.

   c. In the Object Editor, expand Applet, then click its Control child item.

   d. In the Controls list:

   - If you want to hide a field, then select its record in the Controls list and check its Inactive field.
   - If you want to add a field, then add a new record in the Controls list. Complete only the fields listed. Use the indicated guidelines.

Field	Guideline
Name	Enter a name for this field, such as City
Caption	Enter the caption you want for this field in the user interface, such as City
Field	Enter the field that you determined in Step 3 on page 239, such as City
HTML Display Mode	Delete the default value, so the field is empty
HTML Row Sensitive	Check
HTML Type	Pick Text
Sort	Check
Text Alignment	Pick an alignment

Field	Guideline
Visible	Check
Visible - Language Override	Enter Y

5 Configure the appropriate applet Web template for VBC User Registration Initial Form Applet to display or hide the field.

6 Recompile the Siebel repository file and unlock the User Registration project.

To remove a field from the self-registration user interface, you do not have to delete the field from the applet in which it appears. Instead, configure the applet so that the field is not displayed.

Modifying Input Arguments for the Workflow Process

In the Query User step of User Registration Forgot Password Process, you specify the input fields to the FindContact method in the User Registration business service that are used to find a matching user record. You must modify this step to add or delete an input field.

You make this change by modifying the input arguments for the Query User step for a revised copy of the User Registration Forgot Password Process workflow process, then activating this copy. When you create input arguments, enter the fields and values described in Table 23.

Table 23. Values for Input Arguments for Query User Step

Field	Guideline
Input Argument	Enter the name of the field in the User Registration business component that you noted in Step 3 on page 239 of "Modifying the User Interface for User Registration" on page 238, such as City. This is the field in the existing user records with which the comparison is made.
Type	Pick Process Property.
Property Name	Pick the process property that corresponds to the field in the User Registration business component that you noted in Step 3 on page 239 of "Modifying the User Interface for User Registration" on page 238, such as City. The process property has the same name as the field, by convention.
Property Data Type	This field automatically populates with the data type of the process property.

Related Topics

"About Modifying the Workflow Process for Forgotten Passwords" on page 236

"Modifying Workflow Process to Query Null Fields" on page 237

Internal Administration of Users

You can provide an employee, a customer, or a partner user with access to one or more Siebel Business Applications by performing the following tasks:

- Provide the user with a method to be authenticated and thus to connect to a database account.
- An internal administrator uses a Siebel employee application, such as Siebel Call Center, to add the user to the Siebel database.

Implement your authentication architecture before adding new users. As an ongoing task, you must arrange that each new user can be authenticated at login. The setup and administration that you must perform for each new user depends on the authentication architecture you implement:

- **Database security adapter authentication.** You must enter the user name for a valid database account in the user's user ID field. You must provide the user ID and the password to the database account to the new user.
- **LDAP or ADSI security adapter authentication.** You can configure your application so that when you create or modify user records in the Siebel database, the security adapter propagates those changes to the user directory. Therefore, no separate administration of the user directory is required.

  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 Business Applications and you cannot propagate a user's Siebel user ID to the directory.

  NOTE: Make sure the application user has write privileges to the user directory. The application user is the only user who creates or modifies users in the directory.
- **Web SSO authentication.** You must maintain corresponding records in the external authentication system, the user directory, and the Siebel database for each user. If you want to implement a mechanism for synchronizing these records, then you must develop the utility independently, and implement it at the Web site level. Configuration guidelines are not provided in Siebel Business Applications documentation. You must provide authentication credentials to the new user.

About 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 Sales, do not have a position or a division. The S_EMP_PER table underlies the Employee business component, to which employees and partner users belong, in addition to the tables that underlie the User business component.

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 might be stored in various other types of records, using a field such as CREATOR_LOGIN (where a foreign key to the user record is not used instead). Values for such fields are not automatically updated when the user ID is updated. If you change the user ID, then you must also update such values in other records.

For more information about the functions of responsibilities, positions, divisions, and organizations, see Chapter 9, "Configuring Access Control." See the following topics for information on adding users to the Siebel database:

- "Adding a New Employee" on page 242
- "About Adding a New Partner User" on page 244
- "Adding a New Contact User" on page 245
- "Modifying the New Responsibility for a User Record" on page 247

Adding a New Employee

The procedure in this topic describes how to add a new employee record to the Siebel database.

At a minimum, an employee must have a position, a responsibility, and a Siebel user ID. You can also associate attributes with employee records such as skills, tools, assignment rules, and availability. By doing so, you can use the employee record and its attributes with features such as Siebel Assignment Manager.

The following procedure creates a User record for the employee only as a stage in allowing the employee to access the database.

To add a new employee

1. Log in as an administrator to an employee application, such as Siebel Call Center, and then navigate to the Administration - User screen, then the Employees view.

   The Employees list appears.

2. Add a new record.

3 Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier. If you implement database authentication, then this field must be the login name for a database account.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Responsibility	Required. Pick one or more responsibilities which include appropriate views for the employee. If the administrator who creates the employee user has a value in his or her New Responsibility field, then that responsibility is assigned to the employee user by default. For information about the New Responsibility field, see "Modifying the New Responsibility for a User Record" on page 247.
New Responsibility	Optional. If the administrator who creates this user has a value in his or her New Responsibility field, then that responsibility is assigned to this field by default. For information about the New Responsibility field, see "Modifying the New Responsibility for a User Record" on page 247.
Position	Required. To be an employee, a user must have a position. If you assign multiple positions, then the position you specify as Primary is the position the user assumes when he or she logs in.
Division	Required. This field is populated automatically with the division to which the Primary position belongs.
Territory	This field is a read-only multi-value group. You are not able to enter a value manually. When you complete the Position field, the Territory field is populated automatically with territories with which the position is associated. (This field appears on the More Info form.)
Organization	This field value is inherited from the user who creates this user, but the field is editable. Users whose positions are in this organization have access to this employee record. (This field appears on the More Info form.) For information about organization access control, see Chapter 9, "Configuring Access Control."

Completing Employee Setup

You can set up employees either before or after you assign them a responsibility. For more information about completing employee setup, see the initial setup topic of *Siebel Applications Administration Guide*. Also see *Siebel Assignment Manager Administration Guide*.

Deactivating an Employee

You can deactivate an employee by dissociating the employee record from its responsibilities, altering the user ID, changing the employee's status to Terminated, and removing the employee's access to the database. The following procedure describes these tasks.

To deactivate an employee

1. Navigate to the Administration - User screen, then the Employees view.
2. In the Employees list, select the employee you want to deactivate.
3. In the More Info view tab, delete all records from the Responsibility field.
4. Change the user ID slightly, to indicate that the employee is no longer current.

   You might want to establish a convention for renaming user IDs when you deactivate employees. One possible convention is to append some text such as "expired" to the user ID. For example, you might change CARD to CARD-expired. That way you can continue to see the person's name associated with previous activity in history records.
5. Select the Job Information tab.
6. Change the Employment Status field from Active to Terminated.
7. Remove the employee's access to the database.

   If you implemented database user authentication, then you can remove the user's database account. If you implemented external authentication, then delete the user from the directory from which the user's database credentials are retrieved.

   NOTE: In the case of external authentication, if the external user directory (such as LDAP or ADSI) is shared by many applications, do not delete the user from the directory. Make sure that the user's database access user name and password are different from that user's directory user name and password. Otherwise the user might be able to access the database directly using some database connection tools.

Related Topics

"About Adding a User to the Siebel Database" on page 241

"Modifying the New Responsibility for a User Record" on page 247

About Adding a New Partner User

A partner user is typically an employee in a partner company or a consultant to your company.

A partner user must have a position in a partner organization to be associated with that organization or to belong to position-based teams, such as opportunity or account teams.

You can assign a position to a new partner user from the following sources:

- Positions that you create internally and associate with the delegated administrator's partner organization
- Positions created by delegated administrators in the partner organization

You can register and administer partner users in the Administration - Partner screen in Siebel Partner Manager or another Siebel employee application for which you have licensed this screen. For information about using the Administration - Partner screen, see *Siebel Partner Relationship Management Administration Guide*.

Related Topics

"About Adding a User to the Siebel Database" on page 241

"Modifying the New Responsibility for a User Record" on page 247

Adding a New Contact User

The procedures in this topic describe how to add a new contact user record to the Siebel database and how to promote a contact to a contact user.

Users who are not employees or partner users do not have positions. These users include, for example, customers who use Siebel Sales or students who use Siebel Training. They are called customer or contact users to distinguish them from employee and partner users.

Contacts, such as contacts at a customer account, can exist in the database without having login capability. You create such contacts as Persons in the Administration - User screen. The procedure in this topic applies to contact users to whom you are providing a login to the Siebel database.

CAUTION: You can modify field values for existing contact users, such as in the event of a name change. However, changing the user ID for such a user presents special issues, because this ID might be stored in various types of records, using a field such as CREATOR_LOGIN (where a foreign key to the user record is not used instead). Values for such fields are not automatically updated when the user ID is updated. If you change the user ID, then you must manually update such values in other records.

The following procedure describes how to add a new contact user.

To add a new contact user

1. Log in as an administrator to a Siebel employee application, navigate to the Administration - User screen, then the Users view.

   The Users list appears.

2. Add a new record.

3. Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Account	Pick one or more accounts to associate to the user. Specify one as the primary account. By default, the user sees this account when he or she logs in. For information about the function of the account in delegated administration, see “Delegated Administration of Users” on page 248.
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 the contact user has a value in his or her New Responsibility field, then that responsibility is assigned to the new contact user by default.
New Responsibility	If the administrator who creates this user has a value in the New Responsibility field, then that responsibility is assigned to this field by default. For information about the New Responsibility field, see “Modifying the New Responsibility for a User Record” on page 247.
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.
Work Phone # Home Phone # Fax #	The application interprets only the digits the user provides. Any separators are disregarded.

The new user appears in the Users list.

Promoting a Contact to a Contact User

You can promote an existing contact to a contact user by assigning user credentials and a responsibility to a Person record (a contact), as described in the following procedure.

To promote an existing contact to a contact user

1. Log in as an administrator to a Siebel employee application.
2. Navigate to the Administration - User screen, then the Persons view.

   The Persons list appears.
3. Select the record of the contact to promote.
4. Enter values for the User ID, Password, Responsibility, and New Responsibility fields.

   For information, see "Adding a New Contact User" on page 245.

Related Topics

"About Adding a User to the Siebel Database" on page 241

"Modifying the New Responsibility for a User Record" on page 247

Modifying the New Responsibility for a User Record

A user record might or might not have a value in the New Responsibility field in the Users view. If a value does exist, then whenever the user creates a new user, the new user's Responsibility field is assigned the value in the creating user's New Responsibility field by default. This principle applies when a user of any type (employee, partner user, contact user) creates any other type of user.

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 might or might 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 might make sense to leave employee's New Responsibility field empty. If most of your new employees are assigned the same responsibility or you want to create a batch of new employee records that all have the same responsibility, then it is probably more efficient to assign a New Responsibility value to the administrator who adds the employees.

An internal administrator can modify New Responsibility values for employees, partner users, and contact users in the same administration screen.

To modify a user's New Responsibility field value

1. Log in as an administrator to a Siebel employee application and navigate to the Administration - User screen, then the Users view.

   The Users list appears, containing all the employees, partner users, and contact users in the database.

2. In the Users list, select the user record to modify.
3. In the form, pick a new value in the New Responsibility field, then save the record.

   The user must log out and log in for the New Responsibility value to become active.

Related Topic

"About Adding a User to the Siebel Database" on page 241

Delegated Administration of Users

A delegated administrator is a user of a Siebel customer or partner application whose responsibility provides views that allow the delegated administrator to register and administer other users of that application. Delegated administration is typically implemented in business-to-business relationships.

Delegated administration of users minimizes your internal administrative overhead by moving some of the administrative load to administrators in your customer or partner companies.

See the following topics for further information about delegated administration of users:

- "User Authentication Requirements for Delegated Administration" on page 249
- "Access Considerations for Delegated Administration" on page 249
- "Registering Contact Users (Delegated Administration)" on page 250
- "Registering Partner Users (Delegated Administration)" on page 252

User Authentication Requirements for Delegated Administration

Delegated administration is default functionality of most Siebel customer and partner applications, but it is available only if you implement LDAP or ADSI security adapter authentication.

Delegated administration cannot be implemented if you use database authentication. If you want to implement delegated administration in a Web SSO authentication environment, then you are responsible for configuring the functionality in your external authentication application, in your user directory, and in your security adapter. Such configuration guidelines are not provided in Siebel Business Applications documentation.

Delegated administration requires you configure the LDAP or ADSI security adapter to propagate new and modified user data from the Siebel database to the user directory.

If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow Siebel user IDs stored in the directory to be managed from within Siebel Business Applications, including delegated administration of users. For information about user authentication, see Chapter 5, “Security Adapter Authentication.”

NOTE: Make sure the application user for your Siebel customer or partner application has write privileges to the user directory.

Related Topic

“Delegated Administration of Users” on page 248

Access Considerations for Delegated Administration

A delegated administrator has restricted access to user data.

- **Customer applications.** A delegated administrator can only see users who are associated with accounts with which the delegated administrator is associated. The My Account User Administration View is based on the Account (Delegated Admin) business component. This business component essentially restricts a delegated administrator’s access to data that is associated with the accounts with which the delegated administrator is also associated.
- **Partner applications.** A delegated administrator can only see partner users whose positions are in the same partner organization to which the delegated administrator’s position belongs.

A delegated administrator can add regular registered users or other delegated administrators. However, an administrator at your host company must add the first delegated administrator in:

- Each account for a Siebel customer application
- Each partner organization for a Siebel partner application

Creating a delegated administrator internally requires that you provide a user with a responsibility that includes the views needed for delegated administration. Your Siebel application provides seed responsibilities for delegated administrators of customer and partner applications. For information about seed responsibilities, see Appendix B, "Seed Data."

NOTE: Delegated user administration screens, navigation, and procedures vary somewhat among Siebel Business Applications. The remaining topics describe delegated administration that is representative of customer and partner applications.

Related Topic

"Delegated Administration of Users" on page 248

Registering Contact Users (Delegated Administration)

A delegated administrator who uses a Siebel customer application must belong to at least one account. The delegated administrator registers a user in the currently active account. The new user inherits membership in that account.

A delegated administrator must assign at least one responsibility to a new user. A delegated administrator can only assign responsibilities, including seed responsibilities, to users who are associated to same organization that the delegated administrator is associated with.

The delegated administrator is associated with the organization to which the proxy employee for the application belongs. The proxy employee is provided as seed data and is associated with the default organization. As with other seed data that Siebel Business Applications provide, you cannot modify the proxy employee. This means that to associate a delegated administrator with an organization other than the default organization, you have to make a copy of the proxy employee record and rename it. You then assign the renamed proxy employee to the organization that you want to associate the delegated administrator with. A responsibility is associated with an organization by an administrator at your company using an employee application such as Siebel Call Center.

For example, if the application object manager in use is the eCustomer Object Manager (ENU) and the proxy employee (PROXYE) is assigned the position Proxy Employee in Default Organization, then the eCustomer Object Manager (ENU) runs under the Default Organization context. If you need to run the eCustomer Object Manager (ENU) under the China Organization, then you create a copy of:

- eCustomer Object Manager (ENU) and rename it (for example, eCustomer_China)
- Proxy Employee and rename it (for example, PROXYE_CHINA)

You then assign the modified proxy employee (PROXYE_CHINA) to a position in the China Organization. This results in the application (http://WebServer/eCustomer_China) connecting to the China Organization because PROXYE_CHINA is associated with a position in this organization.

For more information on the proxy employee, see "Seed Employee" on page 383.

To register a new customer user (by a delegated administrator)

1 Log into a Siebel customer application that implements delegated administration, such as Siebel Sales or Siebel eService.

NOTE: The delegated administrator must have user type Web Delegated Customer Admin.

2 Click My Account, and then click User Administration under My Company.

Lists of delegated accounts and associated users appear.

3 In the Delegated Accounts list, select the account with which you want to associate the new user.

The users in this account appear in the Users list.

4 Create a new record.

5 Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Responsibility	Pick one or more responsibilities, such as a seed responsibility provided for contact users. If the delegated administrator who creates this user has a value in the New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "Modifying the New Responsibility for a User Record" on page 247.
Home Phone # Work Phone # Work Fax #	The application interprets digits only in these telephone number entries. Any separators are disregarded.

The new record appears in the Users list.

Related Topic

"Delegated Administration of Users" on page 248

Registering Partner Users (Delegated Administration)

A delegated administrator using a partner application, such as Siebel Partner Portal, has a position in a partner division. The delegated administrator can only assign to a new partner user a position from those included in the partner organization to which the partner division belongs.

A partner user must have a position in a partner organization to be associated with that organization or to belong to position-based teams, such as opportunity or account teams. A delegated administrator in a partner company can assign a position to a new partner user from the following sources:

- Positions that you create internally and associate with the delegated administrator's partner organization
- Positions created by delegated administrators in the partner organization

A delegated administrator can only assign responsibilities to partner users whom your host company associates with the delegated administrator's partner organization. An administrator at your company associates partner organizations with responsibilities using an employee application such as Siebel Partner Manager. To provide a new partner user with access to the database, a delegated administrator must assign a responsibility when registering the partner user.

To register a new partner user (by a delegated administrator)

1. Log into a partner application that implements delegated administration, such as Siebel Partner Portal.

   NOTE: The delegated administrator must have user type Web Delegated Customer Admin.

2. Navigate to the Administration screen.
3. In the Explorer, expand the organization in which you will create the partner user.
4. Click the Users child item to display the users in this organization.
5. In the Edit User form, create a new record to add a new user. Complete the following fields, then save the record. Use the indicated guidelines.

Field	Guideline
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.

Field	Guideline
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP or ADSI security adapter authentication, the password is propagated to the user directory. For database authentication, the password is propagated to the database.
Position	If you assign multiple positions, then the position you specify as Primary is the position the partner user assumes when he or she logs in.
Responsibility	Pick one or more responsibilities, such as a seed responsibility provided for partner users. If the delegated administrator who creates this user has a value in the New Responsibility field, then that responsibility is assigned to this user by default. For information about the New Responsibility field, see "Modifying the New Responsibility for a User Record" on page 247.
Work Phone # Home Phone # Work Fax # Pager #	The application interprets digits only in these telephone number entries. The user can enter any separators.

The new partner user record appears in the Users list.

Related Topic

"Delegated Administration of Users" on page 248

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:

- "Editing Personal Information" on page 254
- "Changing a Password" on page 254
- "Changing the Active or Primary Position" on page 255

Profile forms, names, and navigation paths differ somewhat across Siebel Business Applications. The procedures in these topic are representative of those in Siebel employee, partner, and customer applications. Procedures in individual applications might 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. The following procedure describes how to edit personal information.

To edit personal information

1. Depending on the application, the user does one of the following:
   - In a Siebel customer application, the user clicks My Account, and then clicks User Profile under My Settings. The User Profile form appears.
   - In a Siebel partner application, the user clicks Profile. The Personal Profile form appears.
   - In a Siebel employee application, the user navigates to the User Preferences screen, then the Profile view. The User Profile form appears.
2. The user clicks Edit to make the form fields editable, if necessary.
3. The user enters or changes data in editable fields, then saves the record.

Related Topic

"Maintaining a User Profile" on page 253

Changing a Password

If you implement database or security adapter authentication, then a user can change the login password.

NOTE: If you want to implement similar functionality in a Web SSO authentication environment, then 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 Business Applications documentation.

To change a password, a user accesses the profile form as described in "Editing Personal Information" on page 254, and then completes the appropriate fields. The password-related fields are not editable if the password cannot be changed in the current authentication architecture.

Mobile users using the Siebel Mobile Web Client can also change their passwords for the local database and for synchronization. For details, see *Siebel Remote and Replication Manager Administration Guide*.

Related Topic

"Maintaining a User Profile" on page 253

Changing the Active or Primary 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. If users are associated with more than one position, then they have visibility to all the records associated with any of the catalogs that are 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.

Changing the Active Position in a Siebel Employee Application

The following procedure describes how to change the active position in a Siebel employee application.

To change the active position in a Siebel employee application

1. Navigate to the User Preferences screen, then the Change Position view.

   The Change Position list appears.

2. Click on a position record to select it, and then click Change Position.

   A check appears in the Active Position field for the selected position.

Changing the Primary Position in a Siebel Partner Application

A partner user can change the primary position as described in the following procedure. 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.

Related Topic

"Maintaining a User Profile" on page 253

9 Configuring Access Control

This chapter outlines the mechanisms provided by Siebel CRM to control access to data and Siebel application functionality by users once they have accessed a Siebel application and been authenticated. It includes the following topics:

- About Access Control on page 258
- Access Control Mechanisms on page 266
- Planning for Access Control on page 276
- Setting Up Divisions, Organizations, Positions, and Responsibilities on page 283
- About View and Data Access Control on page 285
- Listing the Views in an Application on page 286
- Responsibilities and Access Control on page 287
- Viewing Business Component View Modes on page 291
- Configuring Access to Business Components from Scripting Interfaces on page 295
- Viewing an Applet's Access Control Properties on page 297
- Listing View Access Control Properties on page 299
- Example of Flexible View Construction on page 302
- About Implementing Access-Group Access Control on page 304
- Implementing Access-Group Access Control on page 308
- Managing Tab Layouts Through Responsibilities on page 315
- Managing Tasks Through Responsibilities on page 319
- Administering Access Control for Business Services on page 321
- Administering Access Control for Business Processes on page 327
- Clearing Cached Responsibilities on page 327
- About Configuring Visibility of Pop-Up and Pick Applets on page 328
- About Configuring Drilldown Visibility on page 330
- Party Data Model on page 332

About Access Control

Access control is the term used to describe the set of Siebel application mechanisms that control user access to data and application functionality. As you work with this chapter, determine how the terminology and concepts presented here correspond to your company's internal terminology and structure. This chapter explains the Siebel access mechanisms, but you have to decide during the planning stage how to combine the mechanisms to meet your business and security needs.

In Siebel application terms, a screen represents a broad area of functionality, such as working on accounts. The set of screens to which a user has access is determined by the applications that your company has purchased. Each screen is represented as a tab at the top of the window. In the example below, the Accounts screen is displayed.

Each screen contains multiple views to provide different kinds of access to the data. To the user, a view is simply a Web page. Within a view, the user might see lists of data records or forms, presenting individual or multiple records, and sometimes child records. (These lists and forms are referred to as applets in a configuration context.) Each view (or grouping of views) is represented by text in the link bar below the screen tabs.

For example, Figure 5 shows the Account List View, which corresponds to the applet title My Accounts (the current visibility filter selection). Multiple view modes provide access to different views that filter the data differently. In the Account List View, the current user can view accounts owned or assigned to this user. Choosing All Accounts from the visibility filter displays the All Account List View instead, assuming the user has access to this view.

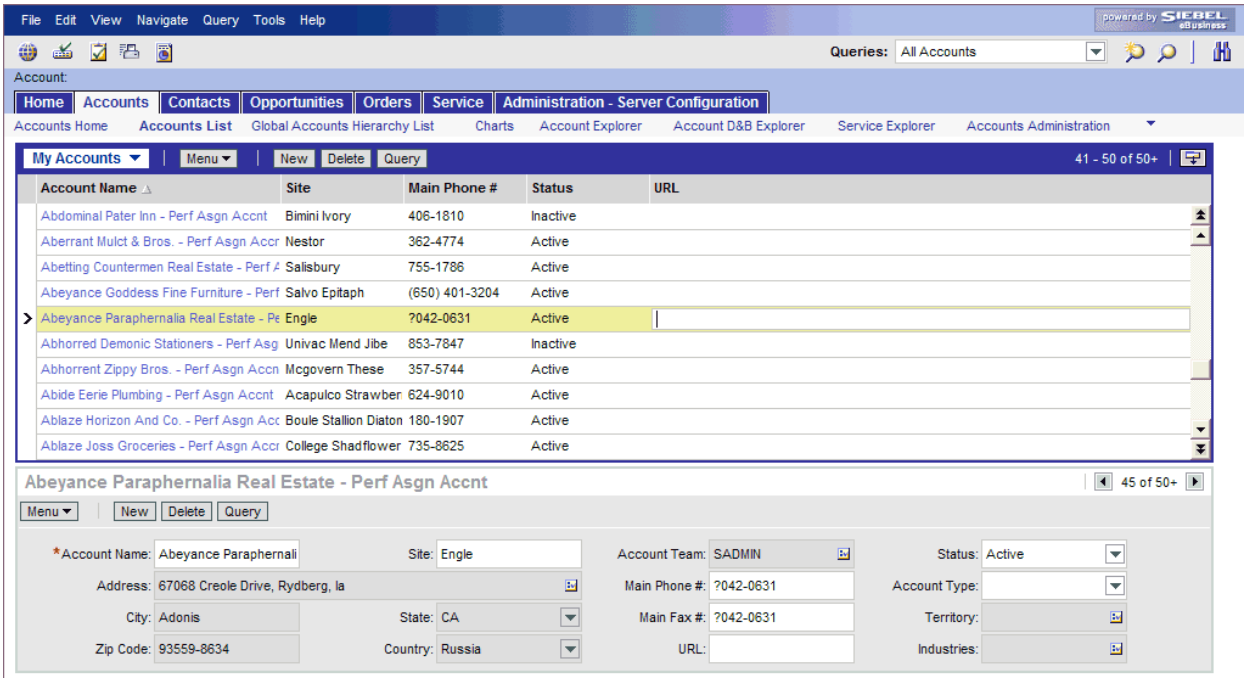

Figure 5. My Accounts View

To control the resources and privileges that users are entitled to once they have accessed a Siebel application and have been authenticated, Siebel CRM provides the following access-control elements:

- **View-level access control.** A screen is composed of views, and the collection of views to which users have access determines the application functionality available to them. Access to views is determined by responsibilities.

  Organizations are generally arranged around job functions, with employees being assigned one or more functions. In Siebel CRM, these job functions are called responsibilities. Each responsibility is associated with one or more views, which represent data and functionality needed for a job function. Each user must be assigned at least one responsibility to access the Siebel application.

  Siebel Business Applications ship with many predefined responsibilities and you can also define any additional responsibilities you require. For additional information, see "Responsibilities and Access Control" on page 287.

- **Record-level access control.** Record-level access control is used to assign permissions to individual data items within an application so that only authenticated users who need to view particular data records have access to that information. You can control the data records that each user can see through a variety of mechanisms, including direct record ownership by a user (personal access control) or being on the same team as the record owner (team access control). The following topics examine access control further:

  - "Access Control for Parties" on page 260
  - "Access Control for Data" on page 264

- **Business Components and Data Access.** Within Siebel CRM, views are based on business components and must use one of the view modes specified for the business component. A business component's view mode determines the record-level access control mechanisms that can be applied to the business component in any view. Applet and view properties also determine the data available in a view. For additional information, see "About View and Data Access Control" on page 285.

Figure 6 illustrates the Siebel access control elements. As shown in the figure, responsibilities provide access to views, and the data records visible to a user on a view are determined by the type of access control that applies to the data, the business component view mode, and view and applet visibility properties.

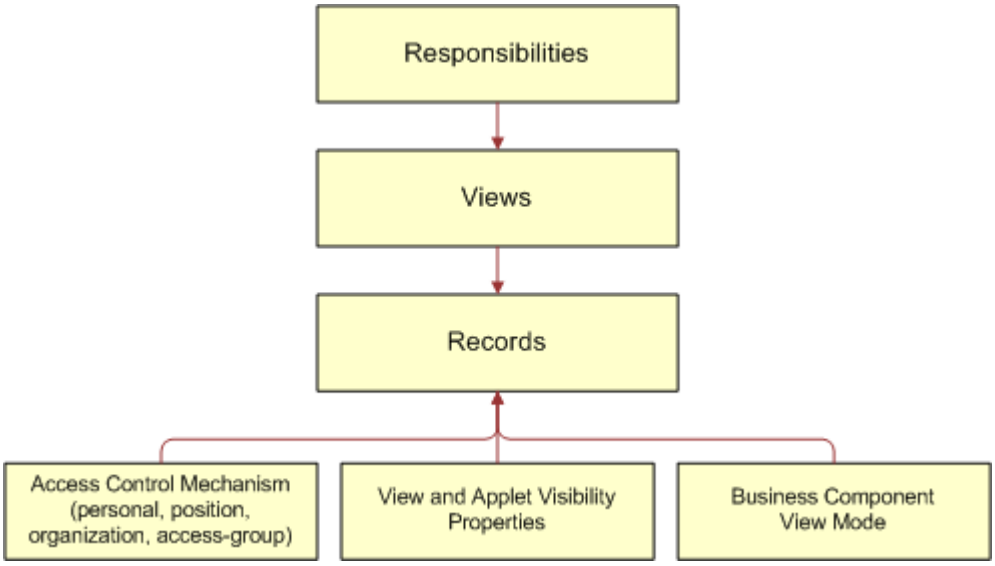

Figure 6. Siebel Business Applications Access Control Elements

Access Control for Parties

Individual people, groupings of people, and entities that represent people or groups are unified in the common notion of *parties.* Different party types have different access control mechanisms available.

NOTE: For technical information about how parties function at the data model level, see “Party Data Model” on page 332.

Parties are categorized into the following party types: Person, Position, Organization, Household, User List, and Access Group. Table 24 on page 261 describes the qualitative differences among different parties and identifies the applicable party type for each party.

Table 24. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Person (or Contact)	Person	■ An employee at a customer company. ■ An employee at a competitor's company.	■ A Person is an individual who is represented by a Person record in the database. ■ Without additional attributes, a Person has no access to your database.
User	Person	■ A registered customer on your Web site. ■ A self-registered partner user, that is, one who has no position.	■ A User is a Person who can log into your database and has a responsibility that defines what application views are accessible. ■ A self-registered partner on a Siebel partner application has a responsibility, but does not have a position like a full Partner User has.
Employee	Person	An employee at your company.	■ An Employee is a User who is associated with a position in a division within your company.
Partner User	Person	An employee at a partner company.	■ A Partner User is a User who is associated with a position in a division within an external organization. Therefore, a Partner User is also an Employee, but not an internal one.

Table 24. Party Types and Parties

Party	Party Type	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 can have a parent position. It can also have child positions. ■ One or more employees can be associated with an internal position, and one or more partner users can be associated with an external position. ■ An employee or partner user can be associated with more than one position, but only one position is active at any time.
Account	Organization	A company or group of individuals with whom you do business.	■ An account is typically made up of contacts. ■ An account is not a division, an internal organization, or an external organization. ■ An account can have a parent account. It can also have child accounts. ■ An account can be promoted to a partner organization.

Table 24. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
Division	Organization	■ An organizational unit within your company such as Manufacturing or Corporate. ■ A group of people operating within a particular country.	■ A division exists for the purposes of mapping a company's physical structure into the Siebel database and for providing a container for position hierarchies. ■ A division can have a parent division. It can also have child divisions. ■ Data cannot be associated directly with a division. (Divisions that are not designated as organizations do not drive visibility.)
Organization	Organization	■ An organizational unit within your company, such as your European organization. Countries are not units of access control in Siebel Business Applications; use organizations to manage access control for specific groupings of countries. ■ A partner company.	■ An organization is a division that is designated as an organization. ■ An organization exists for the purpose of providing a container in which positions can be associated with data. ■ An organization can be internal or it can be a partner organization. ■ A division can be associated with only one organization: itself or an ancestor division that is also an organization.
Household	Household	■ A group of people, typically a family, who reside at the same residence. ■ A group of purchasers who live in different residences.	■ Typically, a household is a group of individual consumers who are economically affiliated and share a common purchasing or service interest. ■ A household can have any combination of contacts, users, employees, and partner users as members. ■ An individual can belong to more than one household.

Table 24. Party Types and Parties

Party	Party Type	Examples	Distinguishing Features
User List	User List	■ A support team made up of some internal employees and some partner users.	■ A user list is a group of people. It can have any combination of contacts, users, employees, and partner users as members. ■ A user list cannot have a parent or children.
Access Group	Access Group	■ Your partner IT service providers and business-to-business customer companies that buy networking equipment. ■ A partner community, such as the resellers of a particular sector of your product line.	■ An access group is a group of any combination of parties of type Position, Organization, and User List. That is, it is a group of groups. ■ An access group can have a parent access group. It can also have child access groups.

Related Topic

"About Access Control" on page 258

Access Control for Data

The type of data and whether the data is categorized determines which access control mechanisms can be applied. The following groupings of data are necessary for the purpose of discussing access control:

- **Customer data**
  - Customer data includes contacts and transactional data such as opportunities, orders, quotes, service requests, and accounts.
  - Access is controlled at the data item level, through a mechanism such as individual record ownership or ownership by an organization.
- **Master data**
  - Master data includes the following referential data: products, literature, solutions, resolution items, decision issues, events, training courses, and competitors.
  - Master data can be grouped into categories of similar items, for example, hard drives. Categories can then be organized into catalogs, for example, computer hardware, which are hierarchies of categories. Access can be controlled at the catalog and category levels through access groups, which is the recommended strategy for controlling access to master data. For more information about creating catalogs, see *Siebel eSales Administration Guide*.

- Master data can be associated with organizations. By associating master data with organizations, access can be controlled at the data item level. This strategy requires more administration than the access group strategy.

  NOTE: Divisions provide a way to logically group positions and assign currencies. Organizations provide a mechanism to control data access.

- **Other data**
  - Other data includes referential data that is not master data, such as price lists, cost lists, rate lists, and SmartScripts.
  - Access is controlled at the data item level.

Data Categorization for Master Data

Master data can be organized into catalogs made up of hierarchical categories. Organizing data this way serves two purposes:

- **Ease of navigation.** Categorized data is easier to navigate and search. For example, it is easy to find products of interest in a product catalog organized by product lines and subgroups of related products. For example: Computer Hardware, Hard Drives, and then Server Drives.
- **Access control.** Access to catalogs and categories of master data can be granted to collections of users. This is an efficient means to control data access in given business scenarios. For example, you can control partner users' access to your internal literature.

You can categorize master data to represent hierarchical structures, such as product catalogs, geographical categories, service entitlement levels, training subject areas, or channel partners. A catalog is a single hierarchy of categories, as illustrated in Figure 7.

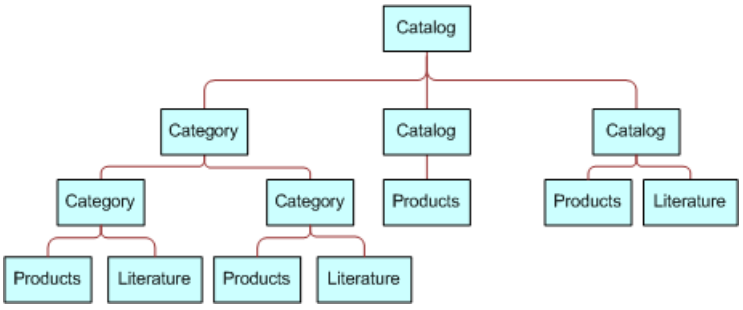

Figure 7. Example Category Hierarchy

The following properties apply to catalogs and categories:

- A catalog is a collection or hierarchy of categories.
- Individual data items are contained in categories.
- A category can contain one or more types of master data.
- A category can be a node in only one catalog.
- A data item can exist in one or more categories, in one or more catalogs.

- A catalog can be public or private. If it is private, then 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.

Related Topic

"About Access Control" on page 258

Access Control Mechanisms

The major access control mechanisms include the following, which are described in the topics that follow:

- **Personal access control.** For details, see "About Personal Access Control" on page 266.
- **Position access control.** This includes single-position, team, and manager access control. For details, see:
  - "About Position Access Control" on page 267
  - "About Single-Position Access Control" on page 268
  - "About Team (Multiple-Position) Access Control" on page 268
  - "About Manager Access Control" on page 269
- **Organization access control.** This includes single-organization, multiple-organization, and suborganization access control. For details, see:
  - "About Organization Access Control" on page 271
  - "About Single-Organization and Multiple-Organization Access Control" on page 271
  - "About Suborganization Access Control" on page 273
- **All access control.** For details, see "About All Access Control" on page 274.
- **Access-group access control.** For details, see "About Access-Group Access Control" on page 275.

About Personal Access Control

If individual data can be associated with a user's Person record in the database, then you can restrict access to that data to that person only. Typically, you can implement personal access control when data has a creator or a person is assigned to the data, usually as the owner. The following are some examples:

- In the My Service Requests view, a Web site visitor can only see the service requests he or she has created.
- In the My Expense Reports view, an employee can see only the expense reports the employee has submitted for reimbursement.
- In the My Activities view, a user can see only the activities the user owns.

Some views that apply personal access control are My Activities, My Personal Contacts, My Change Requests, and My Service Requests. The words *My* and *My Personal* are frequently in the titles of views that apply personal access control. However, *My* does not always imply personal access control. Some *My* views apply position or organization access control. For example, the My Opportunities view applies position access control.

Related Topic

"Access Control Mechanisms" on page 266

About Position Access Control

A position is a job title in a division of an internal or partner organization. A position hierarchy represents reporting relationships among positions. Positions provide an appropriate basis for access control in many scenarios, because a position in an organization is typically more stable than the individual's assignment to the position.

Customer data and some types of referential data can be associated with one or more positions. If individual data can be associated with a position, then you can apply position access control to the data by one or more of the following means:

- **Single-position access control.** You can associate a single position to individual data records. For details, see "About Single-Position Access Control" on page 268.
- **Team access control.** You can associate multiple positions, in the form of a team, to individual data. For details, see "About Team (Multiple-Position) Access Control" on page 268.
- **Manager access control.** You can grant access concurrently to data associated with a position and data associated with subordinate positions in a reporting hierarchy. For details, see "About Manager Access Control" on page 269.

An employee or partner user can be associated with one or more positions, of which only one can be the active position at a given time. All types of position access control for an employee or partner user are determined by the active position.

One of the user's positions is designated as the primary position. When a user logs in, the primary position is the active position. To make a different position the active position, one of the following must happen:

- An employee must designate another position as the active position, from the User Preferences screen.
- A partner user must designate another position as the primary position, and then log in again.
- You can configure an agent who uses Siebel CTI to automatically change positions based on the data provided for an incoming call.

  For information about Siebel CTI and related modules, and about setting up agents, see *Siebel CTI Administration Guide*.

Related Topic

"Access Control Mechanisms" on page 266

About Single-Position Access Control

You can associate a single position to individual data. For example, in the My Quotes view, an employee logged in using a particular position can see only the quotes associated with that position. Another view that applies single-position access control is My Forecasts.

The word *My* is frequently in the titles of views applying single-position access control. However, *My* does not always imply single-position access control. Some *My* views apply personal, organization, or team access control. For example, the My Activities view applies personal access control.

A business component's view modes determine whether single-position access control can be applied in a view that is based on the business component. To have single-position access control available, a business component must have a view mode (usually Sales Rep) of owner type Position with an entry in the Visibility Field column (instead of the Visibility MVField column). For information about business component view modes, see "Viewing Business Component View Modes" on page 291. For information about implementing access control in a view, see "Listing View Access Control Properties" on page 299.

Related Topic

"Access Control Mechanisms" on page 266

About Team (Multiple-Position) Access Control

You can associate multiple positions, in the form of a team, to individual data. For example, in the My Opportunities view, an internal employee or partner with a particular active position can see all the opportunities for which that position is included in the opportunity's sales team. A team can include internal and partner positions.

The display names for fields representing position teams vary with the view in which they appear. Some common views that apply team access control follow, with the display names for the field representing the team:

- The My Opportunities view has a Sales Team field.
- The My Accounts view has an Account Team field.
- The My Contacts view has a Contact Team field.
- The My Projects view has an Access List field.

Although the field for the team can contain multiple positions, only one name is displayed without drilling down. In a view that uses team access control, for example My Projects, the name of the active login is displayed. Other views, such as those using organization access control, can also have a field for the team. In these other views, the name of the login that occupies the primary position is displayed.

The word *My* is frequently in the titles of views applying team access control. However, *My* does not always imply team access control. Some *My* views apply personal, organization, or single-position access control. For example, the My Activities view applies personal access control.

A business component's view modes determine whether team access control can be applied in a view that is based on the business component. To have team access control available, a business component must have a view mode (usually Sales Rep) of owner type Position with entries in the Visibility MVField and Visibility MVLink columns (instead of the Visibility Field column). One of a team's members is designated as the primary member. The primary member is a factor in manager access control, but not in team access control.

If a business component is configured for team access control, any new record added for that type of component follows this rule: the user who created the record is added to the record's team and is set to be the primary. For information about business component view modes, see "Viewing Business Component View Modes" on page 291. For information about implementing access control in a view, see "Listing View Access Control Properties" on page 299.

Related Topic

"Access Control Mechanisms" on page 266

About Manager Access Control

You can indirectly associate a position with data associated with subordinate positions in a reporting hierarchy. For example, in the My Team's Opportunities view, an employee with a particular active position can see opportunities associated with that position and opportunities associated with subordinate positions.

Manager-subordinate relationships are determined from a position hierarchy. One position hierarchy is included as seed data when you install your Siebel application. You can specify one parent position for a position, which represents that the position is a direct report to the parent. The parent of an internal position can be in the same division or a different division. For example, a sales manager in the Sales division can report to a sales vice president in the Corporate division.

In a view using manager access control, an employee or partner user has access to data according to the behavior outlined in the following topics.

Business Component Uses Position Access Control

If a view uses manager access control, and if the business component on which the view is based uses position access control, then the following behavior applies:

- If the business component on which the view is based uses single-position access control, then the user sees data associated directly with the user's active position or with subordinate positions.

- If the business component on which the view is based uses team access control, then the user sees data for which the user's active position is on the team or any subordinate position that is the primary member on the team. This is the standard behavior, known as primary manager visibility.

  A business component using team access control can be configured to allow the user to see data for all subordinate positions, regardless of whether they are the primary position for a record. This is known as nonprimary manager visibility.

  To configure nonprimary manager visibility, define a user property called Manager List Mode for the business component and set it to Team (rather than the default value of Primary). For more information about the Manager List Mode user property, see *Siebel Developer's Reference*.

  CAUTION: Configuring nonprimary manager visibility to support mobile users requires changes to docking visibility rules. Customers who require this functionality must engage Oracle's Advanced Customer Services. Contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.

NOTE: The value of the Visibility Applet Type field determines the access control properties that apply to a view. However, if a more restrictive value is specified for the Visibility Applet Type field for another view that is based on the same business component, then the restrictions of this visibility type are applied to both views. For example, if two views are based on the same business component, and if Manager visibility is selected for one view and Sales Rep Visibility is selected for the other view, then the restrictions of the Sales Rep Visibility type are also applied to the user's active position or team positions on the view that has implemented Manager access control. As a result, the user does not have access to data associated with subordinates' positions.

Business Component Uses Personal Access Control

If a view uses manager access control, and if the business component on which the view is based uses personal access control, then the behavior is as follows:

- For single-owner access control, the user sees data associated directly with the user's active position or with subordinate positions.
- For multiple-owner access control, the user sees data for which the user's active position is on the team, or any subordinate position that is the primary member of the team.

Views that apply manager access control generally contain the phrase *My Team's* in the title, such as My Team's Accounts. (In some cases, the word *My* is omitted.) There are no business component view modes specific to manager access control. Manager access control is set at the view level. It requires that the business component on which the view is based has a view mode with owner type Position or Person.

NOTE: In a view using manager access control, if the manager user has no subordinate positions defined, then the user cannot create new records in the view. The New button and the New Record command are unavailable.

Related Topics

"Viewing Business Component View Modes" on page 291

"Access Control Mechanisms" on page 266

"Listing View Access Control Properties" on page 299

About Organization Access Control

When individual data can be associated with an organization, you can apply organization access control to the data by one or more of the following means:

- **Single-organization access control.** You can associate a single organization with individual data. For details, see "About Single-Organization and Multiple-Organization Access Control" on page 271.
- **Multiple-organization access control.** You can associate multiple organizations with individual data. For details, see "About Single-Organization and Multiple-Organization Access Control" on page 271.
- **Suborganization access control.** You can grant access concurrently to data associated with an organization and data associated with subordinate organizations in the organizational hierarchy. For details, see "About Suborganization Access Control" on page 273.

NOTE: Siebel Assignment Manager is also organization-enabled; that is, assignment rules can use organization as a criterion.

A user is associated with one organization at any given time, the organization to which the user's active position belongs. For information about changing the active position of an employee or a partner user, see "About Position Access Control" on page 267.

A contact user is indirectly associated with an organization through the proxy employee specified for a Siebel customer application. For information about proxy employees, see Chapter 5, "Security Adapter Authentication," and "Seed Data" on page 383.

Related Topic

"Access Control Mechanisms" on page 266

About 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 25 on page 272 lists data on which you can apply organization access control and indicates, for some of the most commonly used Siebel objects, whether a single organization, or multiple organizations, can be associated with the data.

Table 25. Data Enabled for Organization Access Control

Object Type	Object	Relationship
Customer data	Account	Multiple
	Competitor	Multiple
	Contact	Multiple
	Forecast Series	Multiple
	Household	Multiple
	Marketing Event/Activity	Multiple
	Opportunity	Multiple
	Order	Multiple
	Partner	Multiple
	Product Defect	Multiple
	Project	Multiple
	Quote	Multiple
	Service Request	Multiple
	User List	Multiple
Referential data (includes master data)	SmartScript	Multiple
	Literature	Multiple
	Price List	Multiple
	Cost List/Rate List	Multiple
	Period	Single
	Product	Multiple
	Catalog	Not Applicable (catalogs use access-group access control)
Administrative data	Employee	Multiple
	Division	Single
	List of Values Type	Multiple
	List of Values	Single
	Position	Single
	Responsibility	Multiple

NOTE: Customizable products that you create with Siebel Configurator include some exceptions to organizational access rules. For information about customizable product visibility, see *Siebel Product Administration Guide*.

All (but not *All across*) is frequently in the title of views applying single- or multiple-organization access control. For example, the All Contacts view applies single-organization access control, and the All Product Defects view applies multiple-organization access control. However, *All* does not always imply single- or multiple-organization access control. Some *All* views apply *All* access control. For example, the All Service Requests view applies *All* access control.

A business component's view modes determine whether single-organization or multiple-organization access control can be applied in a view that is based on the business component.

- To have single-organization access control available, a business component must have a view mode (typically Organization) of owner type Organization with an entry in the Visibility Field column (instead of the Visibility MVField column).
- To have multiple-organization access control available, a business component must have a view mode (typically Organization) of owner type Organization with entries in the Visibility MVField and Visibility MVLink columns (instead of the Visibility Field column).

For information about *All* access control, see "About All Access Control" on page 274. For information about business component view modes, see "Viewing Business Component View Modes" on page 291.

Related Topic

"Access Control Mechanisms" on page 266

About Suborganization Access Control

Suborganization access control, based on hierarchical organizations, is analogous to manager access control, which is based on hierarchical positions. For any organization in the organizational hierarchy, you can grant access to data associated with subordinate organizations. This access control mechanism is designed to provide rollup views of data.

For example, a director of a continental sales organization can see the data rolled up from subordinate regional sales organizations. A vice-president in the corporate sales organization can then see rollups of the continental sales organizations and the regional sales organizations. Subordinate relationships are determined from the organizational hierarchy, as an administrator can view by navigating to Administration - Group, and then 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.

Related Topics

"Access Control Mechanisms" on page 266

"Viewing Business Component View Modes" on page 291

About All Access Control

All access control provides access to all records that have a valid owner, as defined in any of the business component's view modes. The owner can be a person, a position, a valid primary position on a team, or an organization, depending on the view modes that are available for the business component.

All users with a view in their responsibilities that applies *All* access control see the same data in the view. A user's person or position need not be associated with the data.

All access control essentially provides a view of data across all organizations. For example, in the All Quotes across Organizations view, a user sees all the quotes that are associated with any internal or external organization in the Enterprise, for which there is a valid person, position or organization owner.

The phrases *All across* and *All* are frequently in the titles of views applying *All* access control. For example, the All Opportunities across Organizations and the All Service Requests views apply *All* access control. However, *All* does not always imply *All* access control. Some *All* views apply single-organization or multiple-organization access control. For example, the All Contacts view applies single-organization access control.

A separate property (Admin Mode) provides the means to see all records in a view using team access control, including those without a valid owner. Admin mode allows the administrator to modify records that otherwise no one could see. You specify Admin mode for a view in the Admin Mode Flag property.

There are no business component view modes specific to *All* access control. *All* access control is set at the view level.

Related Topics

"Access Control Mechanisms" on page 266

"Viewing Business Component View Modes" on page 291

About Access-Group Access Control

Access groups are used to control access to master data by diverse groups of party types. An access group is a collection of any combination of positions, organizations, account, households, and user lists. Its members are instances of party types other than Person; that is, its members cannot be individual people. For example, an access group could consist of several partner organizations and user lists to which you want to grant access to a particular set of your sales tools.

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. Although you can add divisions to access groups, doing so has no effect on visibility. Use organizations instead.

You can create hierarchies of access groups. An access group can belong to only one access group hierarchy. That is, an access group can have only one parent access group. For example, the access group mentioned above might belong to a hierarchy of access groups for the purpose of granting differing levels of access to sales tools.

You can grant access groups access to catalogs and categories of master data: products, literature, solutions, resolution items, decision issues, events, training courses, and competitors. For example, branches in the access group hierarchy above could be granted access to categories in a hierarchical catalog in which each category contains sales literature and decision issue items. For an illustration of an access group hierarchy (master data), see “Access Control for Data” on page 264.

A category of master data can contain any combination of master data items. You can only control access to catalogs and categories of master data. You cannot control access to individual master data items using access-group access control.

When access groups are associated with a catalog or with categories in the catalog, you can apply access-group access control. You can control access to the data in one of the following ways:

- **Group.** While in a given category, the user sees either a list of the category’s first-level subcategories (child categories) to which he or she has access or all the data records in the current category, depending on the applet being used. If the user is at the catalog level, the user sees the first-level categories.
- **Catalog.** The user sees a flat list of all the data in categories across all catalogs to which the user has access. This access control type is typically used in product picklists and other lists of products, such as a recommended product list.

Related Topics

“Access Control for Data” on page 264

“Access Control Mechanisms” on page 266

“About Implementing Access-Group Access Control” on page 304

Planning for Access Control

Two main strategies are available for controlling access to data in Siebel Business Applications:

- **Multiple-organization access control.** This strategy limits data access to only those organizations that have a need to see the information. Organizational access control can be implemented across internal or external organizations. This strategy can be applied to transaction data, master data, and other referential data. For more information, see "About Organization Access Control" on page 271.
- **Access-group access to catalogued data.** This strategy can be implemented with all party types. It is designed to reduce access control administration by associating hierarchical groups of users with similarly organized data. This strategy can be applied to master data only. For more information, see "About Access-Group Access Control" on page 275.

CAUTION: Configuring changes in access control for a Siebel application can be a complex task. Such changes can have significant implications for the entire application and can involve significant risks. For these reasons, it is recommended that you contact Oracle's Professional Services for a design review before undertaking any major modifications to access control in your Siebel application. Contact your Oracle sales representative to request assistance from Oracle's Professional Services.

For additional information on planning for access control, see the following topics:

- "Access Control and Business Environment Structure" on page 276
- "About Planning for Divisions" on page 278
- "About Planning for Organizations" on page 279
- "About Planning for Positions" on page 280
- "About Planning for Responsibilities" on page 282

Access Control and Business Environment Structure

As part of implementing an access control strategy for your application, you must define your company's structure, outside partner relationships, and so on. You also define the types of data and objects that people need to access and work with to perform their job functions. How you define the structure of your business environment directly impacts how access control applies to your users.

This topic provides some background information about business environment structure. If your enterprise is large and complex, you can accurately reflect its structure as you set up your Siebel Business Applications. You can build multilevel hierarchies of organizations, divisions, and positions. You build a hierarchy by associating positions, for example, with other positions through parent-child relationships.

Defining your business environment structure involves setting up the elements shown in Table 26.

Table 26. Elements of Business Environment Structure

Element	Parent-Child	Description
Divisions	Y	Subunits of your company's (or partner company's) organizations. Used to set default currencies. Not used to control visibility of data.
Organizations	Y	The major parts or entities that make up your company (or your partner companies). Used to control visibility of data. See "About Organization Access Control" on page 271.
Positions	Y	Control the data set (records) to which a user has access. See "About Position Access Control" on page 267.
Responsibilities	N	Control the views to which a user has access.
Employees	N	Individual users in your company and in partner companies who have access to your company's data.

You can set up divisions, organizations, positions, responsibilities, and employees in any order. You can also associate these types of records with one another in a variety of ways. For example, to link a responsibility and an employee, you can associate the employee with the responsibility from the responsibility record, or you can associate the responsibility with the employee from the employee record.

NOTE: Because organizations are based on divisions, it is recommended that you create your hierarchy of divisions first, and then determine which of these divisions to designate as organizations.

CAUTION: Changing your company structure, such as positions and divisions, can cause Siebel Remote components (Transaction Router) to reevaluate access control for all objects related to the objects that have changed. This can result in diminished performance. For more information, see *Siebel Remote and Replication Manager Administration Guide.*

Benefits of Multiple Organizations

Using organizations provides the following benefits:

- It allows your company to partition itself into logical groups, and then display information appropriate to each of those groups.
- It provides the ability to limit visibility (access) to data based on the organization to which positions are assigned.
- It affects both customer data (accounts, opportunities, service requests, and so on) and master data (price lists, literature, and so on).

- It allows you to assign skills to organizations, which allows Assignment Manager to make assignments based on organization.
- It allows you to set up multitenancy for call centers. For more information, see *Siebel CTI 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 might 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 might want to use organizations to support specific versions of a limited number of data entities such as products and price lists.
- **Complex global enterprise.** If you have a full-scale global enterprise that encompasses multiple internal and external businesses, each of which is made up of multiple business units, your company benefits from implementing organizations. In this circumstance, some data can be available only to some business units, while other information can be shared at the corporate level.
- **Internal and external units.** If your company shares data with external partner companies, you can set up each of these companies as an organization. You can make fewer views available to these external organizations than to your internal organizations. You can also configure the employee list so that it shows only employees who belong to the user's organization.
- **Different rules for business units.** If you would like to make different Siebel Assignment Manager or Siebel Workflow rules apply to different parts of your company, then your company benefits 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 who log in through a Web site, you can set up a customer organization to control their access to views and data. If you have channel partners who log in through a Web site, you set up channel partner organizations to control their access.

  For more information on using organizations with Siebel customer and partner applications, see *Siebel Partner Relationship Management Administration Guide*.

Related Topic

"Planning for Access Control" on page 276

About Planning for Divisions

This topic and those that follow explain the common tasks for defining a company structure in your Siebel application. These include tasks for defining divisions, organizations, responsibilities, and positions.

Divisions belong to organizations and have no direct effect on visibility. Divisions help you to group positions, to record addresses, and to maintain default currencies. User reporting structures are defined by their parent positions, but their country of operation and currency are defined by their division. To implement Siebel Business Applications, you must set up at least one division.

An organization can contain multiple divisions, but a given division can only be part of one organization. Organizations can be arranged into a hierarchy of parent organizations and suborganizations. You can also promote a division to an organization. Multiple divisions can be arranged in a multilevel hierarchy by assigning some divisions as the parents of others.

You can assign positions to a division. When you associate employees with those positions, the employees become associated with the division.

NOTE: You cannot delete or merge division records, because business components throughout your Siebel application refer to organization records. Deleting or merging a division would cause invalid references on transaction records. This would lead to unexpected negative results, such as valid data not appearing in the user interface.

Related Topics

"Planning for Access Control" on page 276

"About Planning for Organizations" on page 279

"About Planning for Positions" on page 280

"About Planning for Responsibilities" on page 282

About Planning for Organizations

Organizations are designed to represent the broadest divisions of your company. An organization controls the data access of the employees that are assigned to it. Organizations can be internal, or they can be external (in the case of Siebel Partner Relationship Manager).

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 might want to delegate administration of users to organizations that access only their users. To do this, you must configure the appropriate views using Siebel Tools. For more information on configuring views, see *Configuring Siebel Business Applications*.

The following are best practices for working with organizations:

- Merging organizations is not recommended. Because many business objects are configured for multiple-organization access control, you might disrupt these relationships to a significant extent and get unexpected results.

- It is recommended that you do not change the name of the default organization, which is Default Organization. This record is seed data that is referenced in many places. If your company decides to change the default organization name, the name must be unique from any other organization or division name. References to Default Organization in other locations must also be changed.

  For example, if you are using Siebel Assignment Manager, you might have to rename references in assignment objects to the new name for the default organization. For more information, see *Siebel Assignment Manager Administration Guide* and *Configuring Siebel Business Applications*.

NOTE: You cannot delete organization records. Business components throughout 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.

Related Topics

"Planning for Access Control" on page 276

"About Planning for Divisions" on page 278

"About Planning for Positions" on page 280

"About Planning for Responsibilities" on page 282

About Planning for Positions

A position represents a specific job slot within your company. As you define your company structure, define specific positions with each level in the hierarchy of divisions. Positions determine which records users have access to. You must be logged on to a server database to add positions.

Positions and Employees

An employee must have a position 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 can have multiple associated employees. One employee can be associated with multiple positions. There can be only one primary employee for a position, but an employee can be primary for more than one position.

There is a drawback to having multiple employees associated with a position. Because a position can have only one primary employee, only the primary employee is visible in the Employee field. If you search for an employee in a positions list, you might not find relevant position records in which the employee is not primary for the position.

Only the primary employee for a position appears in the Account Team, Opportunity Sales Team, and Contact Access lists. However, all the employees in that position can access the My Accounts, My Opportunities, and My Contacts views.

A position can be associated with only one organization. If you want an employee to have visibility to multiple organizations, you must create a position for each organization and assign that employee to each position. The employee can then see one organization's data at a time by changing positions.

Your Siebel application allows users to change their position to another position to which they have already been given access by the administrator. A user can change positions while logged in by choosing Tools, User Preferences, and then Change Position, selecting a different position in the list, and clicking the Change Position button. For instance, a sales representative can 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.

Position Administration

Positions can be set up in a multilevel hierarchy, which allows for manager access control. The parent position gains visibility to all the sets of data visible to the individual child positions. (Usually, the data is displayed only where the child position is the primary on the team or record.)

CAUTION: Do not delete a position. This can cause unexpected and negative results. For example, if you delete a position that is primary for an account, and you do not select a new primary position for that account, Assignment Manager might not be able to assign resources to activities for that account.

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.

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 Framework: Workflow Guide*.
- Enterprise Integration Manager (EIM), if you are referring to these positions in EIM import SQL scripts. For more information, see *Siebel Enterprise Integration Manager Administration Guide*.
- The Position field of the Employees view.

NOTE: If you change a mobile user's position, that user's visibility rules change. In this case, it is recommended that the user reextract his or her local database. However, if you change only the position name (for example, from Sales Representative to Sales Associate), then reextraction is not required because in the database table where position names are stored, this column has enterprise-wide visibility. In other words, changes to this column are distributed to all users.

Related Topics

"Planning for Access Control" on page 276

"About Planning for Divisions" on page 278

"About Planning for Organizations" on page 279

"About Planning for Responsibilities" on page 282

About Planning for Responsibilities

Responsibilities determine which views users have access to. For example, the System Administrator responsibility allows access to all views. Defining responsibilities lets you limit user access to views, and therefore to your Siebel application's information and functions. You must assign responsibilities to all users. Without a responsibility, a user cannot use the Siebel application, because that user cannot access any views.

You can also assign tab layouts and tasks to responsibilities. For more information, see "Managing Tab Layouts Through Responsibilities" on page 315 and "Managing Tasks Through Responsibilities" on page 319.

To define a responsibility, you must specify which views are available to that responsibility. It is recommended that you use the responsibilities that are provided as seed data, where applicable. These can be copied and then customized. Then define any additional responsibilities you require that correspond to the major job functions in your organization.

For example, you might use or create responsibilities for the marketing administrator, the sales manager, and sales representatives. The sales representative responsibility might have access to all views except those reserved for sales management, marketing administration, and applications administration. The sales manager responsibility might have access to the same views as the sales representative, plus the sales manager views, and so on.

As appropriate, you can specify that a view is read-only for a given responsibility.

NOTE: You cannot modify or delete the seed responsibilities. For instance, you cannot change the Siebel administrator responsibility. You can copy the seed responsibilities and modify the copies.

When you are defining responsibilities, consider the following issues:

- Grant access to the System Preferences view to only a selected group of administrators; do not give end users access to the System Preferences view. System preferences control many things throughout the Siebel system, including some server logic and processing for Siebel Remote and Siebel Assignment Manager.
- Do not add Administration views to responsibilities associated with end users. Likewise, limit access to the Master Forecasts, Mobile Web Clients, Responsibilities, Views, and Territories views. The work performed with these views has far-reaching implications for the entire application.
- Where users require access to data presented in a view, but do not need to create or modify data, specify that the view is read-only for this responsibility. (If any one responsibility for a user is associated with a view that is *not* marked with the Read Only View flag, the view will not be read-only for this user, regardless of how the flag is set for any other responsibility.)
- You might want to hide access to license keys by deleting the license key-related views from a user's responsibility. For more information about license keys, see *Siebel Applications Administration Guide*.
- If you add the Internal Division view to a user's responsibility, all organizations in the Organizational picklist are displayed. By default, only the organization the user belongs to appears in this picklist.
- If you log into the application through the normal Siebel Web Client, you can add new views to responsibilities in the Administration - Application, Responsibilities view.

Related Topics

"Planning for Access Control" on page 276

"About Planning for Divisions" on page 278

"About Planning for Organizations" on page 279

"About Planning for Positions" on page 280

Setting Up Divisions, Organizations, Positions, and Responsibilities

This topic outlines procedures for setting up divisions, organizations, positions, and responsibilities.

Setting Up Divisions

This topic describes how to set up divisions.

To set up a division

1 Navigate to the Administration - Group screen, then the Internal Divisions view.

The Internal Divisions view appears.

2 In the form, add a new record and complete the necessary fields.

Some fields are described in the following table.

Field	Guideline
Parent Division	If this division is a subdivision, select the parent division. This allows a division to be associated with another division.
Organization Type	Indicates the type of organization, which controls where in the application a division will appear for selection purposes. For example, divisions with Organization Type set to 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 division is copied into the Organization view.

Setting Up Organizations

This topic describes how to set up organizations.

To set up an organization

1 Navigate to the Administration - Group screen, then the Organizations view.

The Organizations view appears.

2 In the form, add a new record and complete the necessary fields.

Some fields are described in the following table.

Field	Guideline
Parent Organization	If this organization is a suborganization, select the parent organization. This allows an organization to be associated with another organization.
Partner Flag	Used for Siebel Partner Relationship Manager. This is a read-only check box. When the box is checked, this indicates that the organization represents an external enterprise that is a partner of your company. **NOTE:** Partners are registered and promoted to organizations using the Approved Partners view in the Administration - Partner screen, as described in *Developing and Deploying Siebel Business Applications*.

Setting Up Positions

This topic describes how to set up positions.

To set up a position

1 Navigate to the Administration - Group screen, then the Positions view.

The Positions view appears.

2 In the form, add a new record and complete the necessary fields.

Some fields are described in the following table.

NOTE: Most fields in the form are filled in automatically from the Employee record of the active employee. If you have not set up employees, you can associate them with positions later.

Field	Guideline
End Date	Last day for the currently associated employee to be associated with this position.
Last Name	Select one or more employees to occupy the position. In the Assigned Employees dialog box, select the Primary field for the employee whom you want to make primary for this position.
Parent Position	If this position is a subposition, select the parent position. This allows a position to be associated with another position.
Position Type	Type of position. This field is informational and has no impact on visibility.
Territory	This field is a read-only multi-value group. You are not able to enter a value manually. For use by Siebel Assignment Manager.

Setting Up Responsibilities and Adding Views and Users

This topic describes how to set up responsibilities and add views and users.

To define a responsibility and add views and users

1 Navigate to the Administration - Application screen, then the Responsibilities view.

The Responsibilities view appears.

NOTE: By default, the Responsibilities view shows all responsibilities, regardless of organization. However, you might want to configure new views in Siebel Tools that restrict the visibility to responsibilities. For more information on configuring views, see *Configuring Siebel Business Applications*.

2 In the Responsibilities list, add a new record and enter a name and description for the responsibility.

3 In the Organization field, select an organization for the responsibility.

4 To add views, do the following:

a In the Views list, add a new record.

b Select the appropriate views in the Add Views dialog box and click OK.

When you add a view, set the flag Read Only View if users with this responsibility only require read access to the view.

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.

Related Topic

"About View and Data Access Control" on page 285

About View and Data Access Control

The particular data displayed in a view and whether a view is displayed at all are determined by settings made for related components. You configure most of these settings in Siebel Tools. This topic specifies where to find these settings within Siebel Tools, but in most cases does not provide procedures to implement them. Changing any settings in Siebel Tools requires recompiling the Siebel repository file. For more information about required practices when using Siebel Tools, see *Configuring Siebel Business Applications* and *Using Siebel Tools*.

The following components determine what views a user sees:

- **Application.** Each Siebel application includes a licensed set of views. When a user is in an application, the user has no access to views that are not included in the application. For additional information on application views, see "Listing the Views in an Application" on page 286.
- **Responsibilities.** Every user has one or more responsibilities, which define the collection of views to which the user has access. If a particular view is not in a user's responsibilities, then the user does not see that view. A wide-ranging view such as All Opportunities Across Organizations is not typically included in the responsibility for an employee such as a district sales representative. For additional information on responsibilities, see "Responsibilities and Access Control" on page 287.

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; these include 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 is determined, for example *owned by* or *created by*. For additional information on business component view mode, see "Viewing Business Component View Modes" on page 291.
- **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. For additional information on applet visibility properties, see "Viewing an Applet's Access Control Properties" on page 297.
- **View visibility properties.** A view's visibility properties determines the access control mechanism that is applied to the business component on which the view is based. For example, the business component might have personal or position access control available. The view specifies which of these to use, and in which form to use it. For additional information on view visibility properties, see "Listing View Access Control Properties" on page 299.

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. For an example of how the visibility applet specified for a view determines the type of data access control that applies to the view, see "Example of Flexible View Construction" on page 302.

Listing the Views in an Application

This topic describes how to list the views that are included in your Siebel application.

Each Siebel application is associated with a set of screens. Each screen is in turn made up of a set of views. In a particular application, all users are limited to the views that are licensed to your company and that are defined for the application. The licensed views are specified in the license key, which is determined by the features you purchase for your Siebel Business Applications.

To see which views an application includes

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, then the Views view.

   The views defined for an application are listed.

Related Topic

"About View and Data Access Control" on page 285

Responsibilities and Access Control

A responsibility corresponds to a set of views. Each user must be assigned at least one responsibility. When you assign responsibilities to a user, the user has access to all the views contained in all of the responsibilities assigned to the user and that are also included in the user's current application.

If a view in an application is not included in a user's responsibilities, the user will not see the view or a listing of the view in the Site Map, in the link bar, or in any other picklist. If the user does not have access to any of the views in a screen, then that screen's listing in the Site Map and its screen tab are not displayed.

For example, the responsibility assigned to an administrator might include the views in the Administration - Application screen. The administrator sees this screen listed in the Site Map and can navigate to the views it includes. A customer care agent typically does not have administrative views in a responsibility, so the agent would not see this screen or its views listed in any context.

Each user's primary responsibility also controls the default screen or view tab layout for the user. For more information, see "Managing Tab Layouts Through Responsibilities" on page 315.

A user can have one or more responsibilities. The user has access to all the views in the union of all the responsibilities assigned. For example, you could assign a sales manager both the Sales Manager responsibility and the Field Sales Representative responsibility.

NOTE: Modifying visibility or responsibility settings for an application can in some cases require that the associated Application Object Manager (AOM) be restarted in order for these new settings to take effect for users of the Siebel Web Client. If you have only modified responsibilities, then you can clear cached responsibilities instead, without restarting the Application Object Manager. For more information, see "Clearing Cached Responsibilities" on page 327.

For additional information on using responsibilities to provide access control, see the following topics:

- "About Associating a Responsibility with Organizations" on page 288
- "Local Access for Views and Responsibilities" on page 288
- "Read Only View for Responsibilities" on page 289
- "Assigning a Responsibility to a Person" on page 289
- "Using Responsibilities to Allow Limited Access to Server Administration Views" on page 290

About Associating a Responsibility with Organizations

You can associate a responsibility with one or more organizations. Associate responsibilities with organizations only when you are implementing delegated administration of users, such as for Siebel Partner Portal (for Siebel Partner Relationship Manager).

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 can 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: Associate each responsibility with at least one organization if you include views that use either position or organization access control in the responsibility.

Related Topic

"Responsibilities and Access Control" on page 287

Local Access for Views and Responsibilities

Each view and each responsibility has a Local Access flag. Together, these settings determine whether views can be accessed by Siebel Mobile Web Client users with particular responsibilities.

The setting of the Local Access flag does not affect access to a view for users using either the Siebel Web Client or Siebel Developer Web Client.

When Local Access is set to TRUE (checked), all users with the view in one of their responsibilities can access the view when using the Siebel Mobile Web Client (connected to the local database). When Local Access is set to FALSE (unchecked), users cannot access the view when using the Mobile Web Client.

The Local Access flag appears in the following locations:

- Default Local Access flag in Administration - Application, Views. This setting defines a default setting to be inherited for the view, unless the setting is overridden in another context.
- Local Access flag in Views list of Administration - Application, Responsibilities. This setting displays or overrides the default setting applicable to a view record that is a child to the current responsibility. The setting affects a view only as it is made available to users through association with a specific responsibility record.

- Local Access flag in Responsibilities list of Administration - Application, Views. This setting displays or overrides the default setting applicable to the view record that is the parent to the current responsibility. The setting affects a view only as it is made available through association with a specific responsibility record.

The Local Access field is a mechanism for controlling which views mobile users can work in when using the Siebel Mobile Web Client. In addition to enabling or disabling local access to views based on responsibility, administrators can provide different sets of views for access by different mobile users. For more information, see *Siebel Remote and Replication Manager Administration Guide*.

CAUTION: Disable access to views applying All access control by setting the Local Access field to FALSE. A view with All access control can cause unpredictable and possibly undesirable results for a mobile user. For information about All access control, see "About All Access Control" on page 274.

Related Topic

"Responsibilities and Access Control" on page 287

Read Only View for Responsibilities

Each responsibility has a Read Only View flag. Set this flag to True to prevent a user from creating data in a view or modifying existing data in a view. To make sure that a user cannot create or modify data in a view, you must select this flag for all responsibilities associated with the user that allow access to the view.

The Read Only View flag appears in the following locations:

- Read Only View flag in Views list under Site Map, Administration - Application, Responsibilities, and then Responsibilities.
- Read Only View flag in Responsibilities list under Site Map, Administration - Application, Views, and then Responsibilities.

Related Topic

"Responsibilities and Access Control" on page 287

Assigning a Responsibility to a Person

You can add a responsibility to a Person, User, Employee, or Partner record. The following procedure describes how to add a responsibility to a Person record. You can assign a responsibility in the Users list or Employees list in the Administration - User screen.

If the individual does not have a current responsibility, this procedure upgrades the Person to a User. If the individual already has at least one responsibility, then the individual is already a User, an Employee, or a Partner. As such, the individual's record appears in the Persons list also, so this procedure works for any scenario.

To assign a responsibility to a Person

1. Log into a Siebel employee application as an administrator.
2. Navigate to the Administration - User screen, then the Persons view.

   The Persons list appears.
3. Select a Person record.
4. In the form, click the select button on the Responsibility field.

   A list of the responsibilities assigned to this Person appears.
5. In the Responsibilities list, click New.

   A list of responsibilities available for assigning appears.
6. Select one or more responsibilities, and then click OK.

   The selected responsibilities appear in the list of responsibilities for this Person.
7. Click OK.
8. Save the record.

NOTE: If you want to assign the same responsibility to multiple users, you can alternatively add the users to the responsibility through the Administration - Application screen.

Related Topics

"Responsibilities and Access Control" on page 287

"Assigning a Primary Responsibility" on page 316

Using Responsibilities to Allow Limited Access to Server Administration Views

You can configure responsibilities to grant specific users access to some, but not all, of the server administration views in Siebel Business Applications. For example, LOV administrators require access to the LOV administration screens to add new LOV values in multiple languages; however, they do not require access to other administration views. Likewise, the system administrator must be able to access the server management views to monitor the server performance, but only the Siebel administrator requires access to the server configuration views through which Siebel Business Applications are configured.

The following procedure describes how to provide access to a defined set of Siebel Server administration views for specific users.

To allow limited access to server administration views

1. Create a new responsibility, for example, create a responsibility with the name SubAdminRole.

   For information on creating responsibilities, see "Setting Up Responsibilities and Adding Views and Users" on page 285.

2 In the Views list, associate the new responsibility with the Administration - Server views that you want to allow users with the responsibility to access.

3 In the Users list, add users to the SubAdminRole responsibility you have just created. Make sure that the users do not have Siebel Administrator responsibility.

4 Change the value of the AdminRoles parameter for the Server Manager (ServerMgr) component by issuing the following command:

```
srvrmgr> change param AdminRoles="Siebel Administrator,SubAdminRole" for compdef
ServerMgr
```

5 Add the following parameter to the Gateway Name Server gateway.cfg file.

Section	Parameter	Value
[InfraNameServer]	NSAdminRole	Siebel Administrator,SubAdminRole

For information on the gateway.cfg file, see "About Authentication for Gateway Name Server Access" on page 165.

6 Stop and restart the Siebel Server.

Users assigned the SubAdminRole responsibility can now access the Siebel Server Administration views you associated with that responsibility.

Related Topic

"Responsibilities and Access Control" on page 287

Viewing Business Component View Modes

A business component's view modes determine the allowable access control mechanisms that can be applied to the business component in any view. When a view is based on a particular business component, the view must use one of the view modes specified for the business component. For example, the Account business component can only be used in Organization view mode or Sales Rep view mode.

Each view mode also determines how data is associated with a user to determine whether the user gets access. For example, a business component that allows personal access control might connect the data to the person by comparing the data's Owner Id field to the person's user ID. Another business component might apply personal access control through the data's Created by field.

NOTE: If a business component does not have view modes listed, then there is no access control associated with the business component in views that are based on that business component.

You use Siebel Tools to work with properties of business components. For information about working with business components, see *Configuring Siebel Business Applications*.

The following procedure describes how to view a business component's view mode in Siebel Tools.

To view a business component's view mode and visibility fields

1. Launch Siebel Tools.
2. In the Object Explorer, expand the Business Component object type.

   The Business Component subtree appears.
3. Click the BusComp View Mode icon.

   The Business Components list and its BusComp View Modes detail list appear.
4. In the Business Components list, select a business component for which there are records in the BusComp View Modes list.

   A record in the BusComp View Modes list represents one view mode the business component can assume.

Table 27 shows the fields in the BusComp View Modes list that determine the allowable visibility for a business component.

Table 27. Fields that Determine Visibility for Business Components

Field	Description
Owner Type	Specifies the party type that is used to determine whether or not 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.

Table 27. Fields that Determine Visibility for Business Components

Field	Description
Visibility Field	A value in either Visibility Field or Visibility MVField is required. The value in this field is compared with the corresponding value for the user, as specified in Owner Type, to determine whether the user is associated with a record. If the user is associated, 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 is the creator of the service request.
Visibility MVField (or multivalue field)	This field has the same purpose as Visibility Field, except a value in this field indicates that there can be more than one party associated with this business component when using this view mode. For example, the Account business component's Sales Rep view mode determines whether the user is associated with the record by comparing the user's position with the value in the Sales Rep field. When this view mode is used, more than one position can be associated with a record. In some applets, the Sales Rep field has a display name like "Account Team," indicating that more than one position is associated with the record.

Table 27. Fields that Determine Visibility for Business Components

Field	Description
Visibility MVLink (or multivalue link)	An entry in this field is required if there is a value in Visibility MVField. This field specifies which of the business component's multivalue links is used to determine the value in the MVField for this record. Links establish a parent/child relationship between business components, often by specifying an intersection table (in the case of a many-to-many relationship). This multivalue link's Destination Link property indicates which link ultimately defines this relationship. To see a business component's multi-value links and their properties in Siebel Tools, expand the Business Component object in the Object Explorer, and then click Multi Value Link. The Destination Link property is a field in each record. For example, the Account business component's Sales Rep view mode has Position as its MVLink. The Destination Link property for this multi-value link specifies that this relationship uses the Account/Position link. As seen in the Link object type listing in Siebel Tools, this link uses the S_ACCNT_POSTN intersection table to look up the positions associated with an account.
Name	The name typically suggests the view mode. For example, a view mode named Organization typically has an Owner type of Organization. However, the only requirement is that view mode records for a buscomp must have unique names. A business component cannot, for example, have two view modes named Personal. Some view mode names are: ■ **Personal.** This name is typically used when Owner type is Person. ■ **Sales Rep.** This name is typically used when Owner type is Position. ■ **Organization.** This name is typically used when Owner type is Organization. ■ **Group.** This name is typically used when Owner type is Group. ■ **Catalog.** This name is typically used when Owner type is Catalog. For example, the Account business component's Sales Rep view mode determines the association of the user to the record by the user's position. An example of an exception to the typical naming convention is the Service Request business component. Both the Personal and Sales Rep view modes have an Owner type of Person, one interpreting owner by Contact Id and the other by Owned By Id. Both view modes are needed because the creator and the customer care agent both need access to the data based on a person.

Configuring Access to Business Components from Scripting Interfaces

Siebel CRM provides object interface methods that can be used on Siebel business components to make their data and functions available to custom code, for example, to code that is written using Siebel scripting interfaces such as Browser Script. This topic describes how to control the operations that can be performed on business components from the Siebel scripting interfaces.

The following parameters allow you to configure the operations that can be performed on business components from scripting interfaces:

- The Siebel Server parameter, BusCompAccessLevel, can be specified for all business components to configure the operations that can be performed directly on a business component from scripting interfaces.
- The business component user property, DirectUIAccess, allows you to enable or disable operations on a specific business component from the scripting interfaces. The value of the DirectUIAccess property specified for a business component overrides any value set for business components using the BusCompAccessLevel server parameter.

  Depending on the value you configure for the DirectUIAccess parameter, you can also set a value for the DirectUIAccessFieldList business component user property; this allows you to enable write operations on specified business component fields through client-side scripting.

The following procedures describe how to set values for the BusCompAccessLevel server parameter and for the DirectUIAccess and DirectUIAccessFieldList user properties.

Configuring the Scripting Operations Permitted on Business Components (Siebel Server Parameter)

To configure the operations that can be performed on business components from scripting interfaces, specify a value for the Siebel Server parameter BusCompAccessLevel as described in the following procedure.

To configure the scripting operations permitted on business components (Siebel Server parameter)

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. In the Siebel Servers list, select a Siebel Server.
3. Click the Components view tab.
4. In the Components list, select a Siebel Server component.
5. Select the Parameters view tab below the Components list.
6. In the Component Parameters list, locate the BusCompAccessLevel parameter.

7 Specify one of the values shown in the following table to configure access to the component from the scripting interfaces.

Value	Description
None	Do not allow any direct operations on the business component from scripting interfaces.
Readonly (Default value)	Allow read-only operations on the business component from scripting interfaces.
All	Allow all operations on the business component from scripting interfaces.

Configuring the Scripting Operations Permitted on Business Components (Business Component User Property)

To configure the operations that can be performed on a specific business component from scripting interfaces, specify a value for the DirectUIAccess business component user property as described in the following procedure.

To configure the scripting operations permitted on a business component (business component user property)

1 Start Siebel Tools.

2 In the Object Explorer, click Business Component.

3 In the Business Components list, locate the business component for which you want to configure access.

4 In the Object Explorer, expand the Business Component tree, then click Business Component User Prop.

5 In the Business Component User Props list, locate the DirectUIAccess user property, and set the property to one of the values shown in the following table.

Value	Description
None	Do not allow any direct operations on the business component from scripting interfaces.
Readonly (Default value)	Allow read-only operations on the business component from scripting interfaces.

Value	Description
Limitedwrite	Allow limited field-write operations on the business component from scripting interfaces. If you set the value of the DirectUIAccess parameter to Limitedwrite, you also have to set a value for the business component user property DirectUIAccessFieldList (see Step 6 on page 297). If the DirectUIAccess property is set to Limitedwrite but a value is not specified for the DirectUIAccessFieldList property, this is equivalent to setting DirectUIAccess to Readonly.
All	Allow all operations on the business component from scripting interfaces.

6 If you set the value of the DirectUIAccess parameter to Limitedwrite, you also have to set a value for the business component user property DirectUIAccessFieldList to specify the fields that can be updated through browser scripting.

In the Value field of the DirectUIAccessFieldList user property, specify a comma-separated list of fields that can be updated through client side scripting. For example:

Field1,Field2,FieldN

where *Field1,Field2,FieldN* are the names of the fields for which write operations can be performed.

7 Compile and test your changes.

For more information on setting user properties, see *Using Siebel Tools*.

Viewing an Applet's Access Control Properties

A view presents a collection of lists, forms, and trees at once. These lists and forms are referred to as applets in a configuration context.

Applets are reused in different views and can have different access control properties applied in different views. If visibility is defined specifically for a view, then one of the applets in the view is specified as the visibility applet. Several properties of the visibility applet drive the access control of data in the view.

You use Siebel Tools to work with applets and their properties. For more information, see *Configuring Siebel Business Applications*.

Use the following procedure to view an applet's access control properties.

To view an applet's access control properties

1 Launch Siebel Tools.

2 In the Object Explorer, click + to expand the Applet object type.

The Applet subtree and the Applets list appear.

3 To see a particular applet property, click the icon for its subcomponent or click + to expand the subtree for a subcomponent, and then click its subcomponent.

A detail list for the subcomponent appears below the Applets list. Two applet properties in particular contribute to data visibility: Business Component and Display Name.

4 In the Object Explorer, choose Applets, List, and then List Columns.

As shown in Figure 8 on page 298, the List Columns list shows the business component fields that this applet displays. For each business component field, the Display Name entry in the accompanying Properties list shows how that field is labeled in the applet.

For example, the Accounts business component can use either the Sales Rep or Organization field to determine user association with a record. It is useful to know how these fields display in the Account List Applet. The Organization field has display name Organization in the applet, but the Sales Rep field has display name Account Team.

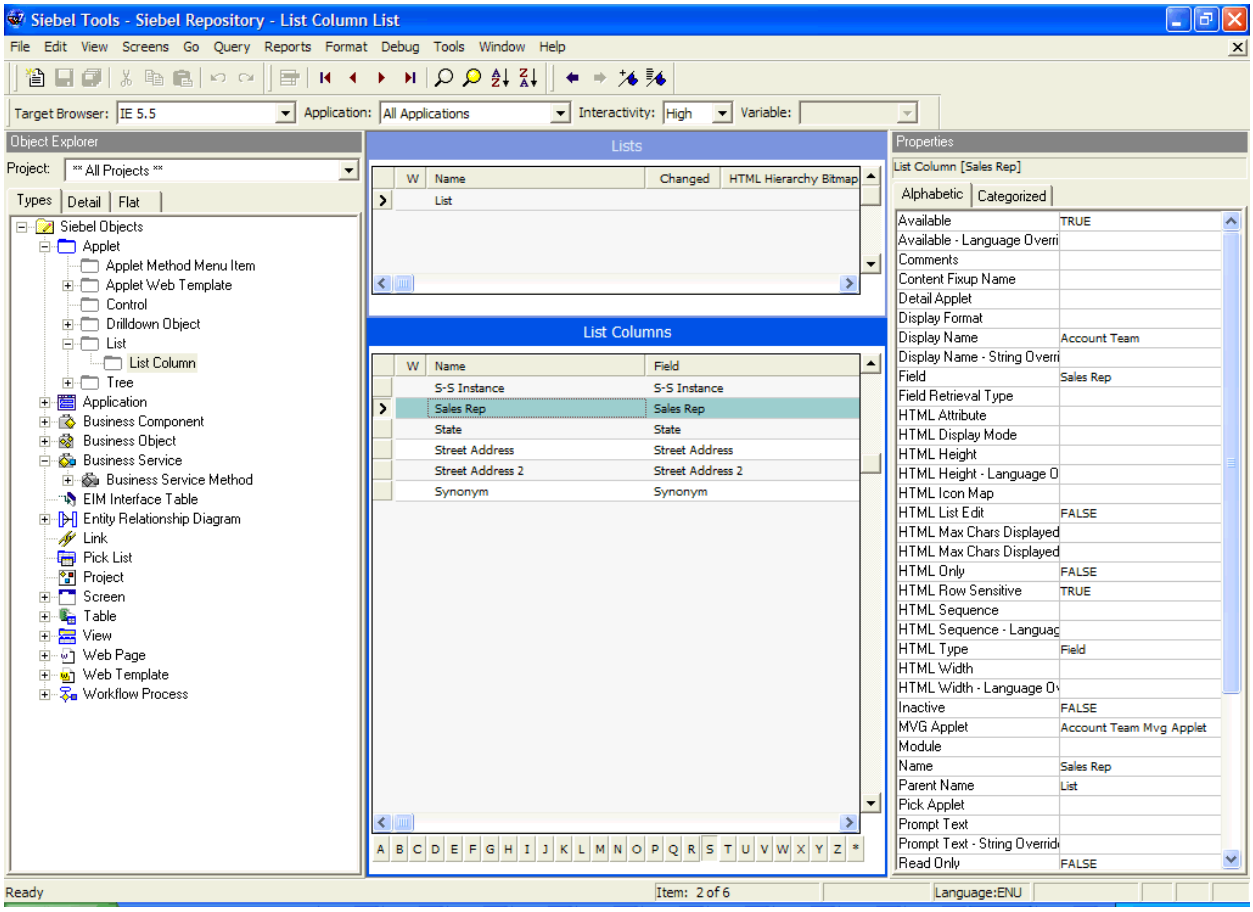

Figure 8. Lists and List Columns for an Applet

Listing View Access Control Properties

A view's access control properties determine what applet is used to drive visibility and what access control mechanism is applied to the business component on which the view is based.

You use Siebel Tools to work with properties of views.

To list a view's access control properties

1. Launch Siebel Tools.
2. In the Object Explorer, click the Views object type.

   The Views list appears.

The following fields in the Views list help determine data visibility.

- **Title.** The title is the name given to a view in the user interface. It is recommended that the title indicates the level of access control on the view's data. For example, My Accounts suggests more restricted visibility than My Team's Accounts.
- **Visibility applet.** Typically, this is the master in a master-detail applet relationship. This applet defines the business component on which the view is based and how fields of the business component are displayed.

  When the view property Visibility Applet is defined on a view, this view is considered to be associated with its own, independent visibility. The Siebel application will re-query this view when you choose it, according to the Visibility Applet Type (the default Visibility Applet Type is All).

  NOTE: Do not specify the Visibility Applet property on detail views, where the current record context and the current query should be retained.

  - A view has an entry in this field if the view is not derived from another view. For example, a view that is listed in the link bar for any screen has a visibility applet, but a view that results from drilling down from another view does not. A view with no visibility applet typically inherits access control properties from the view from which it is derived.
  - Multiple views can have the same visibility applet. For example, both All Account List View and Manager's Account List View have Account List Applet as their visibility applet.
- **Visibility Applet Type.** This field determines the access control mechanism that is applied to that view. It specifies which of the business component's view modes are applied and how they are applied. Following are the choices available in the picklist for this field:
  - **All.** A view of this type applies *All* access control.

    The user can access all records, except for those with a missing or invalid owner.

- **Personal.** A view of this type applies personal access control.

  The user can access records with which the user's Person record is associated, as determined by the business component's Visibility Field.

  To use this visibility applet type, the business component must have a view mode with owner type Person.

  NOTE: The Personal view mode of the Quote business component is specialized to display quotes created by the user and assigned to somebody else.

- **Sales Rep.** A view of this type applies single-position or team access control.

  The user can access records owned by the user's position or records whose team contains the user's position, as determined by the business component's Visibility Field or Visibility MVField. 2

  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. For additional information, see "About Manager Access Control" on page 269.

  To use this visibility applet type, the business component can have a view mode with owner type Position or Person.

- **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 might be able to see extra products in product picklists and other lists of products. This is expected behavior for products that belong to public catalogs.

- **Admin Mode.** This property requires a TRUE or FALSE value. When TRUE, the view operates in Admin mode. When the view is in Admin mode, all insert, delete, merge, and update restrictions for the business component used by applets of the view are ignored (including those restrictions specified by the following business component user properties: No Insert, No Delete, No Merge, No Update).

  Examples of Admin mode views include Account Administration view, Opportunity Administration view, and Product Administration view.

  Admin mode does not override pop-up visibility. It does not override Read Only restrictions on fields in a business component.

  In Admin mode, every record in a view that uses team access control is visible, even those with no primary position designated. (This mode is distinct from *All* visibility, which shows all records that have a primary team member designated.)

CAUTION: Views using Admin mode are intended for access by administrators and are typically included in a grouping of like views in an administration screen, such as Administration - Application. Do not include views in Admin mode in a screen with views not set for Admin mode. When a user transitions from a view that is in Admin mode to one that is not, the target view remains in Admin view, thereby exposing data that is not intended to be seen.

Example of Flexible View Construction

The following example shows how several existing views were constructed, based on the same visibility applet and business component. It suggests how similar view “families” can be constructed in Siebel Tools, but does not give procedures for constructing views. Changing any settings in Siebel Tools requires recompiling the Siebel repository file (SRF). For more information about required practices when using Siebel Tools, see *Configuring Siebel Business Applications*.

Figure 9 shows the BusComp View Modes list in Siebel Tools for the Account business component. As indicated by the Owner Type field, organization and position view modes are allowed. As indicated in Visibility MVField, accounts can be associated with multiple organizations and multiple positions (for example, sales teams).

BusComp View Modes

Name	Changed	Owner Type	Private Field	Visibility Field	Visibility MVField	Visibility MVLink
Organization		Organization			Organization	Organization
Sales Rep		Position			Sales Rep	Position

Figure 9. Account Business Component View Modes

Figure 10 shows five views in the Views list in Siebel Tools. The Title field shows the display name for the view. All five views have Account List Applet as their visibility applet. Account List Applet is based on the Account business component.

Views

Name	Title	Visibility Applet	Visibility Applet Type
Account List View	My Accounts	Account List Applet	Sales Rep
Manager's Account List View	Team's Accounts	Account List Applet	Manager
All Account List View	All Accounts	Account List Applet	Organization
All Accounts across My Organizations	All Accounts across My Organizations	Account List Applet	Sub-Organization
All Accounts across Organizations	All Accounts across Organizations	Account List Applet	All

Figure 10. Example Views Based on the Account Business Component

These five example views provide different lists of account data because they have different visibility applet types specified, as shown in Table 28.

Table 28. Example Account Views and Visibility Applet Types

View	Visibility Applet Type	Data Access
Account List View (displayed as My Accounts)	Sales Rep	Team access control applies. The visibility applet type is applied to a business component for which multiple positions can be associated. For this view, access is granted to account data where the user's position is on the account team.
Manager's Account List View (displayed as Team's Accounts)	Manager	Manager access control applies. The visibility applet type is applied to a business component for which multiple positions can be associated. For this view, access is granted to account data where the user's active position or a subordinate position is the primary position on the account team.
All Account List View (displayed as All Accounts)	Organization	Organization access control applies. The visibility applet type is applied to a business component for which multiple organizations can be associated. For this view, access is granted to account data where a user's primary organization is one of the organizations with which the account is associated.
All Accounts across My Organizations	Sub-Organization	Suborganization access control applies. The visibility applet type is applied to a business component for which multiple organizations can be associated. For this view, access is granted to account data where the user's active organization or a descendant organization is the primary organization.
All Accounts across Organizations	All	All access control applies. The Account business component has only position and organization view modes. For this view, access is granted to all account data for which there is a primary position on the account team or an organization associated with the account.

About Implementing Access-Group Access Control

You associate an access group to a catalog or category of master data. When an access group is associated with a catalog or a category, the users associated with the access group have visibility to the data in the catalog or the category. An access group in this context is an individual node in an access group hierarchy.

The following principles apply to access-group access control:

- **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.

Related Topics

"Scenario That Applies Access-Group Access Control" on page 304

"Viewing Categorized Data (Users)" on page 307

Scenario That Applies Access-Group Access Control

Assume that you want the status of your resellers to determine which of your knowledge resources they have access to. Your resellers include partner organizations and some individual consultants who are not associated with a partner organization. Your solution must meet the following requirements:

- Provide your base resellers access to basic product information resources, for example, service FAQs, product documentation, and product training classes.
- In addition to basic product information, provide your “premier” resellers access to more sales-specific resources, for example, 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, for example, competitive briefs and training classes.
- As the status of a reseller changes, the administration required to change the reseller’s access to data must be minimal.

Figure 11 illustrates one access control structure that solves this business problem.

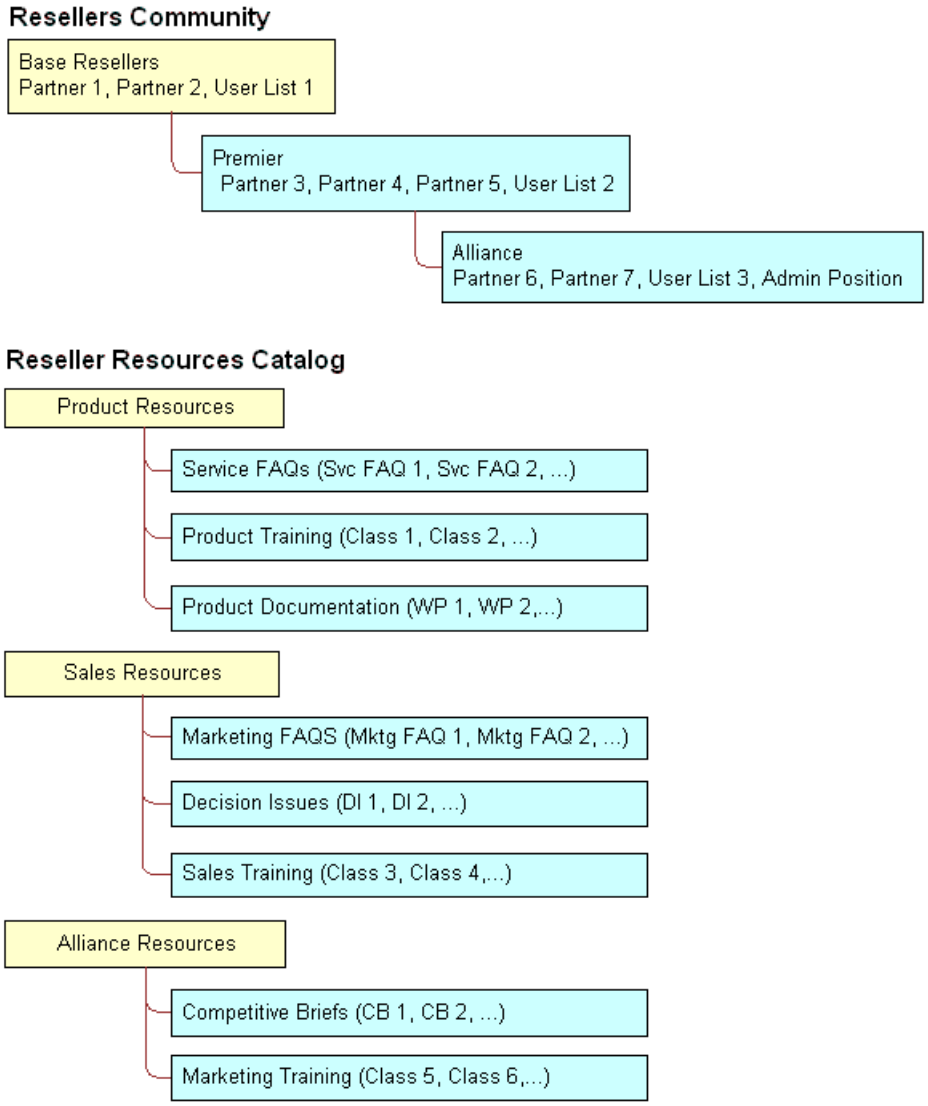

Figure 11. Reseller Resources Access Control Example

This solution assumes that your partners are stored as organizations, in which partner users are associated with positions. The consultants exist as users; they have responsibilities, but not positions, and are not associated with an organization.

The Resellers Community is an access group hierarchy. Each node is an access group whose members are partner organizations and a single user list. The user list in each node contains all consultants of the appropriate status. For internal administrators to have visibility of the catalog, include their positions in the Alliance access group.

The Reseller Resources catalog is constructed of categories containing data and nodes that are empty categories to define access levels.

Apply the following principles to construct this structure:

- Construct the Resellers Community such that the upper levels have the narrowest access to resources. Therefore, the Base Resellers access group is the parent of the Premier access group, which is in turn the parent of the Alliance access group.
- Construct the Reseller Resources Catalog such that the Product Resources, Sales Resources, and Alliance Resources nodes are all first-level categories in the catalog.

  For information about creating and administering catalogs, see *Siebel eSales Administration Guide*.
- 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.

Implementing the Reseller Resources Access Control Structure

The following implementation procedure restricts the base resellers' access to product resources only, premier resellers' access to product resources and sales resources, and alliance resellers' access to all resources.

To implement the Reseller Resources access control structure

1. Construct the Reseller Resources catalog, and specify it as private, with access provided to the Base Resellers access group.

   Access to the catalog is also granted to the Premier and Alliance access groups because access group access is inherited.

2. Associate the Base Resellers access group with the Product Resources category, and use the Cascade button.

   Access is inherited by the Premier and Alliance access groups from the Base Resellers group, and access cascades from the Product Resources category to its subcategories containing data. The resulting behavior is that all the nodes in the Resellers Community have access to all the subcategories in the Product Resources category.

3 Associate the Premier access group with the Sales Resources category, and use the Cascade button.

   Access is inherited by the Alliance access group from the Premier group, and access cascades from the Sales Resources category to its subcategories containing data. The resulting behavior is that the Premier and Alliance groups have access to all the subcategories in the Sales Resources category.

4 Associate the Alliance access group with the Sales Resources category, and use the Cascade button.

   No group inherits access from the Alliance group. Access cascades from the Alliance Resources category to its subcategories containing data. The resulting behavior is that only the Alliance group has access to the subcategories in the Alliance Resources category.

5 Set the catalog to type Partner to make it visible to partners and consultants on partner applications such as Siebel Partner Portal, and to internal administrators on Siebel employee applications in the Info Center screen.

This structure meets the minimal maintenance requirement. If the status of a partner organization changes, add the partner organization to the appropriate access group and delete the partner organization from the old access group. If the status of a consultant changes, add the user to the appropriate user list, and delete the user from the old user list. Recategorized consultants and partner users are granted appropriate new access as defined by the structure.

NOTE: Sales tools of the same type, for example FAQs or product documentation, are in separate categories.

Related Topic

"About Implementing Access-Group Access Control" on page 304

Viewing Categorized Data (Users)

You can configure a catalog to display in Siebel employee applications and in selected customer and partner applications, such as Siebel Sales and Siebel Partner Portal, as default functionality.

In an employee application, such as Siebel Call Center, a user can see categorized data controlled by access group membership in the Info Center and Info Center Explorer screens. Info Center Explorer provides a tree interface for navigating all the catalogs to which the user has access, down to the data item level. Info Center, as compared to Info Center Explorer, shows how categorized data can be presented in Siebel Business Applications using a more open user interface.

To see categorized data in Info Center

1 Navigate to the Info Center screen.

   The Info Center screen appears, showing accessible catalogs and their first-level categories.

2 Click a category link. For example, you might choose Decision Issues.

   The category appears, showing its data items and its first-level subcategories.

3 Click a data item to view it, or drill down on a subcategory link to see its contents.

Related Topic

"About Implementing Access-Group Access Control" on page 304

Implementing Access-Group Access Control

This topic describes the administrative tasks you must perform to implement access-group access control.

To implement access-group access control perform the following tasks:

- Administer catalogs of master data; build the catalogs and categories, associate data, and modify catalog structures as needed.

  For additional information, see "About Administering Catalogs of Data" on page 308.

- Administer the party types that are members of access groups, that is, positions, organizations, households, and user lists.

  For additional information, see "Administration Tasks for Positions, Organizations, Households, and User Lists" on page 309.

- "Administering Access Groups" on page 310.

  Administer access groups; build the access groups and modify their structures as needed.

- "Associating Access Groups with Data" on page 312.

  Associate access groups with catalogs and categories of data.

About Administering Catalogs of Data

You can do the following catalog and category administration tasks in the Administration - Catalog screen:

- Create and delete catalogs and categories of master data.
- Associate data with categories.
- Modify the hierarchical position of a category within a catalog.

For information about creating and administering catalogs, see *Siebel eSales Administration Guide* and *Siebel Partner Relationship Management Administration Guide*. Key principles for setting up a catalog include, but are not limited to:

- Set the Catalog Type field to allow display of the catalog in certain Siebel customer or partner applications, in addition to Info Center and Info Center Explorer in Siebel employee applications. For example, set the Catalog Type to Partner to display the catalog in Siebel Partner Portal, as well as in Info Center.

- Make sure the Active flag is set and the Effective Start Date and Effective End Date fields provide visibility of the catalog during your intended time interval.

Related Topic

"Implementing Access-Group Access Control" on page 308

Administration Tasks for Positions, Organizations, Households, and User Lists

Access groups are made up of positions, organizations, households, and user lists. This topic describes the administration tasks associated with each of these access groups.

About Administering Positions

Perform the following administrative tasks for positions:

- Create positions.

  For information on this task, see "Setting Up Positions" on page 284.

- Associate positions with employees and partner users.

  For information on this task, see "Adding a New Employee" on page 242 and "About Adding a New Partner User" on page 244.

- Maintain position hierarchies.

  For information on this task, see "About Position Access Control" on page 267 and "About Planning for Positions" on page 280.

About Administering Organizations

The Organization group type includes organizations, divisions, and accounts. You must perform the following administrative tasks for organizations:

- Create divisions and accounts.

  For information on creating divisions, see "Setting Up Divisions" on page 283. For information on creating accounts, see *Siebel Applications Administration Guide*.

- Promote divisions to organizations and maintain division hierarchies.

- Associate positions with divisions and with partner organizations.

For information on creating organizations, see "Setting Up Organizations" on page 283. For information on planning for organizations, see "About Organization Access Control" on page 271 and "About Planning for Organizations" on page 279.

About Administering Households

You must perform the following administrative tasks for households:

- Create households.
- Associate contacts with households.
- Maintain household data.

For information on these tasks, see *Siebel Applications Administration Guide*.

Administering User Lists

You can group arbitrary users into user lists for the purpose of granting them access to data through access groups. Users in this context include contact users, employees, and partner users. For information about user lists, see "Access Control for Parties" on page 260.

The following procedure describes how to create a user list and add users to it.

To create a user list

1. Navigate to the Administration - Group screen, then the User Lists view.

   The User Lists list appears.

2. In the User Lists list, add a new record.

   A new user list record appears.

3. Enter a name for the user list. Optionally, change the default entry for Group Type.
4. Save the record.
5. To add users to the user list you created, select the list.
6. In the Users list at the bottom of the view, add a new record.
7. 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.

Related Topic

"Implementing Access-Group Access Control" on page 308

Administering Access Groups

You can group parties of types Position, Organization, Household, and User List into access groups for the purpose of controlling their individual members' access to data.

You administer access groups in the Administration - Group screen. 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 can appear at different levels in multiple branches of the tree. An access group that has no parent access group is the top node of an access group hierarchy. For information about access groups, see "Access Control for Parties" on page 260 and "About Access-Group Access Control" on page 275.

Creating an Access Group

The following procedure describes how to create an access group.

To create an access group

1. Navigate to the Administration - Group screen, then the Access Groups view.

   The Access Groups tree and the Access Groups list appear.

2. In the Access Groups list, add a new record.

   A new access group record.

3. Complete the following fields, then save the record. Use the guidelines below.

Field	Guideline
Name	Required. Provide a name for the access group.
Group Type	Pick Access Group or Partner Community. These labels denote conceptual differences. Functionally, they are the same.
Parent Access Group	Specify a parent access group from which this new group inherits access to data that the parent group has access to.

   The new access group also appears in the Access Groups tree.

Modifying an Access Group

You can modify an access group by adding or deleting members using the following procedure.

To add members to an access group

1. Navigate to the Administration - Group screen, then the Access Groups view.

   The Access Groups list appears.

2. In the Access Groups list, select an access group.

3. In the Members list, add a new record.

   A pop-up list appears that contains positions, organizations, accounts, households, and user lists.

4 Select one or more members, and then click OK.

The selected members appear in the Members list.

5 In the Access Groups list, save the record.

You can delete members from an access group similarly.

Modifying an Access Group Hierarchy

You can modify the hierarchy of an access group by changing an access group's parent as described in the following procedure.

To modify a hierarchy of access groups

1 Navigate to the Administration - Group screen, then the Access Groups view.

The Access Groups list appears.

2 In the Access Groups list, select an access group.

3 Click on the Parent Access Group field.

The text box becomes editable and its entry is highlighted.

4 Do one of the following to modify the hierarchy:

- To make the access group the top node of its own hierarchy, delete the entry in the Parent Access Group field. Click Save.
- From the Parent Access Group field, pick a new parent and click OK. Click Save.

The Access Group tree is updated to reflect the access group's new position in a hierarchy.

Related Topic

"Implementing Access-Group Access Control" on page 308

Associating Access Groups with Data

The individual users in an access group are provided access to data by associating the access group with catalogs or categories of data.

Be aware of the following user interface behaviors related to associating an access group with a catalog or category:

- **Access inheritance.** When you associate an access group with a category, its descendant groups are also associated with the category. However, this inheritance is implemented at run time, and is not represented in the database. As such, the descendant access groups associated with the category are not displayed in the list of groups associated with the category.

- **Cascade button.** Clicking the Cascade button provides the given access group with visibility to all of the child categories of the current catalog or category. Clicking this button repeatedly has no effect. You must manually disassociate the group from the child categories to undo the access cascade.
- **Private catalog.** If you specify a catalog to be private, its categories are all set as private. If you remove privacy at the catalog level, the categories retain privacy. You must then set or remove category privacy individually.

Associating an Access Group with a Catalog

By associating an access group with a catalog of master data, you grant access to the data in the catalog to individual users in the access group.

NOTE: For a catalog and all of its categories to be visible only to the access groups associated with it, the catalog's Private flag must be set.

To associate an access group with a catalog

1. Navigate to the Administration - Catalog screen, then the Access Groups view.

   The Catalogs list appears.

2. Select a catalog.
3. In the Access Groups list, add a new record.

   A pop-up list appears that contains access groups.

4. Select an access group, and then click Add.

   The access group appears in the Access Groups list.

5. In the Access Groups list, save the record.
6. Select an access group, and then click Add.

   The access group appears under the Access Group tab.

7. Complete the following fields, then save the record. Use the guidelines provided below.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer the catalog.
Cascade	Set this flag to automatically associate this access group with the catalog's descendant categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendant categories.

You can disassociate an access group from a catalog similarly.

Associating an Access Group with a Category

By associating an access group with a category of master data, you grant access to the data in the category to individual users in the access group.

NOTE: For a category and all of its subcategories to be visible only to the access groups associated with it, the category's Private flag must be set or the Private flag of the catalog or a category from which the category descends must be set.

To associate an access group with a category

1. Navigate to the Administration - Catalog screen, then the Access Groups view.

   The Catalogs list appears.

2. Drill down on a catalog name.

   The Categories list for the catalog appears.

3. Click the Access Groups view tab.

4. In the Access Groups list, add a new record.

   A multi-value group appears that lists access groups.

5. Select an access group, and then click Add.

   The access group appears in the Access Groups list.

6. In the Access Groups list, save the record.

7. Select an access group, and then click Add.

   The access group appears under the Access Group tab.

8. Complete the following fields, and save the record. Use the guidelines provided below.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer this category.
Cascade	Set this flag to automatically associate this access group with this category's descendant categories (child, grandchild, and so on). The resulting behavior is that users in the access group have access to the data in the descendant categories.

You can disassociate an access group from a catalog similarly. When an access group is disassociated from a category, it is automatically disassociated from all of the category's descendant categories.

Related Topic

"Implementing Access-Group Access Control" on page 308

Managing Tab Layouts Through Responsibilities

Siebel Business Applications administrators can manage default screen and view tab layouts that are specific to job functions. Tab layouts are managed through responsibilities.

Administrators can use the Responsibilities view (Responsibility Detail - Tab Layout View) in the Administration - Application screen to define a default tab layout for each responsibility. Administrators can administer both view access and default tab layout from this view.

To ease the administrative burden of setting up default tab layouts and associating them with responsibilities, Siebel Business Applications ship with many predefined responsibilities that are preconfigured with default tab layouts.

For example, the Universal Agent responsibility for Siebel Call Center has associated with it both screen and view access as well as a default tab layout. These are the views required most often for users holding that job function. Each time a user with this responsibility logs in, this user has access to all screens and views for that responsibility, and for all other responsibilities the user is associated with.

However, the user sees in the application user interface only the simplified default screen and view tab layout associated with the user's primary responsibility, for example, the layout associated with the Universal Agent responsibility, if this is the user's primary responsibility.

Each user can modify personal tab layout settings by using the Tab Layout view in the User Preferences screen (Tools, and then User Preferences). Once the user has modified the tab layout, these settings will always override the default tab layout associated with the user's primary responsibility. For more information, see *Siebel Fundamentals*.

If a user selects a screen from the Site Map that is not part of his or her tab layout, a screen tab is created for that screen which is only available for that session.

The following topics provide additional information on managing tab layouts through responsibilities:

- "Specifying Tab Layouts for Responsibilities" on page 315
- "Assigning a Primary Responsibility" on page 316
- "Exporting and Importing Tab Layouts" on page 317

Specifying Tab Layouts for Responsibilities

This topic describes how to specify the tab layout for a responsibility.

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. To let you manage screens and views for multiple applications, tab layout administration uses four lists:

- **Responsibilities list.** Includes all the responsibilities in the repository.
- **Applications list.** Includes all the Siebel Business Applications in the repository, and specifies for which application you are managing tab layouts.

- **Screen Tab Layout list.** Specifies which screens are displayed for each application.
- **View Tab Layout list.** Specifies which views are displayed for each screen.

You must select an application because you might be administering responsibilities for a different application than the one you are logged into as an administrator. For example, you use Siebel Partner Manager to administer responsibilities for partners who will use Siebel Partner Portal.

To specify the tab layout for a responsibility

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, then the Responsibilities view.
3. In the Responsibilities list, select the responsibility you want to associate tab layouts with.
4. Click the Tab Layout view tab.
5. In the Tab Layout list, select an application associated with the responsibility.
6. The Screen Tab Layout list displays all the screens used by the selected application:
   a. Select the Hide check box for any screens whose screen tabs will not be displayed.
   b. Change the numbers in the Order field to change the sequence in which the screen tabs are displayed.
7. Select each record in the Screen Tab Layout list, and the View Tab Layout list displays all the views for that screen:
   a. Select the Hide check box for any views whose view tabs will not be displayed.
   b. Change the numbers in the Order field to change the sequence in which the screen tabs are displayed.

Related Topic

"Managing Tab Layouts Through Responsibilities" on page 315

Assigning a Primary Responsibility

Each user can have multiple responsibilities assigned, in order to provide access to all necessary views. One responsibility is defined as the primary responsibility. The user sees the tab layout associated with his or her primary responsibility. The Site Map provides this user with access to the superset of screens and views defined in the responsibilities with which the user is associated.

To assign a primary responsibility to a user, perform the following procedure.

To assign a primary responsibility to a user

1. Navigate to the Administration - User screen, then the Users view.
2. Select a User record.

3 In the form, click the select button on the Responsibility field.

A list of the responsibilities assigned to the User appears.

4 In the Responsibilities dialog box, set the primary responsibility for the user by checking the Primary flag of one of the selected responsibilities.

NOTE: By default, the first responsibility assigned to a user (based on timestamp) becomes the primary responsibility. Particularly for customers who are upgrading, verify that the correct primary responsibility is assigned to each user, or specify the desired primary responsibility.

Related Topic

"Managing Tab Layouts Through Responsibilities" on page 315

Exporting and Importing Tab Layouts

To copy a tab layout from one responsibility to another, you can export and import tab layouts. For example, if you have a tab layout associated with one responsibility and you want to apply it to another responsibility, you can first export the desired tab layout settings to an XML file, optionally modify the file, and then import it to the target responsibility.

NOTE: Tab layouts associated with responsibilities are stored in the Siebel File System as attachments. These files are automatically routed to mobile users.

Exporting Tab Layouts

This topic provides the procedure for exporting tab layouts to an XML file.

To export tab layouts

1 Navigate to the Administration - Application screen, then the Responsibilities view.

2 In the Responsibilities list, click the Tab Layout view tab.

3 Select the responsibility that has the desired tab layout.

4 Select a record in the Applications list.

You can select multiple applications and export the tab layouts for a responsibility for one or more associated applications. The XML file will contain screen tab and view tab settings for the selected applications. When you later import the XML file, tags in the file specify the applications that are 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.

NOTE: When you export the tab layout for a responsibility, only the differences between the current tab layout settings and the default tab layout settings are exported. If you want to migrate the tab layout for a responsibility from one Siebel environment to another, rather than just from one responsibility to another, then the XML file you import must include all the tab layout settings for the responsibility, not just the differences. In this case, you must edit the XML file and manually add the tab layout information for any views not already included.

Importing Tab Layouts

This topic provides the procedure for importing tab layouts from an XML file you previously exported to.

To import tab layout to a target responsibility

1 From the application level-menu, navigate to the Administration - Application screen, then the Responsibilities view.

2 Click the Tab Layout view tab and select the target responsibility in the Responsibilities list.

3 Click the menu button in the Responsibilities list and select Import Tab Layout.

4 In the import dialog box, choose the XML file for the Application Tab Layout you want to import.

5 Click Import.

After you have imported the XML file, default tabs in the application correspond to those defined in the file you imported.

NOTE: Importing a tab layout file hides and resequences views for affected users. Although you cannot roll back imported changes directly, you can still modify tab layout settings in the Responsibilities Administration view, or you can modify the XML file and reimport it.

6 (Optional) If the XML file you are importing contains all the tab layout settings for a responsibility, not just the differences between the existing tab layout and the default tab layout, then, after importing the XML file, you must log out of the application, then log back in again to see the updated tab layout.

Related Topic

"Managing Tab Layouts Through Responsibilities" on page 315

Managing Tasks Through Responsibilities

A user with an administrator login can control access to tasks by associating tasks with user responsibilities. To access a task, a user must be assigned the responsibility that allows access to the task. A user who is assigned more than one responsibility can access any task that is associated with one of his or her responsibilities.

The administrator can also define hyperlinks to the tasks associated with a responsibility; these task links then appear on the home page of the users who are assigned the responsibility.

NOTE: For a user to access a task, at least one of the user's responsibilities must be explicitly assigned to the task.

The following topics describe how to associate responsibilities and tasks:

- "Associating Responsibilities with a Task" on page 319
- "Creating Task Links for a Responsibility" on page 320

For more information about tasks, see *Siebel Business Process Framework: Task UI Guide*.

Associating Responsibilities with a Task

This topic describes how you can associate a responsibility with a task to control access to the task. You carry out the following procedure through the Registered Tasks Administration view.

To associate responsibilities with a task

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, then the Tasks view.
3. In the Registered Tasks list, select the task that you want to associate with responsibilities.
4. In the Responsibilities list, click New.

   The Tasks dialog box appears.
5. Select a responsibility, then click OK.

   The responsibility appears in the Responsibilities list and is associated with the task you selected in Step 3.
6. If appropriate, select or clear the check boxes for Allow Delete and Allow Transfer.
   - Allow Delete

     Select the Allow Delete check box if you want an employee with the associated responsibility to be able to delete the task.

- Allow Transfer

  Select the Allow Transfer check box if you want an employee with the associated responsibility to be able to transfer the task.

For information about deleting or transferring tasks, see *Siebel Business Process Framework: Task UI Guide*.

7 Step off the record to save changes.

Creating Task Links for a Responsibility

After creating a responsibility, you can create links to the tasks commonly performed by employees who have that responsibility. These links are then displayed in the task list on the home page for these employees.

For each task link, you enter a caption, an image file, and a description. In addition, specify the view where the task is performed. When the user clicks on the hyperlink for this task on the home page, this view appears. Personalization of this type is already specified for various seed responsibilities.

The following procedure describes how to create task links for a responsibility.

To create task links for a responsibility

1 Log in as an administrator.

2 Navigate to the Administration - Application screen, then the Responsibilities view.

3 In the Responsibilities list, select the responsibility you want to associate with task links.

4 Click the Links tab.

5 In the Links list, do one of the following:

- Click the Add tab.

  Click this tab to display the Add Links list, from which you can select an existing task link to add to the list of task links associated with the responsibility.

- Click the New tab to add a new task link for this responsibility, and enter the following information:

Field	Guideline
Name	Enter the name of the task.
Caption	Enter a caption for the task; this is displayed as a hyperlink in the task list.
Description	Enter a description of the task; this is displayed under the caption in the task list.
Destination View	Click the select button and choose the view that appears when the user clicks the hyperlink for this task.

Field	Guideline
Sequence	Optionally, specify the order in which this task is displayed in the task list for this responsibility on the home page. If this field is left blank, tasks are displayed in the order that you list them here.
Image	Select the graphic image that is displayed as a hyperlink to the left of this task in the task list.
Group	This field is used if search specifications are applied to filter the tasks that are displayed in the task applet, if multiple task applets are associated with the responsibility.

Administering Access Control for Business Services

Business services can be accessed by all users by default. However, the administrator can restrict access to specified business services and business service methods. The administrator can then associate responsibilities with the restricted business services or associate the business services with responsibilities. This allows the administrator to restrict access to business services based on the end user's responsibility. To access a restricted business service, an end user must be associated with the responsibility that allows access to the restricted business service. An end user who is assigned more than one responsibility can access any restricted business service that is associated with one of his or her responsibilities.

For business services that allow you to specify a view mode to access data, you can specify which view mode can be used by different responsibilities. Figure 12 shows the view modes that can be associated with a responsibility to restrict the set of data records a user with the responsibility accesses. The level of visibility broadens as you read from left to right; for example, the Manager view mode grants access to more data than the Sales Rep view mode.

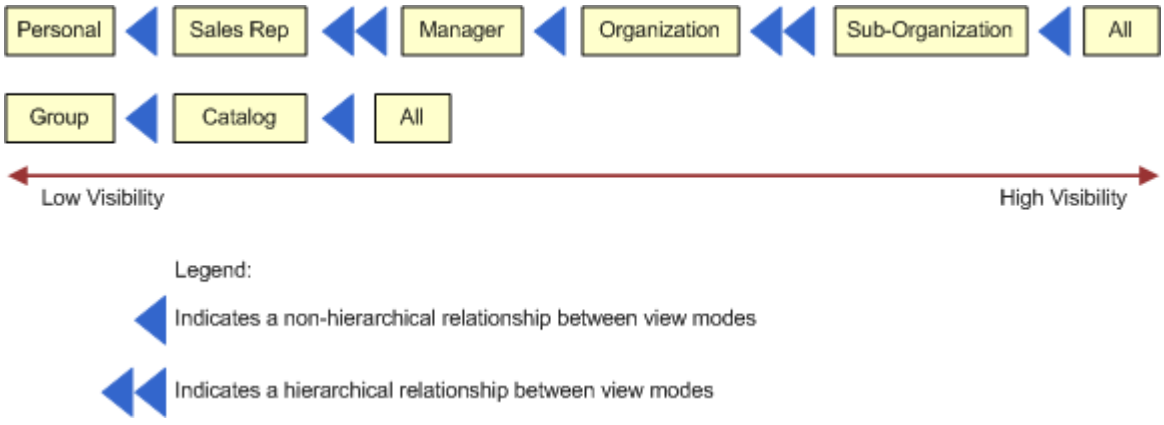

Figure 12. View Modes Associated with Responsibilities

Figure 12 also shows whether or not the relationship that exists between each view mode is hierarchical. For example, the relationship between Manager view mode and Organization view mode is not hierarchical. The relationship between Sales Rep view mode and Manager view mode is hierarchical.

Assigning appropriate view modes allows you to manage access to business services (and associated methods) by end users based on the responsibilities assigned to the end user. The following topics provide more detailed information on the tasks involved in administering access control for business services:

- "Associating a Business Service with a Responsibility" on page 322
- "Associating a Responsibility with a Business Service" on page 323
- "Example of Associating a Responsibility with Business Service Methods" on page 325
- "Clearing Cached Business Services" on page 326
- "Disabling Access Control for Business Services" on page 326

Associating a Business Service with a Responsibility

This topic describes how you can associate a business service with a responsibility to control access to the business service and its methods. You carry out the following procedure through the Responsibilities view.

To associate a business service with a responsibility

1. Log in as an administrator.
2. Navigate to the Administration - Application screen, Responsibilities, and then the Business Service view.
3. In the Responsibilities list, select the responsibility that you want to associate with a business service.
4. In the Business Service list, click New to select a business service to associate with the responsibility selected in Step 3.

   The Business Service dialog box displays the list of business services that are currently associated with the responsibility selected in Step 3.
5. In the Business Service dialog box, click New.

   A new record appears in the Business Service list view.
6. Click the Select button in the Name field.

   The Business Service dialog box appears.
7. Select a business service to associate with the responsibility selected in Step 3, and then click OK.

   The selected business service appears in the Business Service list view.

8 In the Business Service Method list, click New to specify the business service methods to which the responsibility selected in Step 3 gains access.

The Business Service Method dialog box appears. This dialog box displays the list of Business Service methods to which access is currently controlled.

9 If the business service method to which you want to allow the responsibility access appears in the Business Service Method dialog box, select it, then click OK and go to Step 13. If not, go to Step 10.

TIP: To allow you to restrict access to business service methods without associating them with a real responsibility, Siebel Business Applications have provided a responsibility Default Bus Service Method Access Control User. Use the steps described in this procedure to associate all business service methods to which you want to control access with Default Bus Service Method Access Control User. This makes sure that the Business Service Method dialog box is populated with the business service methods to which you want to control access.

10 In the Business Service Method dialog box, click New.

A new record appears in the Business Service Method list view.

11 Click the Select button in the Name field.

The Business Service Method dialog box appears.

12 Select a business service method to associate with the responsibility selected in Step 3 on page 322, and then click OK.

The selected business service method appears in the Business Service Method list view.

NOTE: By default, if you do not specify the business service methods to which the responsibility gains access, then the responsibility gains access to all business service methods of the business service provided that none of the business service methods have restricted access.

13 From the Broadest Visibility list, select the view mode to associate with the responsibility.

NOTE: The business service selected in Step 7 on page 322 must support view modes to allow you to select a value from the Broadest Visibility list.

14 Step off the record to save changes.

Related Topic

"Administering Access Control for Business Services" on page 321

Associating a Responsibility with a Business Service

This topic describes how you can associate a responsibility with a business service to control access to the business service and its methods. You carry out the following procedure through the Business Service Access view.

To associate a responsibility with a business service

1 Log in as an administrator.

2 Navigate to the Administration - Application screen, then the Business Service Access view.

3 In the Business Service list, click New to select a business service.

A new record appears in the Business Service list.

4 Click the Select button in the Name field.

The Business Service dialog box appears.

5 Select the business service to which you want to control access, then click OK.

The selected business service appears in the Business Service list view.

6 In the Access By Responsibility list view, click New.

The Add Responsibilities dialog box appears.

7 Select a responsibility to associate with the business service that you selected in Step 5, and then click OK.

The selected responsibility appears in the Access By Responsibility list view.

8 In the Business Service Method list, click New to specify the business service methods to which the responsibility selected in Step 7 gains access.

The Business Service Method dialog box appears. This dialog box displays the list of business service methods to which access is currently controlled.

9 If the business service method to which you want to allow the responsibility access appears in the Business Service Method dialog box, select it, then click OK and go to Step 12. If not, go to Step 10.

TIP: To allow you to restrict access to business service methods without associating them with a real responsibility, Siebel Business Applications have provided a responsibility Default Bus Service Method Access Control User. Use the steps described in this procedure to associate all business service methods to which you want to control access with Default Bus Service Method Access Control User. This makes sure that the Business Service Method dialog box is populated with the business service methods to which you want to control access.

10 Click the Select button in the Name field.

The Business Service Method dialog box appears.

11 Select a business service method to associate with the responsibility selected in Step 3 on page 322, and then click OK.

The selected business service method appears in the Business Service Method list view.

NOTE: By default, if you do not specify the business service methods to which the responsibility gains access, then the responsibility gains access to all business service methods of the business service provided that none of the business service methods have restricted access.

12 From the Broadest Visibility list, select the view mode to associate with the responsibility.

NOTE: The business service selected in Step 5 must support view modes to allow you to select a value from the Broadest Visibility list.

13 Step off the record to save changes.

Related Topic

"Administering Access Control for Business Services" on page 321

Example of Associating a Responsibility with Business Service Methods

Figure 13 on page 325 shows the modifications made in the Business Services Method applet so that a user with Partner Executive responsibility can invoke the business service methods Query, Update, and Insert of the business service Account Test UDS.

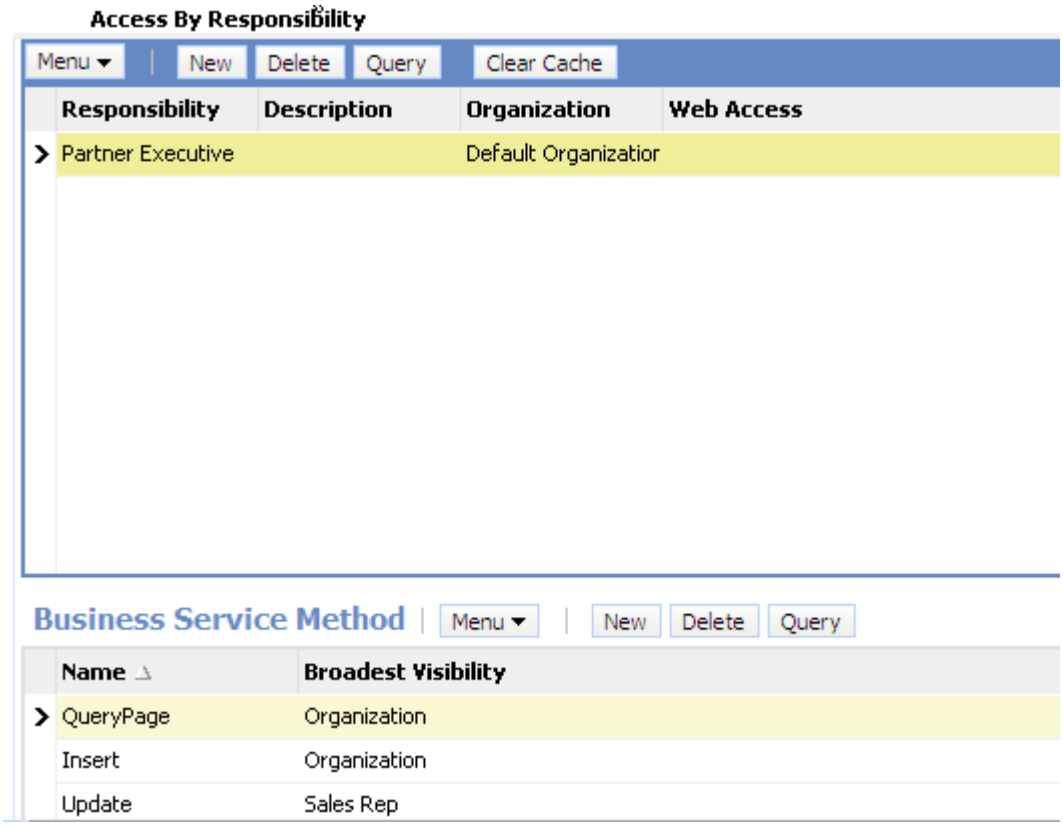

Figure 13. Business Service Methods Associated with a Responsibility

A user with Partner Executive responsibility in the example illustrated in Figure 13 can:

- View all accounts that belong to his or her organization because the business service method Query has Broadest Visibility equal to Organization.
- Update accounts for the sales team of which he or she is a member because the business service method Update has Broadest Visibility equal to Sales Rep.

- Insert a new account as the business service method Insert has Broadest Visibility equal to Organization. If the new account entry matches an existing account entry in the user's organization, then an error message appears.

Related Topic

"Administering Access Control for Business Services" on page 321

Clearing Cached Business Services

A business service is cached when a user logs in who has access to that business service through the responsibility associated with the user. Users have access only to those business services that were defined for applicable responsibilities at the time that they logged in, even though an administrator might have changed access to business services since that time.

If an administrator makes any changes that affect a user's access to a business service and its associated methods, then the administrator must clear the cache in order to instruct the Siebel application to read updated values from the database. Clearing the cache makes these changes to the business service available to users who log in subsequently or who log out and log in again. The Siebel Server does not have to be restarted.

To clear cached business services

1. Navigate to the Administration - Application screen, Responsibilities, and then the Business Service view.
2. Select the business service in the Business Service list, and then click Clear Cache.

   Changes to the business service that you made prior to clicking Clear Cache are made available to end users the next time that they log in.

Related Topic

"Administering Access Control for Business Services" on page 321

Disabling Access Control for Business Services

Enabling access control for business services can have an effect on response times for your Siebel Business Applications. If you do not require access control for business services (that is, you only require prerelease 7.8 access control functionality), then you can disable it at the component level for a specific application. To disable access control for business services, you set the parameter OM - Enable Resource Access Control to FALSE for the selected component. The following procedure demonstrates how to set the value for OM - Enable Resource Access Control.

NOTE: The default value for OM - Enable Resource Access Control is True.

To disable access control for business services

1. Log in as an administrator.
2. Navigate to the Administration - Server Configuration screen, then the Servers view.
3. In the Siebel Servers list, select the Siebel server that hosts the component for which you want to disable access control for business services.
4. In the Components tab, select the component for which you want to disable access control for business services.
5. Click the Parameters tab and query for the parameter OM - Enable Resource Access Control.

   The record for OM - Enable Resource Access Control appears.
6. In the Value on Restart field, enter False.
7. Step off the record to save changes.

Related Topic

"Administering Access Control for Business Services" on page 321

Administering Access Control for Business Processes

Business processes can be accessed by all users by default. However, a user with an administrator login can restrict access to specified business processes and can then associate responsibilities with the restricted business processes, or associate the restricted business processes with responsibilities. This allows the administrator to restrict access to business processes based on the end user's responsibility. To access a restricted business process, an end user must be associated with the responsibility that allows access to it. An end user who is assigned more than one responsibility can access any restricted business process that is associated with one of his or her responsibilities.

To associate business processes with responsibilities, use the same procedures outlined in the following topics describing how to associate business services with responsibilities:

- "Associating a Business Service with a Responsibility" on page 322
- "Associating a Responsibility with a Business Service" on page 323

Clearing Cached Responsibilities

A particular responsibility is cached when a user logs in who has that responsibility. Users have access only to those views that were defined for applicable responsibilities at the time they logged in, even though additional views might have been added by an administrator since that time.

If you add, delete, or modify a responsibility in the Responsibilities view (Responsibilities List View), then you can clear the cache in order to instruct the Siebel application to read updated values from the database. Clearing the cache makes these changes available to users who log in subsequently or who log out and log in again. The Siebel Server does not have to be restarted.

To clear cached responsibilities

1. Navigate to the Administration - Application screen, then the Responsibilities view.
2. In the Responsibilities list, click Clear Cache.

About Configuring Visibility of Pop-Up and Pick Applets

Configuring the visibility of pop-up and pick applets is one method of applying access control to data. Pop-up visibility determines what data is 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 topic provides configuration background information. It does not provide detailed instructions for working in Siebel Tools. For information about using Siebel Tools, see *Configuring Siebel Business Applications*.

There are often circumstances where you need greater flexibility when determining what data is shown in pop-up pick applets. For example:

- Most employees of your company only need to see positions for your organizations when they are assigning a sales representative to the sales team.
- Partner Managers need to see positions for your organization, as well as the partner organizations that they manage.

There are also many scenarios where it is appropriate that your partners have more restrictive visibility than your employees. In order to meet these business requirements, Siebel Business Applications have three capabilities that allow the developer to override the visibility set in the Business Component Popup Visibility Type property at the business component level in favor of another setting. The developer can:

- Set visibility of the Pick List object definition
- Use the visibility Auto All property
- Use the Special Frame Class and User Properties

About Setting Visibility of the Pick List Object Definition

Developers can override the visibility set at the business component level by setting a different visibility type on the Pick List object definition, in the Visibility Type property. When you do this, you override the visibility set at the business component level in a specific instance of that business component for all users of that instance.

For example, you might want partners to be able to add new fund requests and associate those fund requests with campaigns in which they participate. However, you want partners to see only campaigns to which they have access. You can configure a special picklist for this use, and set the visibility on that picklist to Sales Rep, so that partners can only select from accessible campaigns when associating to a fund request.

About 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 checks 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, then this visibility type is 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.

The Visibility Auto All property makes visibility consistent across views and pop-up pick applets. It can override any other visibility type, including Sales Rep, Manager, Organization, and so on. In addition to the Business Component and Pick List properties, the Visibility Auto All property can be set on the Link object as well. The Visibility Auto All property is often used for executives or administrative users, who would usually have access to all of the data in your Siebel application.

About Using the Special Frame Class and User Properties

The developer can use a special frame class and user properties to set visibility for a pick applet on the applet object depending on which application is being used. For example, if users are running Siebel Sales, then the Pick Positions applet for the sales team shows positions only for the user's organization. If users are running Siebel Partner Manager, then 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, then change the frame class of the applet to CSSSWEFrameListVisibilityAssoc.
- If the applet whose visibility is to be overridden is a pick applet, then change the frame class of the applet to CSSSWEFrameListVisibilityPick.
- If the applet whose visibility is to be overridden is an MVG applet, then change the frame class of the applet to CSSSWEFrameListVisibilityMvg.

- Add an applet user property called Override Visibility, with the following values:
  - Name: Override Visibility: [*Application Name*]
  - Value: [*Visibility Type*] where the developer can choose from the standard visibility types
- Set the business component user property Popup Visibility Auto All to FALSE.

The developer can also set visibility on an applet based on whether the user has access to a view or not. The developer must change the frame class of the applet to CSSSWEFrameListVisibilityPick and add the following user property to the applet:

- Name: Override Visibility View: [*View Name*]
- Value: [*Visibility Type*] where the developer can choose from the standard visibility types

For example, to override Campaign Pick Applet popup visibility to All if the user has access to the Campaign Administration List view, add the user property with the following values:

- Name: Override Visibility View: *Campaign Administration List*
- Value: *All*

About Configuring Drilldown Visibility

You can control access to data by configuring the visibility to drilldown views. Drilldown visibility can occur within the same business object or between different business objects. The following sections provide more details on each scenario.

Drilldown Visibility Within the Same Business Object

If the original view and drilldown view are both based on the same business object, and visibility is unspecified in the drilldown view, then 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, then drilling down on a record takes the user to the first visible record of the destination view. It does not to the drilldown record.

Drilldown Visibility Between Different Business Objects

If the original view and drilldown view are based on different business objects, then moving from the original view to the drilldown view might require that you configure visibility in the drilldown view to something other than its standard setting.

If you have to configure visibility in the drilldown view, then note that two types of drilldown object exist:

- ID-based drilldown object
- Bookmark-based drilldown object

The drilldown object is ID-based when it has values specified for the Business Component and Source Field properties. Otherwise, it is a bookmark-based drilldown object.

The visibility rules in the drilldown view are the same for the two types of drilldown object, with the following exception; for an ID-based drilldown, setting the Visibility Type property of an applet's drilldown object overrides the Visibility Applet Type setting of the drilldown view. For example, assume you configure a drilldown object with a visibility type of All. It overrides other visibility types (for example, Sales Rep visibility) on the drilldown view when the user drills down.

The Visibility Type property in a drilldown object only overrides the drilldown view Visibility Applet Type property once, that is, when you drill down. If you navigate to another view in the screen and then return to the drilldown view, then the original visibility of the drilldown view is applied. The visibility is refreshed every time you navigate to a different view in the same screen after drilling down.

For example, assume that you navigate to a view with personal access control in the same screen after drilling down; the drilldown record is no longer visible. If you then navigate back to your original drilldown view (with Sales Rep visibility), then the drilldown record remains invisible. If you navigate to a third view with All visibility, then you can see your drilldown record again.

Visibility Rules for the Drilldown Object Type

If the drilldown view is a detail view that does not have visibility specified and the drilldown object does not have visibility specified, then visibility on the drilldown view's screen applies in the following order:

- All
- Organization
- Manager
- Sales Rep

The above scenario assumes that the business component is configured for visibility.

NOTE: You can only specify visibility on an ID-based drilldown object. For more information about the Drilldown object type, see *Siebel Object Types Reference*.

Visibility Rules for the Link Object Type

After you drill down to another screen, the thread bar is updated. The current view displays its records using a master-detail relationship, based on the value of the link property Visibility Rule Applied in the original view (before the drilldown).

If Visibility Rule Applied is set to Never, then no additional visibility rules apply. The thread context's master-detail relationship determines the records visible in the view, regardless of the visibility setting for the current view. If you change the view using the link bar, then the thread context is retained. Records might be displayed that normally (without the thread context) are not visible in this new view.

If Visibility Rule Applied is set to Always, then additional visibility rules apply. The Siebel application might display an error message when a user performs a drilldown to notify the user that he or she does have the appropriate privileges to see the detail records. For more information about the Link object type, see *Siebel Object Types Reference*.

Example of Visibility in a Drilldown Between Different Business Objects

The following example illustrates how the visibility rules described above apply when a user drills down from the Opportunity business object to the Quote business object. In the Opportunity Quote View, a user drills down on the Name field of an entry in the Opportunity Quote List Applet to the Quote Detail View. In the screen (Quotes Screen) of Quote Detail View, the visibility type of all views accessible by the user are checked. Visibility is applied in the following order:

- If an accessible view has visibility equal to All, then this visibility applies after the user drills down to Quote Detail View.
- If an accessible view has visibility equal to Organization, then this visibility applies after the user drills down to Quote Detail View.
- If the user's position equals Manager and an accessible view has visibility equal to Manager, then Manager visibility applies after the user drills down to Quote Detail View.
- If an accessible view has visibility equal to Sales Rep or Personal, then this visibility applies after the user drills down to Quote Detail View.

An error message appears if the user does not have the appropriate visibility to view the record in the Quote Detail view.

Party Data Model

The S_PARTY table is the base table for all of the parties listed in Table 24 on page 261: Person (Contact), User, Employee, Partner User, Position, Account, Division, Organization, Partner Organization, Household, User List, and Access Group.

For each party record stored in the S_PARTY table, the value of the PARTY_TYPE_CD column denotes the party type. Along with the party type, extension tables provide the primary differentiation between the different parties.

For information about how joins are used to draw data from multiple tables into a single business component, such as is done for Employee, Account, and other business components for party-type data, see *Configuring Siebel Business Applications*.

In Figure 14 on page 333, the base table and extension tables that make up the party data model are shown within the Party boundary box (all of the shaded area). The three tables shown outside of the Party boundary are used to define relationships among parties. Sections that follow illustrate how the party data model applies to various particular parties.

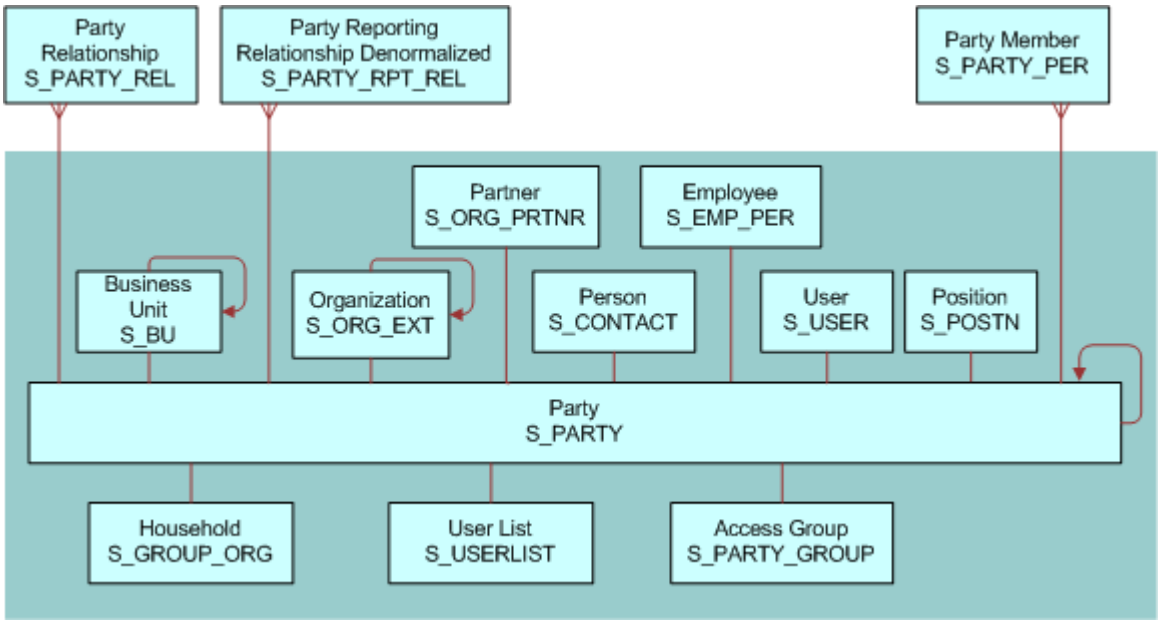

Figure 14. Party Data Model

How Parties Relate to Each Other

Parties have some required relationships, as described below.

- Divisions, organizations, and accounts are instances of the Organization party type.
- A division, internal or partner, is also an organization if its internal organization flag is TRUE (INT_ORG_FLG = “Y”) and it has an associated S_BU record.
- Every division is associated with one organization: either itself or the closest ancestor division that is also an organization.
- Every position is associated with a division. The position is then also automatically associated with one organization: the organization with which the division is associated.
- Persons (contacts), users, employees, partner users are instances of the Person party type.
- Typically, you associate each employee and partner user with one or more positions. The employee or partner user has only one active position at one time. The employee or partner user is automatically associated with one division and one organization at a time; the division and organization associated with the active position.

  CAUTION: Merging employee records is not recommended. You can disrupt party relationships to a significant extent and get unexpected results.

- For purposes of granting visibility to data, associations of parties of type Person with other types of parties are stored using the S_PARTY_PER table. For example, accounts are associated with contacts, users are associated with positions, and so on. A user associated with a position can see data for accounts or opportunities assigned to the position (when this is the active position). Relationships stored in S_PARTY_REL also affect data routing for mobile users.
- Nonstructured and informational relationships between parties are stored in the table S_PARTY_REL. For example, a company and its accounting firm might both be stored as accounts. The relationship between these two accounts can be stored in the S_PARTY_REL table, assuming that your application has been configured to define these relationships.

Person (Contact) Data Model

In Figure 15, the base table and extension table (S_CONTACT) that define a Person, or Contact, are highlighted. A Person is the simplest representation of an individual in the database.

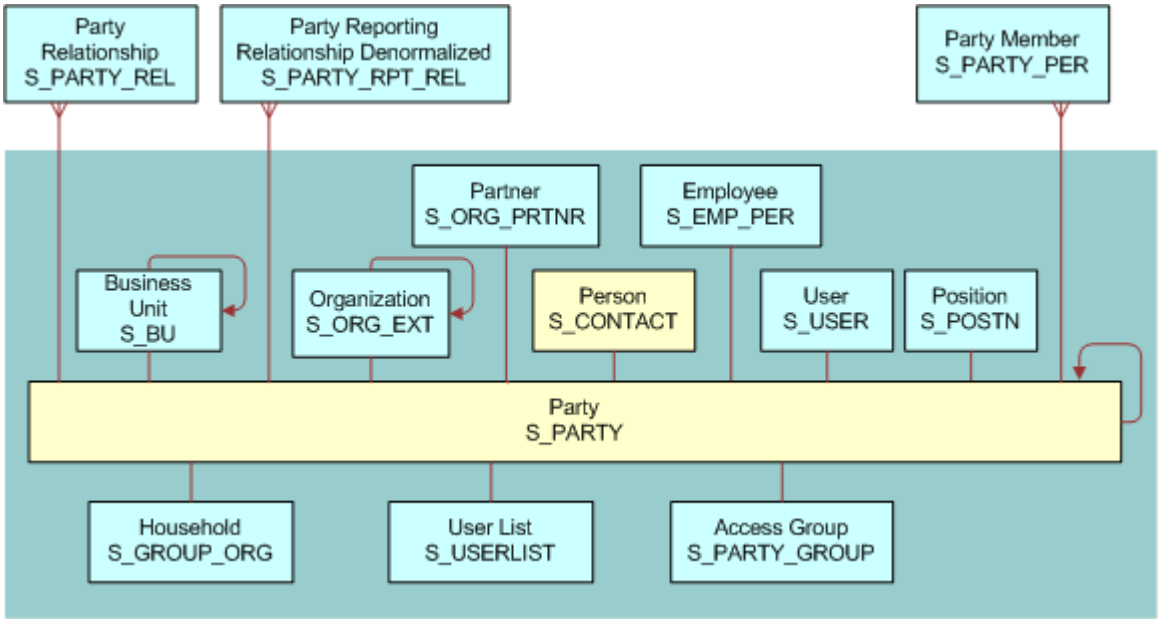

Figure 15. Person (Contact) Data Model

User Data Model

In Figure 16 on page 335 the base table and extension tables (S_CONTACT and S_USER) that define a User are highlighted. A User is a Person with the following added qualities:

- The S_USER table contains a login for this user.
- The S_PER_RESP intersection table (not shown) specifies a responsibility for this user.

- It is possible to promote a contact to a user. For example, adding a User ID value for a person in the All Persons view in the Administration - User screen causes the person to appear as a user in the Users view.

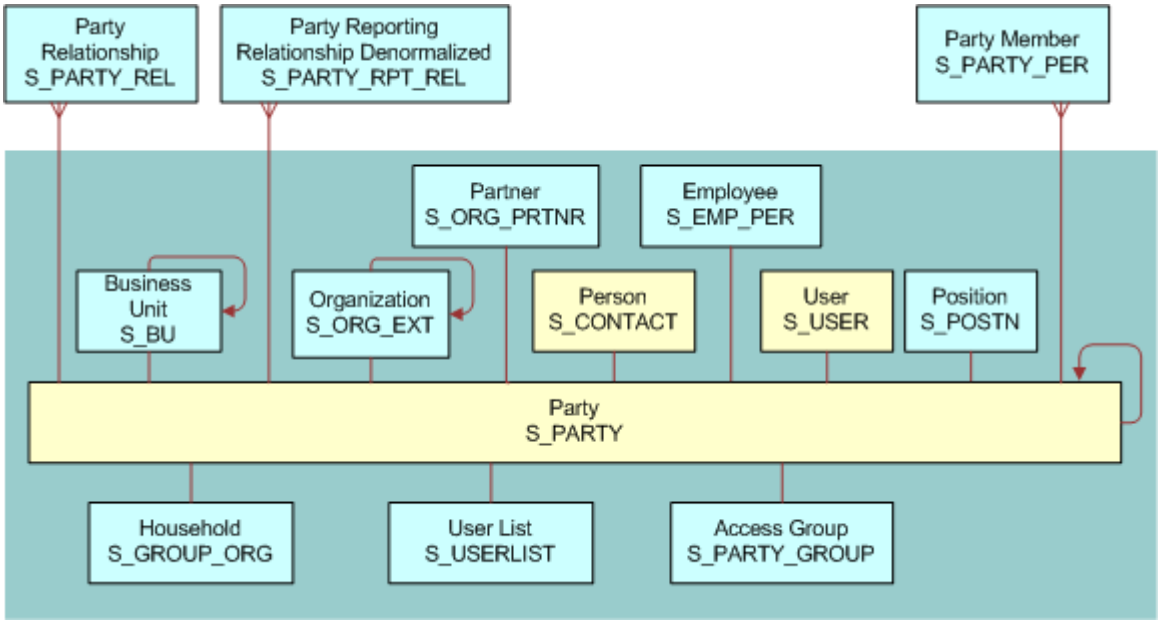

Figure 16. User Data Model

Employee Data Model

In Figure 17 on page 336 the base table and extension tables (S_CONTACT, S_USER, and S_EMP_PER) that define an Employee are highlighted. 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.

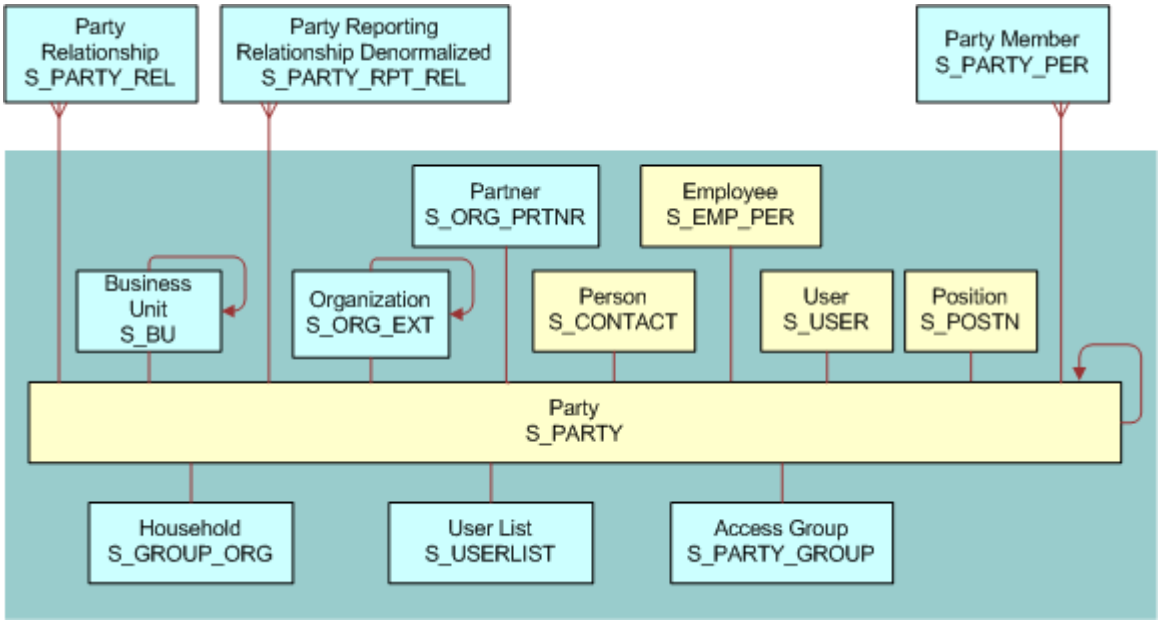

Figure 17. Employee Data Model

Position Data Model

In Figure 18 on page 337 the base table and extension table (S_POSTN) that define a Position are highlighted.

NOTE: In positions, as in other areas of your Siebel application, foreign key references are implemented with the ROW_ID column in the base tables. The ROW_ID column is not visible in the user interface and cannot be changed manually. This is because the integrity between the various base tables would be lost if users were allowed to change this value. Changing a position name does not affect the foreign keys (the ROW_ID in the underlying base table).

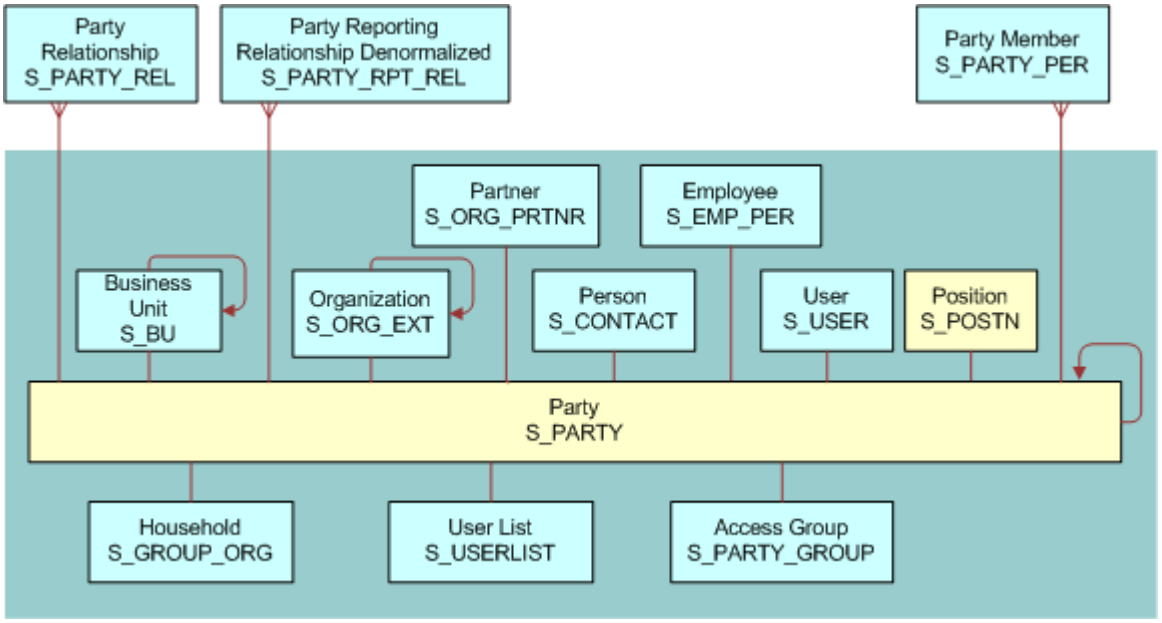

Figure 18. Position Data Model

Account Data Model

In Figure 19 on page 338 the base table and extension table (S_ORG_EXT) that define an Account are highlighted.

NOTE: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.

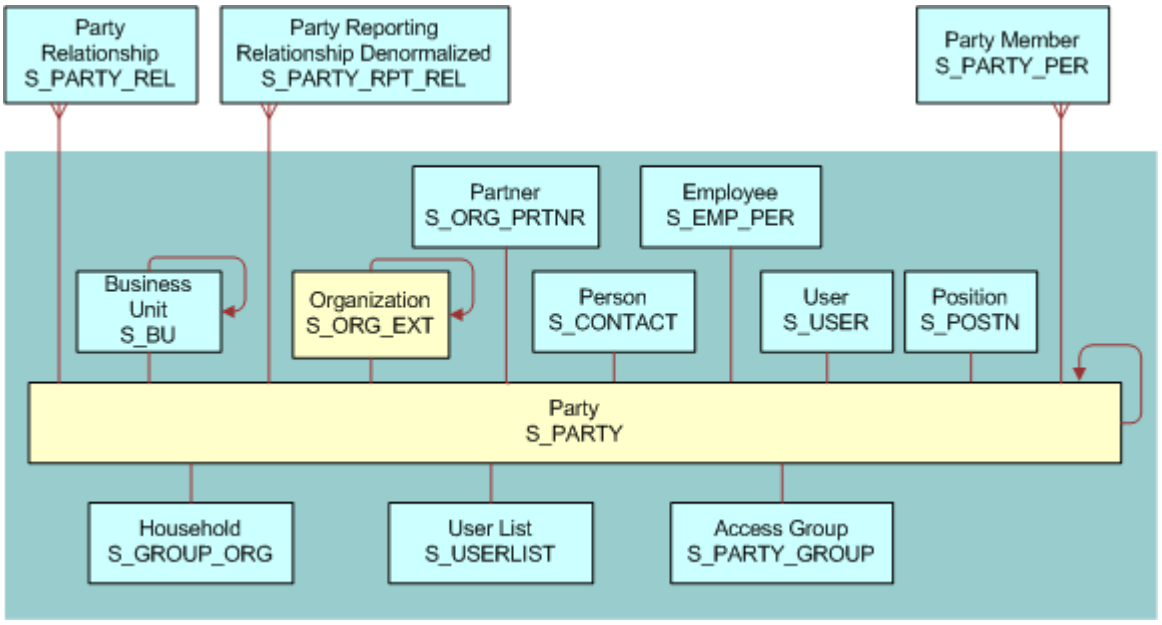

Figure 19. Account Data Model

Division Data Model

In Figure 20 on page 339 the base table and extension table (S_ORG_EXT) that define a Division are highlighted. 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.)

NOTE: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.

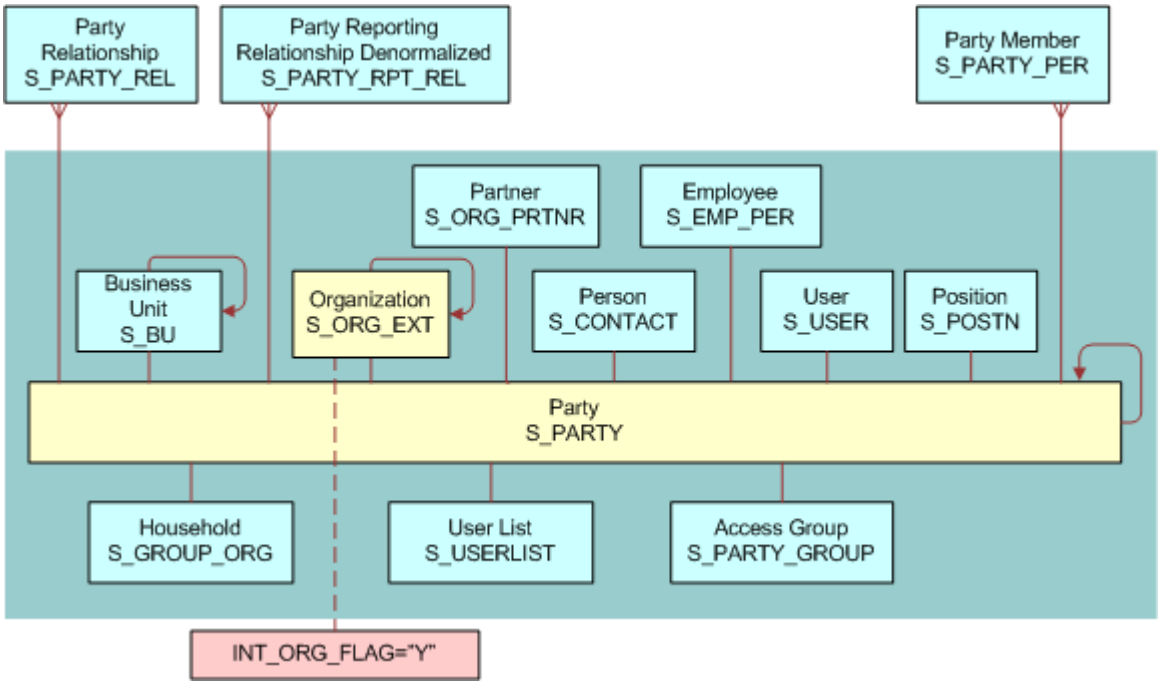

Figure 20. Division Data Model

Organization Data Model

In Figure 21 on page 340 the base table and extension tables (S_ORG_EXT and S_BU) that define an Organization are highlighted. An Organization, sometimes known as a business unit, is also a Division, but has a record in the S_BU table.

NOTE: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.

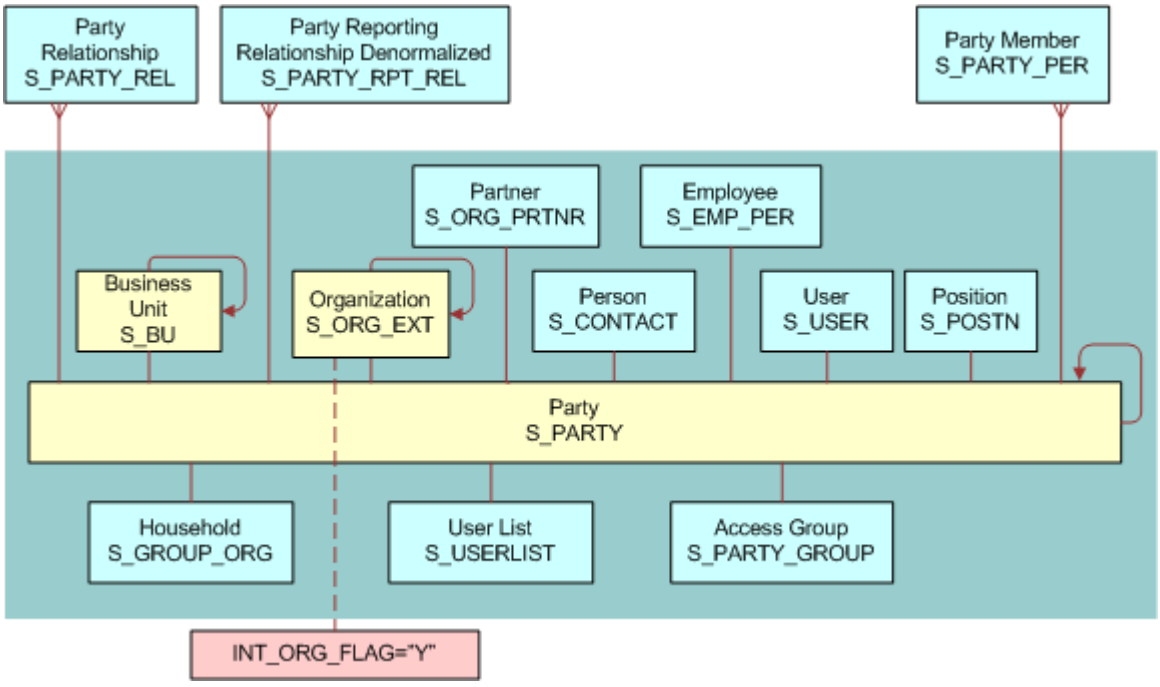

Figure 21. Organization Data Model

Partner Organization Data Model

In Figure 22 on page 341 the base table and extension tables (S_ORG_EXT, S_BU, and S_ORG_PRTNR) that define a Partner Organization are highlighted. A Partner Organization is the same as an Organization but the flag PRTNR_FLG in S_ORG_EXT qualifies it as a Partner Organization.

NOTE: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.

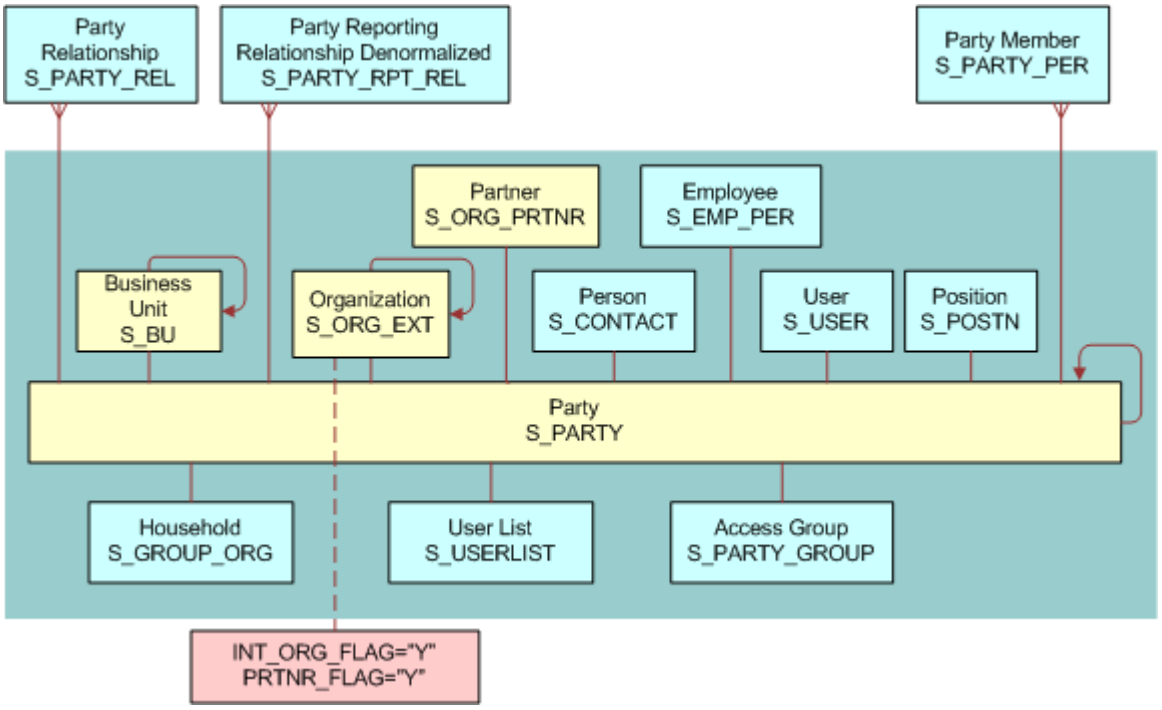

Figure 22. Partner Organization Data Model

Household Data Model

In Figure 23 on page 342 the base table and extension table (S_ORG_GROUP) that define a Household are highlighted.

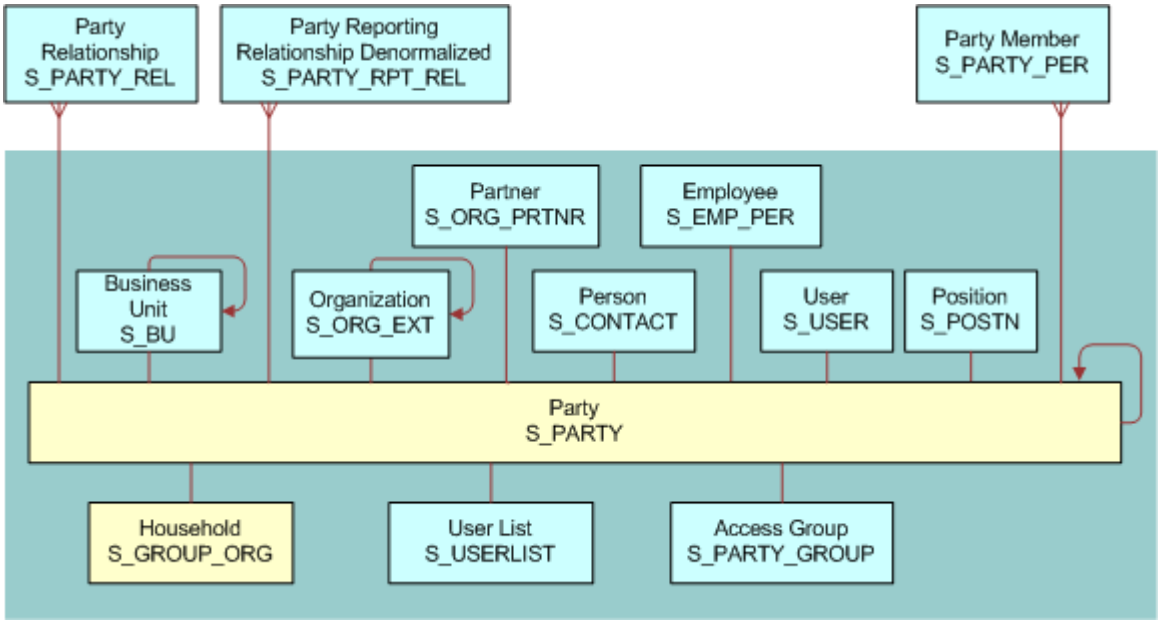

Figure 23. Household Data Model

User List Data Model

In Figure 24 on page 343 the base table and extension table (S_USERLIST) that define a User List are highlighted.

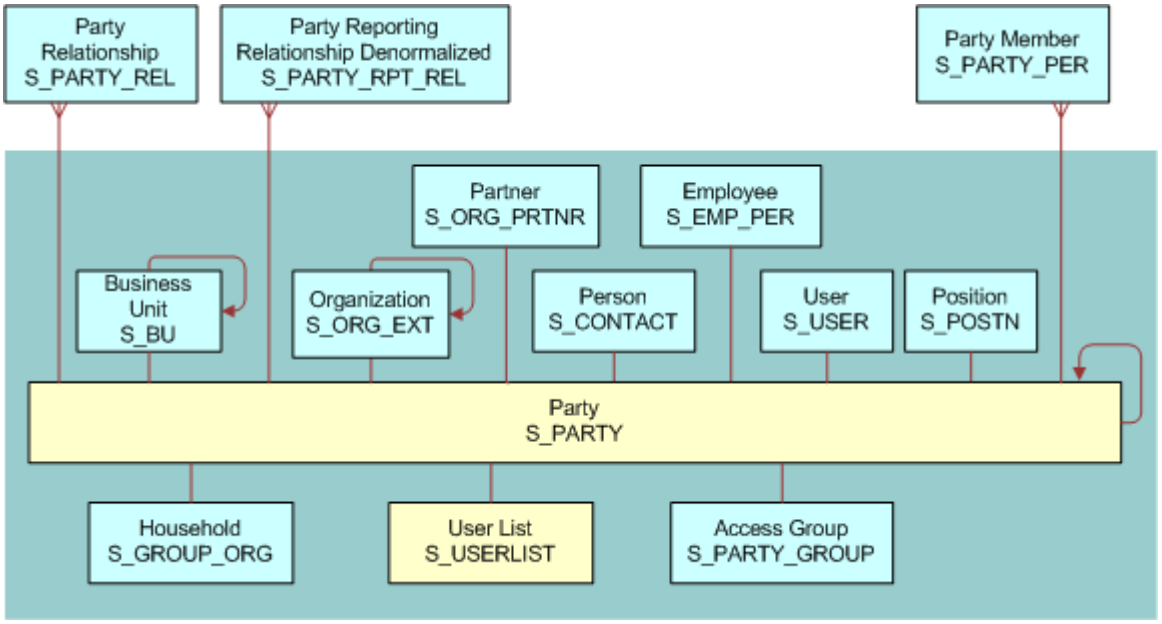

Figure 24. User List Data Model

Access Group Data Model

In Figure 25 on page 344 the base table and extension table (S_PARTY_GROUP) that define an Access Group are highlighted.

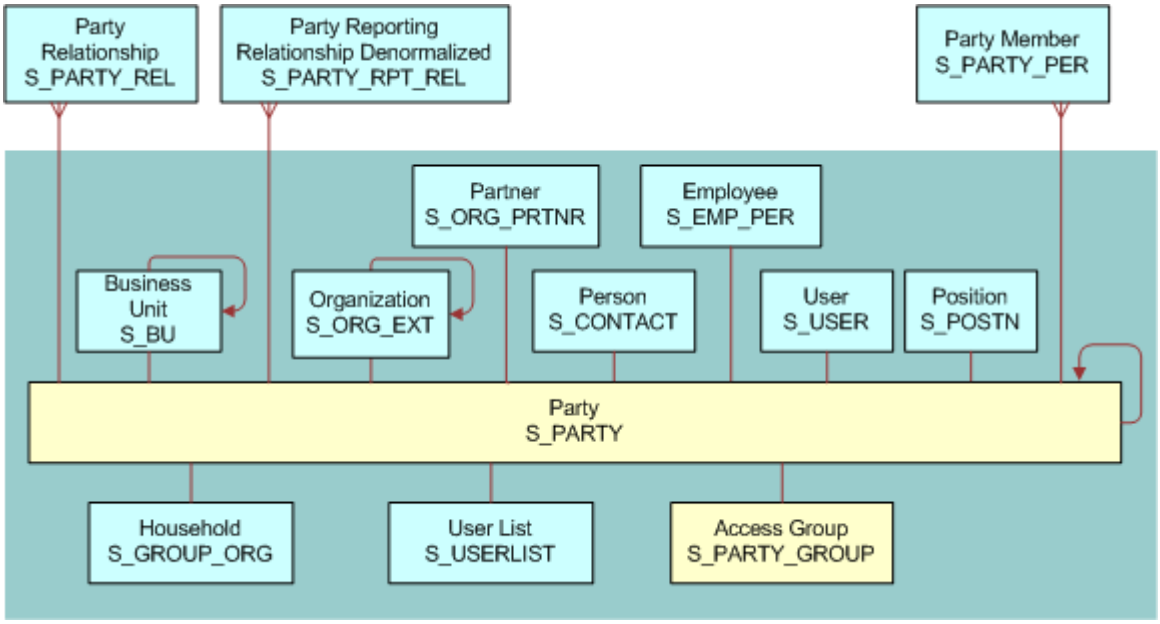

Figure 25. Access Group Data Model

10 Troubleshooting Security Issues

This chapter provides troubleshooting tips and information about security-related issues that can occur in Siebel Business Applications. It includes the following topics:

- Troubleshooting User Authentication Issues on page 346
- Troubleshooting User Registration Issues on page 348
- Troubleshooting Access Control Issues on page 350

Troubleshooting User Authentication Issues

This topic describes problems that can occur when authenticating users. To resolve the problem, look for it in the list of Symptoms or Error Messages in Table 29.

Table 29. Troubleshooting User Authentication Issues

Symptom or Error Message	Diagnostic Steps or Cause	Solution
User is unable to access the Administration - Server Configuration or Administration - Server Management screen. If the Siebel system is configured to use the Siebel Audit Trail feature, then problems running audit trail occur.	This problem can occur when using external authentication, either Web SSO or Siebel security adapter authentication. 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 returns the user's Siebel user ID and, typically, a database account used by many users from a Lightweight Directory Access Protocol (LDAP) or Active Directory Service Interfaces (ADSI) directory.	Use database authentication instead of external authentication for administration users. Administrator users must log into the application using either a different Application Object Manager or a Siebel Developer Web Client; in each case, database authentication must be configured. For more information about database authentication, see "About Database Authentication" on page 102 and related sections. Alternatively, authentication for a secondary data source such as the Siebel Gateway Name Server can be configured.
Adding users or changing passwords is not reflected in the directory.	The PropagateChange parameter is set to FALSE for the security adapter.	Set the PropagateChange parameter to TRUE for the security adapter. For more information, see "Siebel Gateway Name Server Parameters" on page 361.
Responsibilities in the directory conflict with responsibilities in Siebel Business Applications.	User responsibilities are assigned in the directory and in Siebel Business Applications.	It is recommended that you assign user responsibilities in the directory or by using Siebel Business Applications, but not both. For more information, see "Configuring Roles Defined in the Directory" on page 157.

Table 29. Troubleshooting User Authentication Issues

Symptom or Error Message	Diagnostic Steps or Cause	Solution
Upgrading Siebel Business Applications appears to disable Checksum validation.	A security adapter's CRC checksum value must be recalculated whenever you upgrade Siebel Business Applications.	Recalculate the security adapter's CRC checksum value when you upgrade Siebel Business Applications. For information, see "Configuring Checksum Validation" on page 149.

The following error message appears in the application log file:
`Web authentication failed`
	If your installation is configured for Web SSO (without anonymous browsing) and the ProtectedVirtualDirectory parameter is not set, then this message can appear.	Set the ProtectedVirtualDirectory parameter in the eapps.cfg file to the same value as the application directory. For example:
		`[/eSales]`
		`ProtectedVirtualDirectory =/eSales`

Troubleshooting User Registration Issues

This topic describes problems that can occur when users are registered. To resolve the problem, look for it in the list of Symptoms or Error messages in Table 30.

Table 30. Troubleshooting User Registration Issues

Symptom or Error Message	Diagnostic Steps or Cause	Solution
Workflows do not appear in the Business Process Administration screen.	Your server or application is probably running on a different language from the database. For example, a DEU installation is running against an ENU database.	Check your setup. Using Server Manager, connect to the server and run the following command to verify the language: `list param lang` If the language code is incorrect, then run the following command: `change param lang=`*`LANGUAGE`* where *LANGUAGE* is your three-letter database language code. Restart the server.
When I click New User, either nothing happens or an error message appears.	Possible causes include: ■ One or more of the necessary User Registration workflows have not been activated. ■ The language of the 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 "About Activating Workflow Processes for Self-Registration" on page 222. ■ Using Server Manager, connect to the server and run the following command to verify the language: `list param lang` If the language code is incorrect, then run the following command: `change param lang=`*`LANGUAGE`* where *LANGUAGE* is your three-letter database language code. Restart the server.

Table 30. Troubleshooting User Registration Issues

Symptom or Error Message	Diagnostic Steps or Cause	Solution
When I click finish, the following message appears: `Error updating business component at step Insert New User`	The problem can occur if the user being created already exists 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 or not the user exists in the directory. Connect to the LDAP directory, but instead of creating a new user, right-click on People and select Search.
After I click Finish, the following message appears: `View not accessible`	The user was successfully created and could log in. However, the user did not receive the appropriate responsibility and so 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 are not activated; or if they are, the server needs to be restarted.	In the Administration - Server Management screen, restart only the necessary Application Object Managers. Restarting the server also works.
When I click Next in a User Registration view, nothing happens.	There might be another workflow that is being triggered which is disrupting the User Registration workflow. It is also possible that not all necessary workflows have been activated.	Activate all necessary workflows and deactivate any disruptive workflows. For information on these tasks, see: ■ "About Activating Workflow Processes for Self-Registration" on page 222 ■ "Identifying Disruptive Workflows" on page 232
When I click Finish, an error is returned.	Possible causes include: ■ The SecThickClientExtAuthent system preference is not set to TRUE. For information about this system preference, see "Setting a System Preference for Developer Web Clients" on page 143. ■ The Siebel Server has not been restarted since setting the system preferences.	Check to see if the user exists in the Person view in the Administration - User screen. If the user exists but was not given an entry in the LDAP directory, then that user cannot 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, then try to log in as that person.

Troubleshooting Access Control Issues

This topic describes problems related to access control. To resolve the problem, look for it in the list of Symptoms or Error messages in Table 31.

Table 31. Troubleshooting Access Control Issues

Symptom or Error Message	Diagnostic Steps or Cause	Solution
Employee user has trouble logging into a Siebel customer application.	It is not recommended to use an Employee login account to access a customer application (such as Siebel Sales).	Give the Employee user a separate login account for the customer application.
Cannot delete Division records.	You cannot delete division records because business components throughout your Siebel application refer to organizational records. Deleting a division might cause invalid references on transactional records.	Rename the division or promote the division to an organization.
Cannot modify seed responsibility.	Seed responsibilities cannot be modified or deleted.	Make a copy of the seed responsibility you want to modify and make changes to the copy.

Table 31. Troubleshooting Access Control Issues

Symptom or Error Message	Diagnostic Steps or Cause	Solution
Excessive synchronization time for some Mobile users.	The Local Access control field in the Responsibility View list might not be set properly. This setting determines which views mobile users can work in offline.	Make sure the Local Access control field in the Responsibility View list is set properly. For faster synchronization time, reduce the number of views that have local access. For more information, see "Local Access for Views and Responsibilities" on page 288.
Unexpected refresh causes loss of data.	When you enter records on particular views (for example, Service Request List View), records can appear lost if the underlying business component is re-queried before a user is assigned to the access list. This event can occur if the associated detail applet (for example, Service Request Entry applet) expands or collapses to show or hide additional fields. By default, if you collapse or expand a detail applet, the record is committed and the business component is queried again.	You can override the default behavior by setting the user property RestrictedFieldActivation to FALSE; this stops the business component from being re-queried if the detail applet expands or collapses. You can set RestrictedFieldActivation to FALSE in a number of locations. However, for scalability reasons, it is recommended that you only set RestrictedFieldActivation to FALSE in the applet. To set the value of RestrictedFieldActivation in the applet, you add it to the user properties of the applet in Siebel Tools. You can also specify the view mode where you disable an automatic re-query of the business component when a detail applet collapses or expands. To specify the view mode, add the following entry to the user properties of the applet in Siebel Tools: `NoRestrictedFieldActivationMode`*`number`* *`valueOfVisibilityMode`* For example, the following entry overrides the default behavior in the Personal view mode: `NoRestrictedFieldActivationMode1 Personal`

A Configuration Parameters Related to Authentication

This appendix describes the configuration parameters that are applicable to implementing a security adapter. It includes the following topics:

- About Parameters in the eapps.cfg File on page 353
- Siebel Gateway Name Server Parameters on page 361
- Parameters in the Gateway.cfg File on page 372
- Siebel Application Configuration File Parameters on page 376

NOTE: In general, parameter values related to security adapter configuration must be verified by your Lightweight Directory Access Protocol (LDAP) or Active Directory Service Interfaces (ADSI) administrator, or database administrator. Many values shown are examples only and might not be suitable for your deployment.

About Parameters in the eapps.cfg File

The eapps.cfg file contains parameters that control interactions between the Siebel Web Engine and the Siebel Web Server Extension (SWSE) for all Siebel Business Applications deploying the Siebel Web Client. The eapps.cfg file is located in the *SWEAPP_ROOT*\bin directory after you apply a SWSE logical profile, where *SWEAPP_ROOT* is the directory in which you installed the SWSE.

The eapps.cfg file includes sections such as [swe], [defaults], and [connmgmt] and sections for individual Siebel Business Applications, such as [/prmportal_enu] and [/callcenter_enu]. Each parameter value in the [defaults] section is used by all individual applications, unless you override the parameter's value with an entry in an application's own section.

You can edit the parameters in the eapps.cfg file manually using a text editor or you can configure and apply a SWSE logical profile using the Siebel Configuration Wizard. When you edit configuration files, do not use a text editor that adds additional, nontext characters to the file. For information on using the Siebel Configuration Wizard to configure SWSE parameters, see *Siebel Installation Guide* for the operating system you are using.

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

For more detailed information on the eapps.cfg file parameters, see:

- "Authentication-Related Parameters in Eapps.cfg" on page 355
- "SSL and TLS-Related Parameters in Eapps.cfg" on page 360

Sample Eapps.cfg File

The following is a portion of a sample eapps.cfg file. This sample includes some parameters that might not coexist. They are provided so you can see a range of authentication-related parameters. In the eapps.cfg sample, the AnonUserName and AnonPassword values in the [/prmportal_enu] section are used by Siebel Partner Portal instead of the values provided in the [defaults] section.

```
[swe]
Language = enu
Log = all
LogDirectory = D:\sba8x\SWEApp\log
ClientRootDir = D:\sba8x\SWEApp
IntegratedDomainAuth = FALSE

[defaults]
EncryptedPassword = TRUE
AnonUserName = GUESTCST
AnonPassword = fhYt8T*9N4e8&Qay
StatsPage = _492394stats.swe
SingleSignOn = TRUE
TrustToken = mR*739DAPw*94%O2

WebPublicRootDir = D:\sba8x\SWEApp\public\enu
SiebEntSecToken = fJq&29&58hJaY(A8!Z
UserSpec = REMOTE_USER
UserSpecSource = Server
DoCompression = TRUE
SessionTimeout = 900
GuestSessionTimeout = 300
SessionTimeoutWarning = 300

[/prmportal_enu]
AnonUserName = guestcp
AnonPassword = aGr^92!8RWnf7Iy1
ProtectedVirtualDirectory = /p_prmportal_enu
ConnectString = siebel.TCPIP.None.None://172.20.167.200:2320/SBA_8x/
eChannelObjMgr_enu
SiebEntSecToken = ^s*)Jh!#7^s*)Jh!#7

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

Typically, password encryption is in effect by default for the eapps.cfg file, as determined by the setting EncryptedPassword = TRUE. In this case, values for SiebEntSecToken, AnonPassword, and TrustToken must be encrypted. For more information, see "Encrypted Passwords in the eapps.cfg File" on page 46.

NOTE: It is recommended that you set the value for StatsPage to a value other than the default value (_stats.swe).

Authentication-Related Parameters in Eapps.cfg

Table 32 lists the parameters in the eapps.cfg file that relate to authentication. The authentication parameters can be defined in the [defaults] section of the file or in the sections for individual applications.

Table 32. Authentication-Related Parameters in the Eapps.cfg File

Parameter	Description
AnonUserName	This parameter specifies the user name required for anonymous browsing and initial access to the login pages. The user name selected as the anonymous user must be assigned access to views intended for anonymous browsing, but to no other views.
AnonPassword	The password corresponding to the value entered for AnonUserName.
ClientCertificate	When this parameter is set to TRUE in a Web SSO implementation, the user is authenticated through a digital certificate. For information, see "About Digital Certificate Authentication" on page 191.
EncryptedPassword	When this parameter is set to TRUE, the password for the anonymous user and the Web update password are interpreted as encrypted passwords. This parameter is added to the eapps.cfg file (with a value of TRUE) when you apply a SWSE logical profile using the Siebel Configuration Wizard for SWSE. However, if the parameter is not defined in the file, this is equivalent to a value of FALSE. For additional information, see "Encrypted Passwords in the eapps.cfg File" on page 46.
EncryptSessionId	When this parameter is set to TRUE (the default), the session ID is encrypted. When it is FALSE, the session ID is not encrypted. For a Siebel Web Client, the session ID is used in the session cookie (in cookie-based mode) or in the application URL (in cookieless mode). For more information about cookies, see "About Using Cookies with Siebel Business Applications" on page 206.

Table 32. Authentication-Related Parameters in the Eapps.cfg File

Parameter	Description
GuestSessionTimeout	The time, in seconds, that a connection open for anonymous browsing can remain idle before it times out. The default is 300 seconds (5 minutes). Guest sessions are used for anonymous browsing. They permit users to navigate portions of the site without logging in. In contrast to anonymous sessions, guest sessions are associated with an individual Siebel Web Client. These sessions are opened when an unregistered user starts navigating the site, and they remain open until the Web client logs out or times out due to inactivity. When deciding the value to specify for guest user timeout, the primary consideration is whether or not anonymous browsing is being used. If it is, then set guest user timeouts to be greater than the average time users need to deliberate their next action. In other words, this is the time allowed between user actions. Both guest and anonymous sessions use the AnonUserName and AnonPassword parameters to log in.
SessionTimeout	The time, in seconds, from the user's last browser request until the user's connection times out. The default is 900 seconds (15 minutes). Standard sessions are those where users log in using their registered user name and password. Otherwise, standard sessions share many of the same characteristics as guest sessions. For guidelines on setting a value for the SessionTimeout parameter, see "About the SessionTimeout Parameter" on page 359.

Table 32. Authentication-Related Parameters in the Eapps.cfg File

Parameter	Description
SessionTimeoutWarning	Before a session times out, a prompt is displayed allowing users to choose whether or not to extend the session. The time at which this prompt appears is determined by the value selected for the SessionTimeoutWarning parameter. The default value is 60 seconds. **NOTE:** The SessionTimeoutWarning functionality is supported with Siebel standard-interactivity applications only; it is not supported with Siebel high-interactivity applications or with Siebel Open UI. The time at which the timeout warning prompt is displayed is calculated by subtracting the value of the SessionTimeoutWarning parameter from the value of the SessionTimeout parameter. For example, if the SessionTimeout parameter is set to the default value of 900 seconds, and the SessionTimeoutWarning parameter is set to a value of 300 seconds, the timeout warning prompt is displayed after 600 seconds of inactivity (900 minus 300 equals 600). If the user selects OK in response to the timeout warning prompt, then the session timer is reset to zero and is only activated again after another 600 seconds of inactivity have elapsed. If the user selects Cancel, then the session is terminated once the session timeout period is reached. If you do not want users to see a timeout warning prompt, then set the value of the SessionTimeoutWarning parameter to one of the following: ■ - (minus symbol) ■ never ■ 0
SingleSignOn	The SWSE operates in Web SSO mode when this parameter is TRUE. For more information, see Chapter 6, “Web Single Sign-On Authentication.”
SubUserSpec	In a Web SSO environment that implements digital certificate authentication, a value of CN specifies that the Siebel user ID is to be extracted from the certificate’s CN (Common Name) attribute. For more information, see “Configuring the User Specification Source” on page 192.
TrustToken	In a Web SSO environment, this token string is a shared secret between the SWSE and the security adapter. It is a measure to protect against spoofing attacks. This setting must be the same on both the SWSE and the security adapter. For more information, see Chapter 6, “Web Single Sign-On Authentication.”

Table 32. Authentication-Related Parameters in the Eapps.cfg File

Parameter	Description
UserSpec	In a Web SSO implementation, this variable name specifies where the SWSE looks for a user's user name within the source given by UserSpecSource. The value, REMOTE_USER, by default is populated by the authentication filter. If digital certificate authentication is implemented on Windows or AIX, then use the value CERT_SUBJECT, a variable that contains the certificate name. For example, UserSpec/SubUserSpec is CERT_SUBJECT/CN. For other UNIX operating systems, use REMOTE_USER for UserSpec. The SubUserSpec setting is disregarded. For more information, see "Configuring the User Specification Source" on page 192.
UserSpecSource	In a Web SSO implementation, this parameter specifies the source from which the SWSE derives the user credentials: Server, if from the usual Web server user name field; Header, if the variable is within the HTTP request header. For more information, see "Configuring the User Specification Source" on page 192.
ProtectedVirtualDirectory Defined in the section for each individual Siebel application in eapps.cfg. Do not define in the [defaults] section.	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. For more information, see "About the Protected Virtual Directory Parameter" on page 359.
IntegratedDomainAuth Defined in the [swe] section of eapps.cfg.	To support Windows Integrated Authentication for Web SSO, set this parameter to TRUE. This setting causes SWSE to strip out the domain name from HTTP headers, which allows the application to integrate with Windows Integrated Authentication.

About the SessionTimeout Parameter

SessionTimeout is the time, in seconds, from the user's last browser request until the user's connection times out. Table 33 offers guidelines for setting this parameter.

Table 33. Guidelines for Setting Session Timeouts

Session Type	Condition	Recommended Setting
Anonymous session	■ Large numbers of users logging in within a short period of time (login spikes) ■ Frequent logins and logouts	Greater than 30 minutes.
Guest	■ Long intervals between user actions ■ Login view is used for logins ■ Logout occurs on a logout view	Greater than 30 minutes. Less than 5 minutes. Less than 5 minutes.
Regular	■ Employee applications ■ Customer applications ■ High security requirements ■ High continuity (low interaction) with the browser ■ Lightly loaded system	Greater than 30 minutes. 1-15 minutes. Less than 5 minutes. Greater than 30 minutes. Greater than 30 minutes.

All the session timeouts mentioned in Table 33 on page 359 refer to session inactivity. That is, if session timeout is set to 3600 seconds, then it requires one hour of session inactivity for that session to time out. Session inactivity means no request is made to the Siebel Server on that session. Any act that sends a ping request to the Siebel Server, such as sending notifications, resets the session timeout period. If the update interval is less than the SessionTimeout set in the eapps.cfg file, then the session never times out.

If you use the Siebel Portal Framework to implement portal views, then note that the Siebel application times out if user activity in the portal view exceeds the time that is specified by SessionTimeout. Note also that, by default, portal views send a ping status request to their server every 120 seconds (2 minutes) to keep their session alive. For more information about the Siebel Portal Framework, see *Siebel Portal Framework Guide*.

About the Protected Virtual Directory Parameter

The ProtectedVirtualDirectory parameter specifies a Web server virtual directory that represents the protected location of the Siebel application. This parameter is required in a Web SSO implementation.

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 "(Optional) Creating Protected Virtual Directories" on page 183.

For example, if you used the suggested name for the protected virtual directory for Siebel eService, enter:

```
[/eservice_enu]
ProtectedVirtualDirectory = /p_eservice
```

If your Web SSO implementation is not configured for anonymous browsing, then set this value to the same directory as your application. For example:

```
[/eservice_enu]
ProtectedVirtualDirectory = /eservice
```

Otherwise, a Web Authentication Failed message might appear in the application's log file.

NOTE: You use examples like those above to secure an entire application. However, if some parts of the application do not require authentication, you must be able to authenticate users when they access a secured part of the application. In this case, set the parameter to an alias where the Web SSO credentials are passed. The Siebel application redirects the authentication request.

SSL and TLS-Related Parameters in Eapps.cfg

SSL and TLS-related parameters can be included in the [connmgmt] section of the eapps.cfg file if you are using SSL or TLS to encrypt SISNAPI communications between the Web server and the Siebel Server. Table 34 describes these parameters. For more information on configuring SSL or TLS encryption, see "Configuring SSL or TLS Encryption for SWSE" on page 68.

NOTE: The use of SSL encryption is not supported for high-security implementations of Siebel Business Applications. It is recommended that you implement TLS encryption where possible. For additional information, see "Using Secure Socket Layer v3.0 with Siebel CRM" on page 55.

Table 34. SSL / TLS Parameters in the Eapps.cfg File

Parameter Name	Description
CACertFileName	Identifies the trusted authority who issued the certificate.
CertFileName	Specifies the name of the ASN.1/PEM certificate file.
KeyFileName	Specifies the name of the PEM private key file.
KeyFilePassword	Specifies the password to decrypt the private key file.

Table 34. SSL / TLS Parameters in the Eapps.cfg File

Parameter Name	Description
PeerAuth	Enables peer authentication during the SSL or TLS handshake. PeerAuth is FALSE by default. Set PeerAuth to TRUE to authenticate certificates from the Siebel Server. The SWSE requires the certifying authority's certificate to authenticate the certificate from the Siebel Server.
PeerCertValidation	Independently verifies that the hostname of the SWSE computer matches the hostname presented in the certificate.

For additional information on the eapps.cfg file, see "About Parameters in the eapps.cfg File" on page 353 and "Authentication-Related Parameters in Eapps.cfg" on page 355.

Siebel Gateway Name Server Parameters

Parameters for the Siebel Gateway Name Server can be set at one or more of the Enterprise, Siebel Server, or component levels. They are set in the Administration - Server Configuration screen of a Siebel employee application, such as Siebel Call Center. The following rules apply:

- Parameters you set at the Enterprise level configure all Siebel Servers throughout the enterprise.
- Parameters you set at the Siebel Server level configure all applicable components on a specific Siebel Server.
- Parameters you set at the component level configure all the tasks, or instances, of a specific component.
- Parameters you set for an enterprise profile (named subsystem) configure the applicable security adapter.

For purposes of authentication, most of the components of interest are Application Object Managers, such as the Call Center Object Manager or the eService Object Manager. The Synchronization Manager component also supports authentication.

A particular parameter set at a lower level overrides the same parameter set at a higher level. For example, if Security Adapter Mode is set to LDAP at the Enterprise level, and Security Adapter Mode is set to ADSI at the component level for the eService Object Manager component, then the ADSI security adapter is used for Siebel eService.

Parameters configured for Siebel security adapters are configured for the enterprise profile (for GUI Server Manager) or named subsystem (for command-line Server Manager). For more information about configuring security adapters, see Chapter 5, "Security Adapter Authentication."

NOTE: You can set parameters on the Siebel Gateway Name Server using Siebel Server Manager or you can do so using the Siebel Configuration Wizard. For information on editing Gateway Name Server parameters using the Siebel Configuration Wizard, see "Configuring LDAP or ADSI Security Adapters Using the Siebel Configuration Wizard" on page 123. For information on using Siebel Server Manager to edit Gateway Name Server parameters, see *Siebel System Administration Guide*.

The following topics provide detailed information on the Gateway Name Server parameters:

- "Parameters for Database Authentication" on page 362
- "Parameters for LDAP or ADSI Authentication" on page 364
- "Parameters for Custom Security Adapter Authentication" on page 370
- "Parameters for Application Object Manager" on page 371

Parameters for Database Authentication

This topic outlines the Gateway Name Server parameters related to database authentication. The database authentication parameters can be defined for the InfraSecAdpt_DB named subsystem or the InfraDataSource named subsystem.

The parameters in Table 35 are defined for named subsystems of type InfraSecAdpt_DB, that is, they can be set for the DBSecAdpt named subsystem, or a similar security adapter with a nondefault name.

Table 35. Database Authentication Parameters for InfraSecAdpt_DB Named Subsystems

Parameter	Description
CRC (alias DBSecAdpt_CRC)	This parameter is used to implement checksum validation to verify that each user gains access to the database through the correct security adapter. This parameter contains the value calculated by the checksum utility for the applicable security adapter DLL. For more information, see "Configuring Checksum Validation" on page 149. **CAUTION:** Do not reset or change the value of the DBSecAdpt_CRC parameter. Changing the value of this parameter can disrupt the correct functioning of your Siebel application.
DataSource Name (alias DataSourceName)	Specifies the data source for which you are specifying password hashing parameters.

Table 35. Database Authentication Parameters for InfraSecAdpt_DB Named Subsystems

Parameter	Description
Propagate Change (alias DBSecAdpt_ PropagateChange)	Set this parameter to TRUE to allow administration of the current user's password in the database through Siebel Business Applications. If this parameter is set to TRUE (the default setting): ■ Users can change their passwords from within a Siebel application on the User Profile screen (navigate to Tools, User Preferences, and then User Profile) and the change is propagated to the database. ■ An administrator can change the password associated with his or her own login ID using the Administration - User screen in the Siebel Web Client, and the change is propagated to the database. The administrator cannot change other users' passwords from the Administration - User screen.
Security Adapter Dll Name (alias DBSecAdpt_ SecAdptDllName)	Specifies the DLL that implements the security adapter API required for integration with Siebel Business Applications. The file extension need not be explicitly specified. For example, sscfsadb.dll implements the Siebel database security adapter in a Windows implementation, and libsscfsadb.so does so in a UNIX implementation. If the DLL name for the adapter is used in a UNIX implementation, then it is converted internally to the actual filename DLL.

The parameters in Table 36 are also for database authentication environments, and are defined for named subsystems of type InfraDataSource, that is, they may be set for the ServerDataSrc named subsystem, or another data source. The named subsystem is specified as the value for the DataSourceName parameter for the database security adapter.

Table 36. Database Authentication Parameters for InfraDataSource Named Subsystems

Parameter	Description
Hash User Password (alias DSHashUserPwd)	Specifies password hashing for user passwords. Uses the hashing algorithm specified using the DSHashAlgorithm parameter. For details, see "About Password Hashing" on page 158.
User Password Hash Algorithm (alias DSHashAlgorithm)	Specifies the password hashing algorithm to use, if DSHashUserPwd is TRUE. The default value, RSASHA1, provides hashing using the RSA SHA-1 algorithm. The value SIEBELHASH specifies the password hashing mechanism provided by the mangle algorithm from Siebel Business Applications (supported for existing customers only). For details, see "About Password Hashing" on page 158.

Parameters for LDAP or ADSI Authentication

This topic outlines the Gateway Name Server parameters related to LDAP or ADSI authentication. The LDAP or ADSI authentication parameters, described in Table 37, are defined for named subsystems of type InfraSecAdpt_LDAP; they can be set for the named subsystems LDAPSecAdpt or ADSISecAdpt, or a similar security adapter with a nondefault name.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description
Application Password (alias ApplicationPassword)	Specifies the password in the directory for the user defined by the ApplicationUser parameter. ■ In an LDAP directory, the password is stored in an attribute. ■ In ADSI, the password is stored using ADSI user management tools; it is not stored in an attribute.
Application User (alias ApplicationUser)	Specifies the user name of a record in the directory with sufficient permissions to read any user's information and do any necessary administration. This user provides the initial binding of the LDAP directory or Active Directory 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=*example.com*" (including quotes) for LDAP. The security adapter uses this name to bind. **NOTE:** You must implement an application user.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description

Base DN (alias BaseDN)	Specifies the Base Distinguished Name, which is the root of the tree under which users of this Siebel application are stored in the directory. Users can be added directly or indirectly below this directory.
	
	A typical entry for an LDAP server might be:
	
	`BaseDN = "ou=people, o=domain_name"`
	
	where:
	
	■ o denotes organization and is typically your Web site's domain name
	
	■ ou denotes organization unit and is the subdirectory in which users are stored
	
	A typical entry for an ADSI server might be:
	
	`BaseDN = "ou=people, DC=qatest, DC=siebel, DC=com"`
	
	Domain Component (DC) entries are the nested domains that locate this server. Therefore, adjust the number of DC entries to represent your architecture.

CRC (alias CRC)	Use this parameter to implement checksum validation in order to verify that each user gains access to the database through the correct security adapter. This parameter contains the value calculated by the checksum utility for the applicable security adapter DLL. If you leave this value empty, then the system does not perform the check. If you upgrade your version of Siebel Business Applications, then you must recalculate and replace the value in this parameter. For more information, see "Configuring Checksum Validation" on page 149.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description
Credentials Attribute Type (alias CredentialsAttributeType)	Specifies the attribute type that stores a database account. For example, if CredentialsAttributeType is set to dbaccount, then when a user with user name HKIM is authenticated, the security adapter retrieves the database account from the dbaccount attribute for HKIM. This attribute value must be of the form `username=U password=P`, where `U` and `P` are credentials for a database account. There can be any amount of white space between the two key-value pairs and no space within each pair. The keywords `username` and `password` must be lowercase. If you implement LDAP or ADSI security adapter authentication to manage the users in the directory through the Siebel client, then the value of the database account attribute for a new user is inherited from the user who creates the new user. The inheritance is independent of whether you implement a shared database account, but does not override the use of the shared database account.
Hash DB Cred (alias HashDBPwd)	Specifies password hashing for database credentials passwords. For details, see “About Password Hashing” on page 158.
Hash User Password (alias HashUserPwd)	Specifies password hashing for user passwords. Uses the hashing algorithm specified using the HashAlgorithm parameter. For details, see “About Password Hashing” on page 158.
Password Attribute Type (alias PasswordAttributeType)	Specifies the attribute type under which the user’s login password is stored in the directory. The LDAP entry must be userPassword. However, if you use the LDAP security adapter to authenticate against Microsoft Active Directory, then set the value of this parameter to unicodePWD. Active Directory does not store the password in an attribute so this parameter is not used by the ADSI security adapter. You must, however, specify a value for the Password Attribute Type parameter even if you are using the ADSI adapter. Specify a value of unicodePWD.
Password Expire Warn Days (alias PasswordExpireWarnDays) (ADSI only)	Specifies the number of days to display a warning message before a password expires. You can only specify a value for this parameter when the directory server in use is Active Directory. You can specify a value when the security adapter in use is an ADSI or LDAP security adapter.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description
Port (alias Port)	Specifies the port on the server computer that is used to access the LDAP server. Typically, use 389, the default value, for standard transmission or use 636 for secure transmission. This parameter is used by the LDAP security adapter only. For ADSI, you set the port at the directory level, so this parameter is not used. You must, however, specify a value for the Port parameter even if you are using the ADSI adapter; specify either port 389 or 636.
Propagate Change (alias PropagateChange)	Set this parameter to TRUE to allow administration of the directory through Siebel Business Applications. When an administrator then adds a user or changes a password from within a Siebel application, or a user changes a password or self-registers, the change is propagated to the directory. A non-Siebel security adapter must support the SetUserInfo and ChangePassword methods to allow dynamic directory administration.
Roles Attribute Type (alias RolesAttributeType)	Specifies the attribute type for roles stored in the directory. For example, if RolesAttributeType is set to roles, then when a user with user name HKIM is authenticated, the security adapter retrieves the user's Siebel responsibilities from the roles attribute for HKIM. Responsibilities are typically associated with users in the Siebel database, but they can be stored in the database, in the directory, or in both. The user gets access to all of the views in all of the responsibilities specified in both sources. However, it is recommended that you define responsibilities in the database or in the directory, but not in both places. For details, see "Configuring Roles Defined in the Directory" on page 157.
Salt User Passwords (alias SaltUserPwd)	Set this parameter to TRUE to specify that salt values are to be added to user passwords before they are hashed. This parameter is ignored if the HashUserPwd parameter is set to FALSE. Adding salt values to user passwords is not supported if you are using Web Single Sign-On. For further information on salt values, see "About Password Hashing" on page 158.
Salt Attribute (alias SaltAttributeType)	Specifies the attribute that stores the salt value if you have chosen to add salt values to user passwords. The default attribute is title.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description
Security Adapter Dll Name (alias SecAdptDllName)	Specifies the DLL that implements the security adapter API required for integration with Siebel Business Applications. The file extension need not be explicitly specified. For example, enter sscforacleldap to implement the LDAP security adapter in a Windows implementation. For the ADSI security adapter, enter sscfadsi. On supported UNIX operating systems, the file name can be libsscforacleldap.so or libsscforacleldap.sl. If the DLL name for the LDAP security adapter is used in a UNIX implementation, then it is converted internally to the actual filename.
Server Name (alias ServerName)	Specifies the name of the computer on which the LDAP or Active Directory server runs. ■ You must specify the fully qualified domain name of the LDAP server, not just the domain name. For example, specify ldapserver.example.com, not example.com. ■ If TLS is configured between the Siebel Server computer and the Active Directory server computer, you must specify the fully qualified domain name of the Active Directory server. If the Siebel Server and Active Directory server are in the same domain, then specify the complete computer name of the Active Directory server. Do not specify the IP address of the Active Directory server for the ServerName parameter.
Shared Credentials DN (alias SharedCredentialsDN)	Specifies the absolute path (not relative to the BaseDN) of an object in the directory that has the shared database account for the application. If it is empty, then the database account is looked up in the user's DN as usual. If it is not empty, then the database account for all users is looked up in the shared credentials DN instead. The attribute type is still determined by the value of CredentialsAttributeType. For example, if SharedCredentialsDN is set to: `"uid=HKIM, ou=people, o=example.com"` when a user is authenticated, the security adapter retrieves the database account from the appropriate attribute in the HKIM record. This parameter's default value is an empty string.
Shared DB Password (alias SharedDBPassword)	Specify the password associated with the Shared DB Username parameter.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description
Shared DB Username (alias SharedDBUsername)	Specify the user name to connect to the Siebel database. You must specify a valid Siebel user name and password for the SharedDBUsername and SharedDBPassword parameters. Specify a value for this parameter if you store the shared database account user name as a parameter rather than as an attribute of the directory entry for the shared database account. To use this parameter, you can use either an LDAP directory or Active Directory. For more information, see "Storing Shared Database Account Credentials as Profile Parameters" on page 153.
Siebel Username Attribute Type (alias SiebelUsername AttributeType)	If UseAdapterUsername is set to TRUE, then this parameter is the attribute from which the security adapter retrieves an authenticated user's Siebel user ID. If this parameter is left empty, then the user name passed in is assumed to be the Siebel user ID.
Single Sign On (alias SingleSignOn)	(TRUE or FALSE) If TRUE, then the security adapter is used in Web SSO mode, instead of using security adapter authentication.
SSL Database (alias SslDatabase)	Specifies whether SSL is used for communication between the LDAP security adapter and the directory. If this parameter is empty, then SSL is not used. To use SSL, the value of this parameter must be the absolute path of the wallet, generated by Oracle Wallet Manager, that contains a certificate for the certificate authority that is used by the LDAP server.
Trust Token (alias TrustToken)	Applies only in a Web SSO environment. The adapter compares the TrustToken value provided in the request with the value stored in the application configuration file. If they match, then the Application Object Manager accepts that the request has come from the SWSE, that is, from a trusted Web server. This parameter's default value is an empty string.
Use Adapter Defined Username (alias UseAdapterUsername)	(TRUE or FALSE) If TRUE, then this parameter indicates that when the user key passed to the security adapter is not the Siebel user ID, the security adapter retrieves the Siebel user ID for authenticated users from an attribute defined by the SiebelUsernameAttributeType parameter. The default value for UseAdapterUsername is FALSE.
User Password Hash Algorithm (alias HashAlgorithm)	Specifies the password hashing algorithm to use if HashUserPwd or HashDBPwd is TRUE. The default value, RSASHA1, provides hashing using the RSA SHA-1 algorithm. The value SIEBELHASH specifies the password hashing mechanism provided by the mangle algorithm from Siebel Business Applications (supported for existing customers only). For details, see "About Password Hashing" on page 158.

Table 37. LDAP and ADSI Authentication Parameters

Parameter	Description
Username Attribute Type (alias UsernameAttributeType)	Specifies the attribute type under which the user's login name is stored in the directory. For example, if UsernameAttributeType is set to uid, then when a user attempts to log in with user name HKIM, the security adapter searches for a record in which the uid attribute has the value HKIM. This attribute is the Siebel user ID, unless the UseAdapterUsername parameter is TRUE. If you implement an adapter-defined user name (UseAdapterUsername is set to TRUE), then you must set the OM - Username BC Field parameter appropriately to allow the directory attribute defined by UsernameAttributeType to be updated from the Siebel client. For more information about implementing an adapter-defined user name, see "Configuring Adapter-Defined User Name" on page 154.
WalletPassword	Specifies the password assigned to the Oracle wallet that contains the certificate for the certificate authority that is used by the LDAP server.

Parameters for Custom Security Adapter Authentication

This topic outlines the Gateway Name Server parameters related to custom security adapter authentication. The Gateway Name Server parameters in Table 38 are for custom security adapter authentication only, and are defined for the named subsystem InfraSecAdpt_Custom.

Table 38. Custom Security Adapter Authentication Parameters

Parameter	Description
Config File Name (alias ConfigFileName)	Specifies the file name that contains custom security adapter configuration parameters. These settings would be other than those defined in this section.
Config Section Name (alias ConfigSectionName)	Specifies the name of the section, in the file specified using the ConfigFileName parameter, that contains custom security adapter configuration settings.

The following parameters are for custom security adapter authentication, and are defined for the named subsystem InfraSecAdpt_Custom. For more information about these parameters, see the descriptions for similar parameters applicable to LDAP or ADSI security adapters, in "Parameters for LDAP or ADSI Authentication" on page 364.

- CRC (alias CustomSecAdpt_CRC)
- Hash DB Cred (alias CustomSecAdpt_HashDBPwd)
- Hash User Password (alias CustomSecAdpt_HashUserPwd)

- Propagate Change (alias CustomSecAdpt_PropagateChange)
- Salt User Passwords (alias CustomSecAdpt_SaltUserPwd)
- Security Adapter Dll Name (alias CustomSecAdpt_SecAdptDllName)
- Single Sign On (alias CustomSecAdpt_SingleSignOn)
- Trust Token (alias CustomSecAdpt_TrustToken)
- Use Adapter Defined Username (alias CustomSecAdpt_UseAdapterUsername)
- User Password Hash Algorithm (alias CustomSecAdpt_HashAlgorithm)

Parameters for Application Object Manager

The Gateway Name Server parameters in Table 39 are defined for the Enterprise, Siebel Server, or Application Object Manager component.

Table 39. Enterprise, Siebel Server, or Application Object Manager Component Parameters

Parameter	Description
AllowAnonUsers	(TRUE or FALSE) Unregistered users are not allowed access to the Siebel application if this parameter value is FALSE. If your Siebel application does not use functionality that requires anonymous browsing, then set the AllowAnonUsers parameter to False.
DisableReverseProxy	If you deploy IBM Tivoli Access Manager WebSEAL to authenticate users of Siebel Business Applications with high interactivity in a Web Single Sign-On deployment, then set DisableReverseProxy to TRUE to disable reverse proxy support. You must disable implicit reverse proxy support as IBM Tivoli Access Manager WebSEAL acts as a reverse proxy server. The default value for DisableReverseProxy is FALSE.
SecureLogin	(TRUE or FALSE) If TRUE, the login form completed by the user is transmitted over TLS. 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 TLS. When SecureBrowse is set to FALSE, views in the application whose Secure attribute is set to TRUE are navigated over TLS. **NOTE:** Siebel customer applications support switching between secure and nonsecure views, but employee applications (such as Siebel Call Center) do not. For more information, see "Configuring a Siebel Web Client to Use HTTPS" on page 201.

Table 39. Enterprise, Siebel Server, or Application Object Manager Component Parameters

Parameter	Description
OM - Proxy Employee (alias ProxyEmployee)	User ID of the proxy employee. For information about the proxy employee, see "Seed Data" on page 383.
OM - Username BC Field (alias UsernameBCField)	This parameter is used only if you implement an adapter-defined user name as described in "Configuring Adapter-Defined User Name" on page 154. This parameter 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. The OM - Username BC Field parameter is case sensitive. The value you specify for this parameter must match the value specified for the parameter in Siebel Tools.

Parameters in the Gateway.cfg File

The gateway.cfg file contains the configuration parameters that determine how access to the Gateway Name Server is authenticated. Gateway Name Server authorization is required whether you use the Siebel Configuration Wizard, Siebel Server Manager, or other utilities to access the Gateway Name Server.

NOTE: Authentication is not required for starting the Gateway Name Server, only for connecting to it.

The gateway.cfg file is located in the *SIEBEL_ROOT*\gtwysrvr\bin (Windows) or *SIEBEL_ROOT*/gtwysrvr/bin (UNIX) directory. The following gateway.cfg file parameters relate to authentication. These parameters are present by default or can be added to the configuration file for gateway authentication. They are grouped by the labeled sections in which they occur in the file. This listing does not include parameters in the gateway.cfg file that are not authentication-related.

You can use any plain text editor to add parameters and their values, or to change values for existing parameters. Changes to the gateway.cfg file are not active until you restart the Siebel Gateway Name Server.

Parameters in sections that directly pertain to security adapters apply only to Gateway Name Server authentication. These parameters are counterparts to the Siebel Gateway Name Server security adapter parameters listed in "Siebel Gateway Name Server Parameters" on page 361.

Parameters in the [InfraNameServer] Section

The parameters in Table 40 apply to Gateway Name Server authentication, whether you implement security adapter authentication or Web SSO authentication.

Table 40. InfraNameServer Parameters in Gateway.cfg

Parameter	Description
Enable Audit Trail	This parameter specifies whether or not all Gateway Name Server connections are logged. If this parameter is set to TRUE, then most accesses to the Gateway Name Server, including logins, writes, modifications, and deletions, are logged. If this parameter is set to FALSE, then only failed login attempts are logged. The default value of this parameter is TRUE. The audit trail is located at the *SIEBEL_ROOT*\gtwysrvr/bin\nameserver_audit.log directory (Windows) or the *SIEBEL_ROOT*/gtwysrvr/bin/nameserver_audit.log directory (UNIX).
NSAdminRole	Defines the user role that is required to access the Gateway Name Server. The default role is Siebel Administrator.

Parameters in the [InfraSecMgr] Section

The parameters in Table 41 are located in the [InfraSecMgr] section of the gateway.cfg file.

Table 41. InfraSecMgr Parameters in Gateway.cfg

Parameter	Description
SecAdptMode	Specifies the security adapter mode. ■ To use database authentication, specify DB. This is the default mode. The Gateway Name Server is configured to use database authentication by default. ■ To use LDAP authentication, specify LDAP. ■ To use Active Directory authentication, specify ADSI. ■ To use a custom security adapter, specify CUSTOM.
SecAdptName	Specifies the security adapter name. ■ For database authentication, specify DBSecAdpt. This is the default value for the SecAdptName parameter. ■ For LDAP authentication, specify LDAPSecAdpt or a name of your choice. ■ For Active Directory authentication, specify ADSISecAdpt or a name of your choice. ■ For a custom security adapter, specify a name such as SecAdpt_Custom. You must add the applicable section to the gateway.cfg file yourself. For example, [SecAdpt_Custom].

Parameters in the [DBSecAdpt] Section

The following parameters are located in the [DBSecAdpt] section of the gateway.cfg file and are specified if you are configuring the database security adapter.

- DBSecAdpt_SecAdptDllName
- DataSourceName
- DBSecAdpt_PropagateChange

For information on these parameters, see the descriptions for equivalent parameters in "Parameters for Database Authentication" on page 362.

Parameters in the [DataSources] Section

The following parameters are located in the [DataSources] section of the gateway.cfg file and are used to specify the data sources for the security adapter you implemented and for the server.

- **ServerDataSrc.** The data source used when database authentication is enabled.
- **LDAPSecAdpt.** The data source used when LDAP authentication is enabled.

Parameters in the [LDAPSecAdpt] or [ADSISecAdpt] Section

The following parameters are located in the [LDAPSecAdpt] or [ADSISecAdpt] sections of the gateway.cfg file, according to whether you are configuring the LDAP or ADSI security adapter for Gateway Name Server authentication. The LDAP or ADSI sections are created in the gateway.cfg file if you specify LDAP or ADSI configuration values using the Siebel Configuration Wizard.

- ApplicationPassword
- ApplicationUser
- BaseDN
- CRC
- CredentialsAttributeType
- HashAlgorithm
- HashDBPwd
- HashUserPwd
- PasswordAttributeType (LDAP only)
- PasswordExpireWarnDays (ADSI only)
- Port
- PropagateChange
- RolesAttributeType
- SaltAttributeType
- SaltUserPwd
- SecAdptDllName
- ServerName
- SharedCredentialsDN
- SharedDBPassword
- SharedDBUsername
- SiebelUsernameAttributeType
- SingleSignOn
- SslDatabase
- TrustToken
- UseAdapterUsername
- UsernameAttributeType
- WalletPassword

For information on these parameters, see the descriptions for equivalent parameters in “Parameters for LDAP or ADSI Authentication” on page 364.

Siebel Application Configuration File Parameters

A configuration file exists for each Siebel application for each language. The parameters in the file determine how the user interacts with the 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 as follows:

- **Configuration file on the Siebel Server.** For users connecting with the standard Siebel Web Client, application configuration files are located in the *SIEBSRVR_ROOT*\bin*LANGUAGE* subdirectory. For example, eservice.cfg is provided for Siebel eService, for implementation in U.S. English, in the *SIEBSRVR_ROOT*\bin\ENU directory.

  NOTE: Most of the security-related parameters applicable to Siebel Servers (and, consequently, Siebel Web Clients) are stored in the Siebel Gateway Name Server, not in the application configuration file.

- **Configuration file on the Siebel Mobile Web Client or Developer Web Client.** For users connecting through the Siebel Mobile Web Client or Developer Web Client, the configuration file is located in the *SIEBEL_CLIENT_ROOT*\bin*LANGUAGE* subdirectory on the client. For example, eservice.cfg is provided for Siebel eService, for implementation in U.S. English, in the *SIEBEL_CLIENT_ROOT*\bin\ENU directory.

  - The Siebel Mobile Web Client connects directly to the local database; it bypasses the Siebel Server.
  - The Siebel Developer Web Client connects directly to the server database; it bypasses the Siebel Server.

In a given configuration file, some parameters might not appear by default. Others might appear with a preceding semicolon (;), indicating that the parameter is a comment and is not being interpreted. The semicolon must be deleted to make the parameter active. Changes to an application configuration file are not active until you restart the Siebel Server or Siebel client. For more information about working with configuration files, see *Siebel System Administration Guide*.

CAUTION: The parameter values that reference directory attributes that you provide for the Siebel LDAP and ADSI security adapters are case-sensitive. The values must match the attribute names in the directory.

The parameters in the following topics are authentication-related parameters that are present by default or can be added to each application's configuration file. They are grouped by the labeled sections in which they occur. This listing does not include parameters in an application's configuration file that are not authentication-related.

Parameters in the [InfraUIFramework] Section

The parameters in Table 42 apply to Siebel Mobile Web Clients and Siebel Developer Web Clients. For a description of the equivalent parameters applicable to Siebel Web Clients, see "Siebel Gateway Name Server Parameters" on page 361.

Table 42. InfraUIFramework Parameters in the Application Configuration File

Parameter	Description
DisableReverseProxy	If you deploy IBM Tivoli Access Manager WebSEAL to authenticate users of Siebel Business Applications with high interactivity in a Web Single Sign-On deployment, then set DisableReverseProxy to TRUE to disable reverse proxy support. You must disable implicit reverse proxy support as IBM Tivoli Access Manager WebSEAL acts as a reverse proxy server. The default value for DisableReverseProxy is FALSE.
SecureLogin	(TRUE or FALSE) If TRUE, then the login form completed by the user is transmitted over TLS. 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 TLS. When SecureBrowse is set to FALSE, views in the application whose Secure attribute is set to TRUE are navigated over TLS. Siebel customer applications support switching between secure and nonsecure views, but employee applications (such as Siebel Call Center) do not. For more information, see "Configuring a Siebel Web Client to Use HTTPS" on page 201. For additional information about the Secure attribute for a view, see *Configuring Siebel Business Applications*.

Parameters in [InfraSecMgr] Section

The parameters in Table 43 on page 378 are located in the [InfraSecMgr] section of the application configuration file. These parameters apply to Siebel Mobile Web Clients and Developer Web Clients only. For a description of the equivalent parameters applicable to Siebel Web Clients, see "Siebel Gateway Name Server Parameters" on page 361.

Table 43. InfraSecMgr Parameters in the Application Configuration File

Parameter	Description
SecAdptMode	Specifies the security adapter mode. ■ For database authentication, specify DB. (DB is the default value for SecAdptMode.) ■ For LDAP authentication, specify LDAP. ■ For ADSI authentication, specify ADSI. ■ For a custom security adapter, specify CUSTOM. If you implement a custom, non-Siebel security adapter, then you must configure your adapter to interpret the parameters used by the Siebel adapters if you want to use those parameters.

Table 43. InfraSecMgr Parameters in the Application Configuration File

Parameter	Description
SecAdptName	Specifies the name of the security adapter. ■ For database authentication, specify DBSecAdpt. For Mobile or Developer Web Client configuration, the section [DBSecAdpt] is created in the configuration file. (DBSecAdpt is the default value for SecAdptName.) ■ For LDAP authentication, specify LDAPSecAdpt (or a name of your choice). For Developer Web Client configuration, the section [LDAPSecAdpt] is created by default in the configuration file if you configure LDAP using the Siebel Configuration Wizard. ■ For ADSI authentication, specify ADSISecAdpt (or another name of your choice). For Developer Web Client configuration, the section [ADSISecAdpt] is created by default in the configuration file if you configure ADSI using the Siebel Configuration Wizard. ■ For a custom security adapter, specify a name such as SecAdpt_Custom. You must add the applicable section to the file yourself. For example, [SecAdpt_Custom].
UseRemoteConfig This parameter applies *only* to the Siebel Developer Web Client	Specifies the path to a configuration file that contains only parameters for a security adapter, that is, it contains parameters as they would be formatted if they were included in a section such as [LDAPSecAdpt] in an application's configuration file. You must provide the path in universal naming convention (UNC) format, that is, for example, in a form like `\\server\vol\path\ldap_remote.cfg`. For detailed information about using this parameter, see "Security Adapters and the Siebel Developer Web Client" on page 167.

Parameters in [DBSecAdpt] Section

The parameters in Table 44 are located in the [DBSecAdpt] section (or equivalent) of the application configuration file if you are configuring the database security adapter. Each authentication-related parameter in an application's configuration file is interpreted by the security adapter for database authentication.

These parameters apply to Siebel Mobile Web Clients and Developer Web Clients only. For a description of the equivalent parameters applicable to Siebel Web Clients, see "Siebel Gateway Name Server Parameters" on page 361.

Table 44. DBSecAdpt Parameters in the Application Configuration File

Parameter	Description
DBSecAdpt_CRC	Use this parameter to implement checksum validation, in order to verify that each user gains access to the database through the correct security adapter. This parameter contains the value calculated by the checksum utility for the applicable security adapter DLL. If you leave this value empty, then the check is not performed. If you upgrade your Siebel Business Applications, then you must recalculate and replace the value in this parameter. For more information, see "Configuring Checksum Validation" on page 149.
DBSecAdpt_PropagateChange	Set this parameter to TRUE to allow administration of credentials in the database through Siebel Business Applications. When an administrator then adds a user or changes a password from within a Siebel application or a user changes a password or self-registers, the change is propagated to the database. For Siebel Developer Web Client, the system preference SecThickClientExtAuthent must also be set to TRUE. For details, see "Setting a System Preference for Developer Web Clients" on page 143.
DBSecAdpt_SecAdptDllName	Specifies the DLL that implements the security adapter API required for integration with Siebel Business Applications. The file extension need not be explicitly specified. For example, sscfsadb.dll implements the database security adapter in a Windows implementation.
DataSourceName	Specifies the data source applicable to the specified database security adapter.

Parameters in Data Source Section

The parameters in Table 45 are located in the data source section of the application configuration file, such as [ServerDataSrc] for the Siebel Developer Web Client, or [Local] for the Siebel Mobile Web Client.

Table 45. Data Source Parameters in the Application Configuration File

Parameter	Description
DSHashAlgorithm	Specifies the password hashing algorithm to use if DSHashUserPwd is TRUE. The default value, RSASHA1, provides hashing using the RSA SHA-1 algorithm. The value SIEBELHASH specifies the password hashing mechanism provided by the mangle algorithm from Siebel Business Applications (supported for existing customers only). For details, see "About Password Hashing" on page 158.
DSHashUserPwd	Specifies password hashing for user passwords. Uses the hashing algorithm specified using the DSHashAlgorithm parameter. For details, see "About Password Hashing" on page 158.
IntegratedSecurity	Applicable only to Siebel Developer Web Client, with Oracle or Microsoft SQL Server database. For details, see "Security Adapters and the Siebel Developer Web Client" on page 167. **NOTE:** Integrated Security is only supported for Siebel Developer Web clients that access Oracle and Microsoft SQL Server databases. This functionality is not available for Siebel Web Clients or Siebel Mobile Web clients.

Parameters in [LDAPSecAdpt] or [ADSISecAdpt] Section

The following parameters are located in the [LDAPSecAdpt] or [ADSISecAdpt] section (or equivalent) of the application configuration file, according to whether you are configuring the LDAP security adapter or the ADSI security adapter. Each authentication-related parameter in an application's configuration file is interpreted by the security adapter (for LDAP or ADSI authentication).

Some parameters apply only to LDAP implementations, or only to ADSI implementations. Some parameters apply only in a Web SSO authentication environment. For more information, see the descriptions for equivalent parameters applicable to Siebel Web Client and other authentication contexts in "Siebel Gateway Name Server Parameters" on page 361.

- ApplicationPassword
- ApplicationUser
- BaseDN
- CRC
- CredentialsAttributeType
- HashAlgorithm
- HashDBPwd
- PropagateChange
- RolesAttributeType
- SecAdptDllName
- ServerName
- SharedCredentialsDN
- SiebelUsernameAttributeType
- SingleSignOn

- HashUserPwd
- PasswordAttributeType
- PasswordExpireWarnDays
- Port
- SslDatabase
- TrustToken
- UseAdapterUsername
- UsernameAttributeType
- WalletPassword

The parameter, EncryptApplicationPassword, can be set in the [LDAPSecAdpt] or [ADSISecAdpt] sections of an application configuration file only; it is not a Siebel Gateway Name Server parameter. Set EncryptApplicationPassword to TRUE if you want to store the encrypted value of the ApplicationPassword parameter in the application configuration file. Use the encryptstring utility to generate the encrypted value of the ApplicationPassword parameter. For information on using the encryptstring utility, see "Encrypting Passwords Using the encryptstring Utility" on page 47.

B Seed Data

This appendix describes seed data provided for your Siebel Business Applications that is relevant to the content of this guide. It also provides information about how to use this data. It includes the following topics:

- Seed Employee on page 383
- Seed Users on page 384
- Seed Responsibilities on page 384
- Seed Position and Organization on page 386

In the tables in this appendix, the term *customer applications* represents the group of Siebel Sales, Siebel eService, Siebel Customer, Siebel Events, and Siebel Marketing applications. For information on the seed data provided with Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 397.

Seed Employee

One Employee record is provided as seed data at installation, as described in Table 46 on page 383. This record does not have a database login or a responsibility, but, like other employees, it does have a position and an organization. The PROXYE user record is not installed with a default password.

Customer users, such as Siebel eService users, are not assigned their own position or organization. When a customer user logs in, the application programmatically associates the proxy employee with the user. The proxy employee provides the following functions:

- Data subsequently created by the user is associated with the organization of the proxy employee, which allows the data to display in views that implement organization access control.
- The user can see data created by the user and by others in views that implement organization access control.

The proxy employee is specified at the application level as a Siebel Gateway Name Server parameter. For information about associating the proxy employee with an application, see "Siebel Gateway Name Server Parameters" on page 361. For information about organization access control, see "Access Control Mechanisms" on page 266.

Table 46. Proxy Employee Seed Data Field Values

Last Name	First Name	User ID	Responsibility	Position	Organization
Employee	Proxy	PROXYE	None	Proxy Employee	Default Organization

Seed Users

Table 47 on page 384 describes nonemployee user records provided as seed data. Default passwords are not provided for these records. If you use a seed user record as the anonymous user record, then you must set the AnonUserName parameter to the seed user ID (for example GUESTCST) when configuring the SWSE, or set it manually in the eapps.cfg file. For information on configuring the SWSE, see *Siebel Installation Guide* for the operating system you are using. For information on manually setting passwords for the anonymous user, see "Encrypted Passwords in the eapps.cfg File" on page 46.

Table 47. User Seed Data Field Values

Last Name	First Name	User ID	Responsibility	New Responsibility	Used by These Applications
Customer	Guest	GUESTCST	Web Anonymous User	Web Registered User	Customer applications
Channel Partner	Guest	GUESTCP	Unregistered Partner Agent	Self-registered Partner Agent	Siebel Partner Portal

Seed Responsibilities

Responsibility records are provided as seed data, as described in Table 48 on page 384. Responsibilities provided for the seed data User records allow users to see views intended for anonymous browsing, including views from which users can self-register or log in. Other responsibilities are assigned programmatically to self-registering users or are assigned to users manually by internal administrators or delegated administrators.

NOTE: For all responsibilities provided in seed data, refer to those listed in the Siebel application.

Table 48. 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	Siebel eSales

Table 48. Responsibilities Seed Data

Name	Organization	Description	Used by These Applications
Web Purchasing Manager	Default Organization	Views for eSales purchasing manager	Siebel eSales
Unregistered Partner Agent	Default Organization	Views provided for anonymous browsing	Siebel Partner Portal
Self-Registered Partner Agent	Default Organization	Limited set of views provided for a user who self-registers	Siebel Partner Portal
Partner Relationship Manager	Default Organization	Views for Siebel Partner Portal partner relationship manager	Siebel Partner Portal
Partner Operations Manager	Default Organization	Views for Siebel Partner Portal partner operations manager, including views for administering users	Siebel Partner Portal
Partner Sales Manager	Default Organization	Views for Siebel Partner Portal partner sales manager	Siebel Partner Portal
Partner Sales Rep	Default Organization	Views for Siebel Partner Portal partner sales rep	Siebel Partner Portal
Partner Service Manager	Default Organization	Views for Siebel Partner Portal partner service manager	Siebel Partner Portal
Partner Service Rep	Default Organization	Views for Siebel Partner Portal partner service rep	Siebel Partner Portal
Registered Customer - Wireless	Default Organization	Views provided for a registered eService user on a wireless device	Siebel eService
Web Training Manager	Default Organization	Views that allow an administrator to see his or her direct reports' course and curriculum enrollment information	Siebel Training
Training Administrator	Default Organization	Views that allow administration of courses and enrollees	Siebel Training

Listing the Views Associated with a Responsibility

The following procedure describes how to list the views associated with a specific responsibility.

To list the views associated with a responsibility

1 Navigate to the Administration - Application screen, then the Responsibilities view.

2 In the Responsibilities list, select a responsibility.

The views for the responsibility appear in the Views list.

Seed Position and Organization

The Proxy Employee Position and the Default Organization Division records are provided as seed data. The position exists within the division, and the division is its own organization. The position and division are both assigned to the seed data Employee record.

C Addendum for Siebel Financial Services

This appendix outlines the differences in the implementation of user authentication, user administration, and basic access control in Siebel Financial Services applications and the implementation that is documented in other topics of this guide. It includes the following topics:

- Siebel Financial Services Applications on page 387
- User Authentication for Siebel Financial Services on page 389
- User Registration and Administration for Siebel Financial Services on page 391
- Basic Access Control for Siebel Financial Services on page 394
- Configuration File Names for Siebel Financial Services Applications on page 396
- Seed Data for Siebel Financial Services on page 397

Siebel Financial Services Applications

The applications listed in Table 49 on page 388 are specific to Siebel Financial Services or are applications that have functionality that is adapted for Siebel Financial Services. The applications are listed as they are named in Siebel Tools.

For some applications, options are listed that, along with functionality modules, determine the screens and views that are licensed to you. A given application can be referred to by one or more product names, as listed in the Products column. Information is categorized for employee, partner, and customer applications.

Table 49. Siebel Financial Services Applications

Tools Application Object Name	Users	Options	Products
Siebel Financial Services	Employees	Siebel Sales Siebel eService Siebel Call Center Siebel Partner Manager	Siebel Finance Siebel Insurance Siebel Healthcare
Siebel Financial Services ERM	Employees	Not applicable	Siebel Employee Relationship Management
Siebel Financial Services Marketing	Employees	Siebel Marketing only	Siebel Finance Siebel Insurance Siebel Healthcare
Siebel Financial Partner Relationship Management (PRM)	Partners	Not applicable	Siebel Partner Relationship Manager for Finance Siebel Agent Portal Siebel Healthcare Group Portal Siebel Healthcare Provider Portal
Siebel eBanking	Customers	Not applicable	Siebel eBanking
Siebel Financial eBrokerage	Customers	Not applicable	Siebel eBrokerage
Siebel Financial eService	Customers	Not applicable	Siebel Insurance/ Healthcare eService Siebel Healthcare Member Portal
Siebel Financial eEnrollment	Customers	Not applicable	Siebel Healthcare Enrollment Portal
Siebel FINS eSales	Customers	Not applicable	Siebel Sales

Table 49. Siebel Financial Services Applications

Tools Application Object Name	Users	Options	Products
Siebel Financial eCustomer	Customers	Not applicable	Siebel Customer
Siebel eEvents Management	Customers	Not applicable	Siebel Events Manager for Finance

NOTE: Siebel Healthcare Group Portal is used as a customer product; that is, users are typically your customers. Technically, Siebel Healthcare Group Portal is a product label for the Siebel Financial partner application. You provide users with their own positions and organizations, unlike users of customer applications.

User Authentication for Siebel Financial Services

This topic contains information for Siebel Financial Services applications that differs from information in other topics of this guide, or that otherwise warrants mention.

LDAP and ADSI Security Adapter Authentication

Security adapter authentication is a prerequisite if you want to implement self-registration or external administration of users. However, not all Siebel Business Applications provide self-registration and external administration of users as default functionalities. For information about the applications in this group that provide self-registration and external administration of users as default functionalities, see "User Registration and Administration for Siebel Financial Services" on page 391.

About Implementing LDAP and ADSI Security Adapter Authentication

Implementation of LDAP or ADSI security adapter authentication is the same for Siebel Financial Services applications as described in other topics in this guide, with the following exceptions. Parameters for Siebel Financial Services applications are listed primarily in the eapps_sia.cfg file. The eapps.cfg file is also included, as documented in other topics in this guide. The eapps.cfg file has an include line that points to the eapps_sia.cfg file. References throughout this topic to the eapps.cfg file refer to the eapps.cfg file *and* the eapps_sia.cfg file.

About Setting Up Security Adapter Authentication

The Responsibility and New Responsibility that are assigned to the seed anonymous user GUESTCST are intended for use with Siebel Financial Services customer applications. These responsibilities differ from the responsibilities assigned to GUESTCST for Siebel customer applications that are not specific to financial services, as documented in other sections of this guide.

If you deploy either Siebel Events Manager for Finance or Siebel customer applications that are not specific to financial services concurrently with any other Siebel Financial Services customer applications, then you must create a separate anonymous user.

The new anonymous user is used for Siebel Events Manager for Finance and for the Siebel customer applications that are not specific to financial services; that is, the applications documented in other sections of this guide. Assign responsibilities to this anonymous user as they are documented for GUESTCST in "Seed Data" on page 383.

When you add TESTUSER to the database, specify values for the Responsibility and New Responsibility fields that are appropriate 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 397 and "Seed Data" on page 383.

About Implementing Web SSO Authentication

Implementation of Web SSO authentication is the same for Siebel Financial Services applications as described in other topics in this guide with the following exceptions.

Parameters for Siebel Financial Services applications are listed primarily in the eapps_sia.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_sia.cfg file. References throughout this topic to the eapps.cfg file apply to the eapps.cfg file and the eapps_sia.cfg file.

About Setting Up Web SSO

The Responsibility and New Responsibility that are assigned to the seed anonymous user GUESTCST are intended for use with Siebel Financial Services customer applications. These responsibilities differ from the responsibilities assigned to GUESTCST for Siebel customer applications that are not specific to financial services, as documented in other sections of this guide.

If you deploy either Siebel Events Manager for Finance or Siebel customer applications that are not specific to financial services concurrently with any other Siebel Financial Services customer applications, then you must create a separate anonymous user.

The new anonymous user is used for Siebel Events Manager for Finance and for the Siebel customer applications that are not specific to financial services; that is, the applications documented in other sections of this guide. Assign responsibilities to this anonymous user as they are documented for GUESTCST in "Seed Data" on page 383.

When you add TESTUSER to the database, specify values for the Responsibility and New Responsibility fields that are appropriate 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 397 and "Seed Data" on page 383.

Parameters in the eapps.cfg and eapps_sia.cfg Files

In addition to the eapps.cfg file, the Siebel Web Engine also uses the eapps_sia.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_sia.cfg file.

Table 50 on page 391 lists the sections in the eapps.cfg and eapps_sia.cfg files that are provided for Siebel Financial Services applications.

Table 50. Sections in eapps.cfg and eapps_sia.cfg Files

Tools Application Object Name	Section in eapps.cfg	Section in eapps_sia.cfg
Siebel Financial Services	None	[/fins]
Siebel Financial Services ERM	None	[/finserm]
Siebel Marketing	[/marketing]	Not applicable
Siebel Financial PRM	None	[/finsechannel]
Siebel eBanking	None	[/finsebanking]
Siebel Financial eBrokerage	None	[/finsebrokerage]
Siebel Financial eService	None	[/finseservice]
Siebel Financial eEnrollment	None	[/finseenrollment]
Siebel FINS eSales	None	[/finsesales]
Siebel Financial eCustomer	None	[/finsecustomer]
Siebel eEvents for Finance	[/eevents]	None

Siebel Application Configuration File Parameters

For names of application configuration files for specific applications, see "Configuration File Names for Siebel Financial Services Applications" on page 396.

User Registration and Administration for Siebel Financial Services

This topic contains information for Siebel Financial Services applications that differs from the information in the topic on registering and administering users in other sections of this guide, or that otherwise warrants mention.

Seed Data

The Responsibility and New Responsibility that are assigned to the seed user GUESTCST are intended for use with Siebel Financial Services customer applications. These responsibilities differ from the responsibilities assigned to GUESTCST for Siebel customer applications that are not specific to financial services, as documented in other sections of this guide.

If you deploy either Siebel Events Manager for Finance or Siebel customer applications that are not specific to financial services concurrently with any other Siebel Financial Services customer applications, then you must create a separate anonymous user. The new anonymous user is used for Siebel Events Manager for Finance and for the Siebel customer applications that are not specific to financial services; that is, the applications documented in other sections of this guide. Assign responsibilities to this anonymous user as they are documented for GUESTCST in "Seed Data" on page 383. For information about seed data specific to Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 397.

Unregistered Users and Anonymous Browsing

Anonymous browsing is default functionality for the following Siebel Financial Services applications:

- Siebel Employee Relationship Management
- Siebel Events Manager for Finance
- Siebel Finance PRM
- Siebel eBanking
- Siebel eBrokerage
- Siebel Finance eSales
- Siebel Healthcare Enrollment Portal

In addition to the GUESTCST and GUESTCP seed user records provided as anonymous users, a seed user record with user ID GUESTERM is provided as the anonymous user for Siebel Financial Services ERM. For information about seed data specific to Siebel Financial Services applications, see "Seed Data for Siebel Financial Services" on page 397.

Self-Registration

User self-registration is default functionality for the following Siebel Financial Services applications.

NOTE: Although self-registration is provided as default functionality for some Siebel Financial Services applications, it is not common in the industry for users to self-register for financial services. More commonly, internal administrators register users by using the Siebel Financial Services application.

- Siebel Finance PRM
- Siebel Events Manager for Finance
- Siebel eBanking
- Siebel eBrokerage
- Siebel Finance eSales

A user can self-register in Siebel Finance PRM as a company or as an individual. By self-registering, the user requests to become a partner and becomes a prospective partner. An internal administrator uses the Administration - Partner screen in Siebel Finance to promote a prospective partner to approved partner and then to registered partner. For information about using the Administration - Partner screen, see *Siebel Partner Relationship Management Administration Guide*.

Internal Administration of Users

Internal administration of users is the same for Siebel Financial Services applications as described in other topics in this guide, except that you can administer partner users in the Administration - Partner screen in Siebel Financial Services. For information about using the Administration - Partner screen, see *Siebel Partner Relationship Management Administration Guide*.

External Administration of Users

Delegated administration is default functionality of Siebel Financial PRM.

NOTE: Although delegated administration is provided as default functionality of Siebel Financial PRM, it is not common in the finance industry for external administrators to register customer or partner users. More commonly, internal administrators register users by using the Siebel Financial Services application.

Access Considerations

Seed responsibilities that provide user administration views for delegated administrators are described in "Seed Data" on page 383. The seed responsibilities for delegated administrators do not include views specific to Siebel Financial Services applications. For a delegated administrator to access appropriate financial services views and user administration views, the delegated administrator must be assigned responsibilities in one of the following ways:

- Assign at least two seed responsibilities to the delegated administrator; one for a regular user of the Siebel application, and the appropriate responsibility for delegated administrators of the application.
- Create a single responsibility that includes all the views you want delegated administrators to have, then assign the responsibility to the delegated administrators.

For information about assigning responsibilities to users, see the topics on internal administration of users and external administration of users in other topics in this guide.

Maintaining a User Profile

Maintaining a user profile is the same for Siebel Financial Services applications as described in other topics in the guide, with the exception of editing personal information. Depending on the Siebel customer application, the user can click My Profile or My Accounts to access the User Profile form.

Basic Access Control for Siebel Financial Services

Basic access control for Siebel Financial Services applications is implemented as described in other topics in this guide, with the following exceptions:

- "Access Control Mechanisms" on page 394
- "Administration of Access-Group Access Control" on page 394

Access Control Mechanisms

The information in this topic applies to access control for opportunities in any view that uses personal, position, or organization access control.

If an opportunity's Secure field is checked, then only positions on the sales team have visibility of the opportunity in any view that applies person, position, or organization access control. For example, in the All Opportunities view, users on the sales team can see a secure opportunity, but other users in the same organization cannot. In the My Team's Opportunities view, a manager cannot see a secure opportunity on which a direct report is a primary unless the manager is also on the sales team. Any activities or events related to a secure opportunity are also hidden from any user who is not on the sales team.

Secure opportunity access control is provided by the following search specification on the Opportunity business component:

```
[Secure Flag] = 'N' OR EXISTS([Sales Rep Id] = LoginId())
```

Access-Group Access Control

Households can also be used in combination with other party types to form an access group. In all access control contexts, include households in lists of the party types that can be members of access groups.

Administration of Access-Group Access Control

This topic provides procedures for associating an access group with a catalog or category when you are using Siebel Financial Services applications.

Associating an Access Group with a Catalog

By associating an access group with a catalog of master data, you grant access to the data in the catalog to individual users in the access group.

NOTE: For a catalog and all of its' categories to be visible only to the access groups associated with it, the catalog's Private flag must be set.

To associate an access group with a catalog

1. Navigate to the Administration - Catalog screen, then the Catalogs view.

   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. Navigate to the Administration - Catalog screen, then the Catalogs view.

   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

The names of the application configuration files that are used by Siebel Financial Services applications differ to the application configuration file names used for other Siebel Business Applications. Table 51 on page 396 contains the names of application configuration files that are used by Siebel Financial Services applications.

Table 51. Siebel Financial Services Application Configuration File Names

Tools Application Object Name	Configuration File Name
Siebel Financial Services	fins.cfg
Siebel Financial Services ERM	finserm.cfg
Siebel Financial Services Marketing	finsmarket.cfg
Siebel Financial PRM	finscw.cfg
Siebel eBanking	finsebanking.cfg
Siebel Financial eBrokerage	finsebrokerage.cfg
Siebel Financial eService	finseservice.cfg
Siebel Financial eEnrollment	finseenrollment.cfg
Siebel FINS eSales	finsesales.cfg

Table 51. Siebel Financial Services Application Configuration File Names

Tools Application Object Name	Configuration File Name
Siebel Financial eCustomer	finsecustomer.cfg
Siebel eEvents Management	eevents.cfg

Seed Data for Siebel Financial Services

This topic contains information for Siebel Financial Services applications that differs from the information in Appendix B, "Seed Data" or that otherwise warrants mention. In this topic, the term *Siebel Financial Services customer applications* represents the group denoted as customer applications in Table 49 on page 388.

The differences in the seed data provided with Siebel Financial Services applications are described in the following topics:

- "Seed Users" on page 397
- "Seed Responsibilities" on page 398

Seed Users

Table 52 on page 397 shows modifications to the seed nonemployee User records that are provided with Siebel Financial Services applications.

The GUESTCP seed User record, which is documented in Appendix B, "Seed Data", functions as the anonymous user for Siebel Financial PRM, the partner application in Siebel Financial Services. The responsibility of the GUESTCP seed User record provides views for anonymous browsing, and the responsibility in its New Responsibility field provides views for users who self-register.

Table 52. 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 53 on page 398 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 Oracle's Siebel Financial PRM. You must build responsibilities for registered partner users based on their various business roles. You can create new responsibilities, or you can copy and modify seed responsibilities for partner users. For information about creating and modifying responsibilities, see Chapter 9, "Configuring Access Control."

Table 53. Seed Responsibilities

Name	Organization	Description and Comments	Used by These Applications
Unregistered Customer	Default Organization	Views provided for anonymous browsing.	Siebel Financial Services customer applications, except Siebel Events Manager for Finance. For Siebel Events Manager for Finance, use Web Anonymous User instead.
Registered Customer		Views for a typical registered user. Associate Default Organization with this responsibility before assigning this responsibility to a user.	Siebel Financial Services customer applications, except Siebel Events Manager for Finance. For Siebel Events Manager for Finance, use Web Registered User instead.
ERM AnonUser	Default Organization	Views provided for anonymous browsing.	Siebel Financial Services ERM.
ERM User	Default Organization	Views for a typical registered user.	Siebel Financial Services ERM.
ERM Manager	Default Organization	Views for employee management. Assign this responsibility to managers in addition to a responsibility that contains views for a regular user.	Oracle's Siebel Financial Services ERM.

Index

Numerics

56-bit encryption, upgrading 86

A

access control
- access-group, about 275
- accessible data, suborganization view 300
- All access control 274
- business environment structure, about and elements (table) 276
- business services, configuring 321, 327
- Catalog access control view 301
- catalogs, overview 265
- customer data 264
- defined 258
- divisions, setting up 278
- drilldown visibility, configuring 330
- license key, role of 287
- manager access control 269, 300
- master data 264
- opportunities in Siebel Financial Services 394
- organization 271, 300
- organizations, setting up 279
- party data model, S_PARTY table 332
- party types, about and table 260
- party types, relationship among 333
- personal 300
- personal access control 266
- pick applets, configuring visibility 328
- Pick List Object, setting visibility 329
- position 267
- positions, setting up 280
- record level 26
- responsibilities, configuring access to business services 321, 327
- responsibilities, defining and adding views and users 282
- responsibilities, role of 157
- single-position access control, about 268
- single-position access control, Manager view 300
- special frame class, using 329
- strategies, list of 276
- suborganization access control 273
- tab layouts, managing through responsibilities 315
- team 300
- team access control, about 268
- troubleshooting issues 350
- view level 25
- view properties, displaying 299
- view-level mechanisms 259
- visibility applet type 299
- Visibility Auto All property, using 329

access control, business component view
- manager setting 270
- role of 286
- single or multiple organization 273
- single-position view mode 268
- suborganization setting 274
- team setting 269

access control, implementing
- applet access control properties 297
- application, role of 286
- application-level access control 286
- business component view modes 291
- Owner party type 292
- responsibilities, about 286
- responsibilities, associating with users 287
- view access control properties 299
- view construction example 302
- visibility applet, role of 286
- visibility properties, role of 286

Access Group base and extension tables, illustration 344

Access group data model, about and diagram 344

access groups
- catalog access control 275
- categories, associating with 314
- categories, disassociating with 314
- creating 311
- data, associating with 312
- disassociating from catalog 313
- hierarchy, modifying 312
- master data catalog, associating with 313
- members, adding 311

access-group access control
- about 275
- administrative tasks, listed 308
- basic principles 304
- business scenario 304
- catalog, associating an access group with in

Financial applications 395
households, administering in Financial applications 394
inheritance rules 304
user's experience 307
Account base and extension tables, illustration 338
Account data model 338
account policies, about implementing 205
adapter-defined user name
deployment option 146
implementing 154
Admin mode, visibility 274, 301
Administration - Server Configuration screen, unable to work in 346
administrative tasks, deactivating employees 244
administrative tasks, organizational
company structure, setting up 277
divisions, setting up 283
organizations, setting up 283
administrative tasks, positions and responsibilities
positions, setting up 284
responsibilities, defining 285
ADSI adapter
Active Directory server, setting up 181
ADSI client requirement 114
ApplicationPassword parameter 364
comparison with LDAP adapter 107
configuring as directory 182
delegated administrator, availability of 249
deployment options 146
deployment options, listed 146
directory, user management recommendation 112
password storage and use 113
passwords 113
security adapter authentication, implementing 128
security adapter process overview 101
Siebel Financial Services, about 389
Siebel Financial Services, implementing 389
ADSI adapter, setup scenario
about implementing 129
configuration file parameter values, table of 136
configuration file parameter, usage guidelines 142
directory records, about 133
installation prerequisites 130
restarting servers 143, 190
testing 144
user records, adding 134
users, creating 133
ADSI security adapter and DNS servers 112
ADSI server, password assignment 182
ADSI standards, security adapter authentication 106
All access control
about 274, 299
mobile user restriction 289
AllowAnonUsers parameter
about 371
setting for LDAP or ADSI 138, 142
setting for Web SSO 188, 190
AnonPassword parameter
about 355
setting for LDAP or ADSI 136
setting for Web SSO 187
AnonUserName parameter
anonymous browsing, setting for 217
setting for LDAP or ADSI 136
setting for Web SSO 187
anonymous browsing
about 214
anonymous user, role of 215
configuration parameters, setting 216
implementing 156, 215
Siebel Financial Services, registering and administering 392
views, setting or removing explicit login 217
anonymous user
about 133, 214
anonymous user record, modifying 215
automatically populated fields 221
implementing 155
parameter controlling 371
seed data responsibilities, about using 216
seed data user IDs 221
self-registration, modifying for 220
Web SSO authentication 185
applets
access control 299
defined 297
display name and visibility 298
pick applet visibility 328
special frame class for visibility 329
viewing properties 297
visibility properties, about 297
application
access control, implications of 286
license key and view visibility 286
Application Object Manager, ADSI adapter requirements 114
application user
about 133
Web SSO authentication 185

write privileges 241, 249
application-level access control, about and view visibility 286
ApplicationPassword parameter
about 364
setting for LDAP or ADSI 141
ApplicationUser parameter
about 364
setting for LDAP or ADSI 141
APPUSER 133
APPUSERPW 133
architecture, Siebel Security
data confidentiality, end-to-end encryption 23
data continuity, auditing for 26
data visibility, authorization to control 25
intrusion, preventing by secure physical deployment 27
mobile solutions, security for 28
secure system access, user authentication for 20
attributes, password storage 113
auditing 26
authentication
architecture differences between Standard and Developer Web Clients 167
database authentication 102
database authentication, implementing 103
methods, comparison table 99
methods, overview 97
Authentication Method parameter 171
authentication options
adapter-defined user name, implementing 154
anonymous browsing, implementing 156
anonymous user, implementing 155
checksum validation 149
credentials password hashing 158
digital certificate authentication 191
password hashing 158
remote configuration 169
roles 157
secure login 203
Secure Sockets Layer, implementing 150
shared database account, implementing 151
user specification source, implementing 192
views, securing 201
auto-login cookie 204, 207

B

BaseDN parameter
about 365
setting for LDAP or ADSI 140
business component view mode
about data access 291
manager setting 270
mode and visibility fields, viewing 292
role in access control 286
single or multiple organization setting 273
single-position setting 268
suborganization setting 274
team setting 269
business components
All access control 274
control properties, displaying 299
overriding visibility 329
self-registration 221
self-registration views 225
view construction example 302
visibility applet, about 299
visibility applet, role in access control 286
visibility properties, role in access control 286
business environment structure
about and elements (table) 276
multiple organizations, benefits of 277
multiple organizations, reasons for 278
business services
configuring access control 321, 327
creating custom 225

C

CACertFileName parameter 69
Cascade button 304
Catalog access control view 301
catalogs
about 265
about accessing 265
access control strategy 276
access control, types of 275
access groups, associating with data 312
access-group access control principles 304
administrative tasks, listed 308
associating access group and data 313
categories, role of 265
controlling access to categories 304
disassociating access groups 313
granting access to 275
navigating 307
properties of 265
role in master data 265
user experience, about 307
categories
access groups, associating with 314
access groups, associating with data 312
access groups, disassociating with 314

administration tasks, listed 308
company structure, described 277
controlling access to 304
inheritance rules 304
relation to catalog 265
categorized data
about user experience 307
viewing in Info Center 307
CERT_SUBJECT variable 358
CertFileName parameter 69, 360
Change Position button 255, 281
checksum utility
about 149
validation, setting up 149
ClientCertificate parameter, about 355
column, encrypted 77
company structure
categories, described 277
setting up 277
configuration file
activating changes in application configuration file 376
AllowAnonUsers parameter 371
ApplicationUser parameter 364
authentication parameters 376
authentication-related parameters 355
BaseDN parameter 365
comments, designating 376
CredentialsAttributeType parameter 366
DBSecAdpt_SecAdptDllName parameter 380
DisableReverseProxy parameter 371, 377
eapps.cfg sample parameters 353
editing, about 376
EncryptApplicationPassword parameter 382
eservice.cfg sample 157
optional parameters 193, 356, 359
parameter values, table of 136
parameter values, usage guidelines 142
PasswordAttributeType parameter 366
PortName parameter 125, 367
relation to client 376
remote configuration file requirement 169
roles, setting 157
RolesAttributeType parameter 367
SecAdptDllName parameter 368
SecureBrowse parameter 371, 377
SecureLogin parameter 371, 377
SharedCredentialsDN parameter 368
SharedDBPassword parameter 368
SharedDBUsername parameter 369
Siebel Gateway Name Server parameters, about and table 361
SiebelAdapterUsername parameter 369
SingleSignOn parameter 369
SsIDatabase parameter 369
TLS-related parameters 360
TrustToken parameter 369
UseAdapterUsername parameter 369
UseRemoteConfig parameter 379
UserNameAttributeType parameter 370
configuring access control 319
contact users
adding new 245
existing contacts, promoting from 247
organizational association 271
cookies
auto-login cookie and Remember My User ID feature 204
auto-login credential 207
enabling 211
persistent 207
Siebel QuickStart 207, 211
corporate network security, overview 17
CRC parameter, about 365
credentials
authentication against directory 106
CredentialsAttributeType parameter 366
role in ADSI authentication 101
role in LDAP authentication 101
security adapter authentication process 106
credentials password hashing 158
CredentialsAttributeType parameter
about 366
setting for LDAP or ADSI 140
Crypt parameter 63
CSSSWEFrameListVisibilityAssoc class 329
CSSSWEFrameListVisibilityPick class 329
CSSSWEFrameUserRegistration class 226, 228
customer data, role in access control 264

D

data confidentiality, end-to-end encryption 23
data continuity, auditing, degrees of 26
data visibility, authorization to control
about 25
access control, record level 26
access control, view level 25
intrusion, preventing by secure physical deployment 27
data, categorized 307
database authentication
about 21
compared to other methods 99
delegated administration, availability of 249
implementing 103

limitations of 102
overview 102
password hashing 158
process overview 102
self-registration 218
database column, encrypted 77
database storage, data confidentiality 25
DBO password, changing 42
DBSecAdpt_CRC parameter, about 380
DBSecAdpt_SecAdptDllName parameter, about 380
deduplication
about 228
deduplication check, disabling 231
fields, modifying 230
Default Organization Division records, seed data 386
delegated administration
authentication requirements 249
delegated administrator responsibility, restricting 288
new customers, registering 251
partner applications, about 252
partner user, registering 252
registering users, about 250
responsibilities, assigning 253
write privileges, user directory 249
delegated administrators
about 248
delegated administration, administrator access 249
inheritance of responsibilities 248
New Responsibility field, editing 248
user authentication requirements 249
deployment options, LDAP and ADSI adapters 146
Developer Web Client
See Siebel Developer Web Client
digital certificate authentication 175, 191
digital certificates, installing on UNIX 60
directory
checking credentials against 106
creating users in 185
directory records, about 133
permissions record parameter 364
requirements 111
role of 101
shared database account deployment option 146
user records, adding 134
user, creating 133
DisableReverseProxy parameter 371, 377
divisions
base and extension tables, illustration 339
division records, deleting 279
Organization party type, in 333
relation to organization 340
role of 278
setting up (procedure) 283
documentation security references, bibliography 29
drilldown visibility, configuring 330
duplicate users
deduplication fields, modifying 230
self-registration deduplication check, disabling 231

E

eapps.cfg file
See configuration file
Employee base and extension tables, illustration 335
employee user
active position, changing 255
contact user, adding new 245
defined 335
Employee data model 335
employee setup, about completing 244
employee, deactivating 244
minimum requirements 242
new record, adding 242
New Responsibility field, population of 247
partner user, adding 244
position access control 267
position, active 255
primary position, changing 255
responsibilities, assigning 289
seed data record 383
employees, deactivating 244
Encrypt client Db password parameter 161
EncryptApplicationPassword parameter, about 382
EncryptedPassword parameter 45, 355
encryption
enabling on database table column 77
end-to-end for data confidentiality 23
Key Database Manager, using 80
Microsoft Crypto, configuring for 63
Mobile Web client, encryption for synchronization 73
new encryption keys, adding 81
RC2 encryption administration 74
RC2 encryption administration, upgrading 77
RSA configuring for 63
search encrypted data 77
Siebel Server for TLS encryption, configuring

for 65
Siebel Server, configuring Microsoft Crypto or RSA for 63
Siebel Web Server Extension, configuring for TLS encryption 68
TLS encryption, configuring Siebel Enterprise or Siebel Server 65, 68
types of 52
Unicode support 95
Web client, configuring for 72
Encryption Type parameter 63
Encryption Upgrade Utility
56-bit encryption upgrading 86
RC2 encryption, modifying the input file 84
RC2 encryption, prerequisites 83
EncryptSessionId parameter (eapps.cfg file) 210
EncryptSessionId parameter, about 355
encryptstring.exe 47
eservice.cfg file, LDAP sample 157
exporting tab layouts 317
external authentication
anonymous user record 214
Developer Web Clients, including 167
login credentials 214
password storage requirement 113
remote configuration option, about 167
remote security configuration file requirements 169
security adapters for 22
system testing 144
testing Web SSO 190

F

fields, self-registration
designating as required 226
locating 226
required property, removing 227
files, cookies 206
FindContact method
Forgot Your Password, modifying 236
input fields, adding or deleting 240
Forgot Your Password? question
architecture 235
comparison fields, modifying 238, 239
input fields, adding or deleting 240
new password, retrieving 233
null fields, processing of 237
Query User step parameters 237
using link, about 232
workflow process, about modifying 236
frame class 329

G

Gateway Name Server authentication
overview 165
Group Access control view 301
GUESTCP user ID 37, 384
GUESTCST user ID 37, 384
GUESTPW 133
GuestSessionTimeout parameter, about 356

H

hashing passwords 158
high interactivity client, self-registration 218
Household
administrative tasks 309
base and extension tables, illustration 342

I

IBM HTTP Server 22
IBM Tivoli Access Manager WebSEAL, disable proxy server 371, 377
IBM Tivoli Directory Server 22
importing tab layouts 317
industry standards, using 18
Info Center
categorized data, viewing 307
Explorer, about 307
IntegratedDomainAuth parameter
about 358
setting for Web SSO 188
IntegratedSecurity parameter 168
internal administrator, modifying New Responsibility field 248
Internet Assigned Numbers Authority, Private Enterprise Number 114

K

Key Database Manager
keyfile password, changing 81
new encryption keys, adding 81
running 80
key exchange for Microsoft Crypto or RSA encryption 64
keyfile password, changing 81
KeyFileName parameter 67, 69
KeyFilePassword parameter 67, 69

L

LDAP adapter
about 129
ApplicationPassword parameter 364
comparison with ADSI adapter 107

configuration file parameter values, table of 136
configuration file parameters, usage guidelines 142
delegated administrator, availability of 249
deployment options 146
directory records, about 133
installation prerequisites 130
restarting servers 143, 190
security adapter authentication 106, 128
security adapter process overview 101
Siebel Financial Services, about 389
Siebel Financial Services, implementing 389
SsIDatabase parameter 369
testing 144
user records, adding 134
users, creating 133
LDAP client
about 115
libsscforacleldap.sl file 368
libsscforacleldap.so file 368
license agreement, replacing default text 225
license key, role in view visibility 287
Local Access flag 288
login
account policies, about implementing 205
database authentication overview 102
password, storage of 113
requirements for views, setting or removing 217
login form
additional features 202
password expiration, about and implementing 205

M

Mainwin
See mwcontrol utility
manager access control, about 269
Manager List Mode user property 270
Manager visibility 269, 300
manager-subordinate relationship, about 269
master data
access control 275, 276
associating with access group 313
organization of 265
role in access control 264
Microsoft Active Directory 22
Microsoft Crypto encryption
configuring for 63
key exchange 64
Microsoft IIS 20
Microsoft Windows, changing SADMIN password 37
mobile applications
device user authentication 28
security, about 28
wireless communication, secure real time 28
mobile users
accessible views 289
authentication, restriction 99
positions and visibility rules 281
Mobile Web client, encryption for synchronization 73
multiple organizations
access control 271
benefits of 277
reasons for 278
mwcontrol utility 60

N

Name Server parameters, editing 143, 190
New Responsibility field
about 221
modifying 247, 248
population of 247
Novell NDS eDirectory 22
null fields, processing of 237

O

Oracle Database Client
about installing 115
installing 117
Oracle iPlanet Web Server 26
Oracle Wallet Manager
about 115
creating a wallet 121
organization access control
about 271
active organization and view access 288
associating responsibilities 288
customizable product visibility 273
multiple organization access, identifying views with 273
multiple-organization access control 271
single and multiple organizations 271
single-organization access control 271
suborganization access control 273
Organization base and extension tables, illustration 340
Organization data model, about 340
Organization group type, administrative tasks 309
Organization party type

defined 340
divisions, about 333
relationship rules 333
Organizational visibility 300
organizations
administrative tasks 309
benefits of 277
divisions, role of 278
multiple organizations, reasons for 278
positions, changing 281
setting up (procedure) 283
setting up, about 279
Owner party type 292
Owner Type Position view mode 300

P

parties
See party types
partner applications
delegated administrators, role of 252
duplication fields 230
primary position, changing 255
responsibilities, assigning 253, 289
self registration 219, 221
self-registration workflow views 224
Partner Organization base and extension tables, illustration 341
Partner Organization data model 341
partner user
adding 244
new user, registering 252
position access control 267
responsibilities, assigning 253, 289
Party base and extension tables, about and diagram 332
Party data model
about 332
Access group data model 344
Account data model 338
Division data model 339
Employee data model 335
Household data model 342
Organization data model 340
Partner Organization data model 341
Person (contact) data model 334
Position data model 337
User data model 334
User list data model 343
party types
about and table 260
access control, categorized master data 275
determining user access 292
parties, defined 261
relationships among party types 333
user lists, adding users 310
user lists, creating 310
password
changing default passwords 36
enabling fields for end user to change password 36
encrypt password in configuration file 382
expiration, about and implementing 205
failed tasks, checking for 43
Forgot Your Password architecture 235
Forgot Your Password link 232
hashing 158
retrieving a new password 233
SADMIN, changing on Windows 37
Table Owner (DBO) and password, changing 42
user profile, changing for 254
Web server images, adding a password for updating 45
PasswordAttributeType parameter
about 366
setting for LDAP or ADSI 140
PeerAuth parameter 67, 361
PeerCertValidation parameter 67, 361
permissions, authentication directory parameter 364
persistent cookie 207
Person base and extension tables, illustration 334
Person data type
contrasted with User 334
responsibilities, assigning 290
personal access control 266, 300
Personal visibility 267
physical deployment, Siebel Reports access 172
pick applets
special frame class, using for visibility 329
visibility 328
Pick List object, setting visibility 329
Popup Visibility Type property 328
Port parameter, setting for LDAP or ADSI 139
PortName parameter, about 125, 367
position access control, about implementing 267
Position base and extension tables, illustration 337
positions
active position, about 255
active position, changing 255
active position, designating 267
administrative tasks, listed 309

changing within organization 281
contact users, adding new 245
deleting 281
multiple employees, about 280
parent-and-child relationships 281
partner users and delegated administrators 252
Position data model 337
position hierarchy 269
position, defined 267
primary position 267
primary position, changing 255
renaming, cautions about 281
role in employee definition 335
setting up (procedure) 284
setting up, about 280
primary responsibility, assigning 316
Private Enterprise Number 114
Private key file name parameter (KeyFileName) 67
Private key file password parameter (KeyFilePassword) 67
ProtectedVirtualDirectory parameter
about 358, 359
not using for LDAP or ADSI 136
setting for Web SSO 188
proxy employee
about 271
seed data positions 386
PROXYE user ID 383

Q

Query User parameters 237

R

RC2 encryption administration
about 74
Key Database Manager, using 80
upgrading 77
RC2 encryption, upgrading to
56-bit encryption, upgrading 86
input file, modifying 84
prerequisites 83
referential data, access control strategy 276
registration, troubleshooting user registration issues 348
Remember My User ID feature 204
remote authentication 170
remote configuration option
applicable authentication strategies 169
external authentication, about implementing 167
implementation guidelines 169
REMOTE_USER variable 358
resources (security references), bibliography of 29
responsibilities
about 282
access control, implications of 286
Administrative views 282
anonymous user 216
assigned by delegated administrator 250
assigning 157
assigning to employee user 289
assigning to Partner 289
assigning to Person 290
associating with partner organizations 252
configuring access to business services 321, 327
configuring access to tasks 319
defined 287
defining 285
inheritance of 247
New Responsibility field 247
organizations, associating with 288
relation to job function 282
responsibility fields and self-registration 221
role of 157
seed data, about and table 384
seed data, modifying 216
seed responsibilities, modifying or deleting 282
System Preferences view, limiting access 282
user, assigning to 289
using roles to associate 114, 157
views, accessing locally 288
views, seeing included in responsibility 385
Reverse proxy server, disable 371, 377
roles
applicable authentication strategies 157
assigning 157
configuration file setting 157
storing in directory 114, 157
RolesAttributeType parameter
about 367
sample setting, eservice.cfg 157
RSA encryption
about 19
configuring for 63
key exchange 64

S

S_BU table 340, 341
S_CONTACT table 334, 335

S_EMP_PER table 335
S_ORG_EXT table 338, 340
S_ORG_GROUP table 342
S_ORG_PRTNR table 341
S_PARTY table
about and diagram 332
Access Group data model 344
Account data model 338
Division data model 339
Employee data model 335
Household data model 342
Organization data model 340
Partner Organization data model 341
Person (contact) data model 334
Position data model 337
User data model 334
User list data model 343
S_PARTY_GROUP table 344
S_PARTY_PER table 334
S_PARTY_REL table 334
S_PER_RESP intersection table 334
S_POSTN table 335, 337
S_USER table 334, 335
S_USERLIST table 343
SADMIN password
default 36
Microsoft Windows, changing on 37
salt user password
about 158, 367
parameter 127
SecAdptDllName parameter
about 368
setting for LDAP or ADSI 139
SecThickClientExtAuthent system preference 143
secure adapter communications deployment option 146
secure login
deployment option 203
implementing 203
SecureBrowse parameter, about 371, 377
SecureLogin parameter
about 377
setting for Web SSO 188
security
architecture, components of 20
industry standards, using 18
overview 17
security adapter
administrator login requirement 241
ASSI adapter requirements 111
comparison of LDAP and ADSI adapters 107
deployment options, listed 146
directory requirements 111
external security adapters, about implementing 100
LDAP and ADSI security adapter authentication 106
LDAP and ADSI security adapter authentication, implementing 128
operation modes 101
overview 100
SharedCredentialsDN parameter 368
Siebel Developer Web Client, and 167
single application access 106
security adapter authentication
adapter-defined user name, implementing 154
administration through Web Client 222
anonymous browsing, implementing 156
anonymous user, implementing 155
as authentication service 106
benefits 106
checksum validation 149
compared to other methods 99
credentials password hashing 158
digital certificate authentication 191
login password storage 113
password hashing 158
remote configuration option, about 169
roles, use of 157
Secure Sockets Layer, implementing 150
set-up, process overview 129
shared database account, implementing 151
user specification source, implementing 192
views, securing 201
security references, bibliography of 29
security roadmap, list of tasks 29
security system access, user authentication for
about 20
database authentication 21
external authentication, security adapters for 22
Web Single Sign-On (SSO) 22
seed data
anonymous user, about 134
anonymous user, using 216
Default Organization Division records, about 386
Employee record 383
GUESTCST user 216
non-employee User records (table) 384
position hierarchy 269
proxy employee 383
Proxy Employee Position, about 386
responsibilities seed data chart (table) 384
responsibilities, modifying 216

self-registration workflow processes, revising 225
Siebel Financial Service, about seed responsibilities and table 398
Siebel Financial Service, about seed users and table 397
Siebel Financial Services, registering and administering 391
user IDs, anonymous users 221
workflow processes, about modifying 224

self-registration
about 218
activating (procedure) 222
anonymous user record, modifying 220
application-specific examples 218
business components 221
components of self-registration 220
configuration parameter 221
custom business services, about 225
deduplication check, disabling 231
fields, redefining required fields 226
license agreement, replacing default 225
registering, user perspective 219
Siebel Financial Services, registering and administering 392
user deduplication, about 228
views, about modifying 224
workflow processes, activating 222
workflow processes, viewing 222

self-registration fields
adding fields to a view 227
automatic population 221
class specification 226
data collection process overview 227
deduplication fields, modifying 230
duplicate user updates, preventing 229
required property, removing 227
required, designating as 226
virtual fields, use of 225

self-registration workflow processes
data collection overview 227
deduplication checks, disabling 231
deduplication fields, modifying 230
duplicate user updates, preventing 229
fields, adding to views 227
new applets, including 228
seed data, revising 225
views, table of 223

ServerName parameter
description 368
setting for LDAP or ADSI 139

session cookies
about 72
modes on the SWSE 206

SessionTimeout parameter, about 193, 356, 359

SessionTimeoutWarning parameter 354, 357

SessionTracking parameter 207

shared database account deployment option 146

shared database account, implementing 151

SharedCredentialsDN parameter
about 368
setting for LDAP or ADSI 141

SharedDBPassword parameter
about 368

SharedDBUsername parameter
about 369

Siebel Configuration Wizard, running for SWSE 69

Siebel database
contact user, adding new 245
employee setup, about completing 244
employee, deactivating 244
new employee, adding 242
New Responsibility field, population of 247
partner user, adding 244
position, role of 242
user records, adding 134, 186

Siebel Developer Web Client
compared to Standard Web Client 167
configuration file 376
security adapter system preference 143

Siebel Enterprise security token 45

Siebel Financial Services
access control mechanisms 394
access-group access control, administering 394
anonymous browsing, registering and administering 392
applications (table) 388
configuration file names, about and table 396
eapps.cfg file and eapps_sia.cfg, about and table 390
external administration of users 393
internal administration of users 393
LDAP and ADSI security adapter authentication 389
LDAP and ADSI security adapter authentication, implementing 389
seed data, registering and administering 391
seed responsibilities, about and table 398
seed users, about and table 397
self-registration, registering and administering 392

unregistered users, registering and administering 392
user profile, about maintaining 393
Web SSO authentication, implementing 390
Siebel Gateway Name Server parameters
about and table 361
custom security adapter authentication 370
database authentication 362, 370
LDAP and ADSI authentication 364, 370
parameters for Application Object Manager 371
Siebel QuickStart cookie 207, 211
Siebel Reports, securing access 172
Siebel Security Adapter Software Developers Kit (SDK), about 23
Siebel Server
configuration file 376
TLS, setting additional name server parameters 68
Siebel Web Client, administering security adapter authentication 222
Siebel Web Engine, sample configuration parameters 353
Siebel Web Server Extension
role in database authentication 102
TLS encryption, configuring 68
SiebelAdapterUsername parameter, about 369
SiebEntSecToken parameter
See Siebel Enterprise security token
single application access 106
single sign-on
See Web SSO
single-organization access control 271
single-position access control 268, 300
SingleSignOn parameter
about 357, 369
not using for LDAP or ADSI 136
setting for Web SSO 187, 189
spoofing attacks, protecting against 357
sscforacleldap.dll file 368
sscfsadb.dll file 380
SslDatabase parameter, about 369
Standard Encryptor 96
standard interactivity, self-registration 218
Standard Web Client and Developer Web Client, compared 167
suborganization access control
about 273
accessible data 300
SubUserSpec parameter, about 357
Sun Java System Directory Server 22
system preferences, editing 143

T

tab layouts
administering tab layout 315
importing and exporting 317
managing through responsibilities, about 315
primary responsibility, assigning 316
Table Owner (DBO), changing and password 42
team access control 268, 300
test user
about 133
Siebel database, adding records for 134
Web SSO authentication 185
testing external authentication system 144
TESTPW 133
TESTUSER 133
TLS communication, about 19
TLS encryption
configuring for 65
Siebel Server, setting additional name server parameters 68
SWSE, configuring for 68
token, Siebel Enterprise 45
transaction data, access control strategies 276
troubleshooting
access control issues 350
Administration - Server Configuration screen, unable to work in 346
user registration issues 348
TrustToken parameter
about 357, 369
not using for LDAP or ADSI 136
setting for Web SSO 187, 189

U

Unicode support 95
UNIX, installing certificates 60
unregistered users
anonymous user record 214
granting view access 215
parameter controlling 371
seed anonymous user, about 216
Siebel Financial Services, registering and administering 392
views, setting or removing explicit login 217
UseAdapterUsername parameter 369
User
contrasted with Employee 335
defined 334
responsibilities, assigning 289
User data model 334

user administration
delegated administrators 248
Siebel database, adding user to 241
user profile, maintaining 253
user authentication
See authentication
User business component, underlying tables 241
user credentials, source designation parameter 358
User data model 334
user deduplication, about 228
user directory
self-registration parameter 221
write privileges 241, 249
User List base and extension tables, illustration 343
User list data model, about and diagram 343
User lists
creating 310
users, adding 310
user profile
about updating 253
active position, changing 255
passwords, changing 254
personal information, editing 254
user records
adding to Siebel database 134
data collection, process overview 227
seed data, provides as (table) 384
user registration
registering, about 213
requirements 214
seed data 214
troubleshooting issues 348
User Registration business component
comparison fields, modifying 239
deduplication fields, excluding 229
deduplication fields, modifying 230
Forgot Your Password architecture 235
new applets 228
Query User step parameters 237
self-registration views 225
User Registration business service 236
User specification source
about 175
implementing 192
UseRemoteConfig parameter 169, 379
UserNameAttributeType parameter
about 370
setting for LDAP or ADSI 140
users, Siebel database, adding to 242
UserSpec parameter
about 358
not using for LDAP or ADSI 136
setting for Web SSO 188
UserSpecSource parameter
about 358
not using for LDAP or ADSI 136
setting for Web SSO 188

V

Validate peer certificate parameter (PeerCertValidation) 67
view access, unregistered users 215
views
adding fields 227
displaying view properties 299
explicit login requirements, setting or removing 217
group access control 301
license key and visibility 286
limiting access to 282
new applets, including 228
responsibility, role in access 287
securing 201
self-registration views, related business components 225
self-registration workflow views, table of 223
view construction, example 302
view, defined 258
virtual directories
creating 183
ProtectedVirtualDirectory parameter 358, 359
virtual fields, self-registration process 225
visibility
All 299
Manager 269
Personal 267
positions, role of 280
responsibilities, role of 282
view visibility properties 286
visibility applet
access control, types of 299
business component and view connection 286
field display, role in 299
view construction example 302
Visibility Applet Type property 330
Visibility Auto All property, using 329
Visibility Type property 329, 331

W

wallet, creating 121
Web browser, security settings for 29

Web Client users, authentication compatibility 99
Web client, configuring encryption for 72
Web server images, adding a password for updating 45
Web servers
IBM HTTP Server 22
Microsoft IIS 20
Oracle iPlanet Web Server 26
Web SSO
about 22
anonymous browsing, implementing 156
anonymous user, implementing 155
checksum validation 149
credentials password hashing 158
digital certificate authentication 191
Secure Sockets Layer, implementing 150
shared database account, implementing 151
Siebel Financial Services, implementing 390
user credential source designation 355, 358
user specification source, implementing 192
views, securing 201
virtual directory 358, 359
Web SSO adapter
adapter-defined user name, implementing 154
ApplicationUser parameter 364
BaseDN parameter 365
CredentialsAttributeType parameter 366
deployment options, listed 146
PasswordAttributeType parameter 366
PortName parameter 125, 367
remote configuration option, about 169
roles, use of 157
RolesAttributeType parameter 367
SecAdptDllName parameter 368
security adapter process overview 101
SingleSignOn parameter 369
SsIDatabase parameter 369
TrustToken parameter 369
UserNameAttributeType parameter 370
Web SSO authentication
about 173
authentication process, overview 176
compared to other methods 99
digital certificate authentication 175
implementation considerations 174
implementation, about 174
remote authentication 170
self-registration 218
setup scenario 181
user specification source option 175
Web SSO, setup scenario
Active Directory server, setting up 181
Active Directory Service Interfaces server, password assignment 182
Active Directory Service Interfaces, configuring as directory 182
creating users in the directory 185
sample configuration 181
setup tasks 180
testing 190
user records, adding to Siebel database 186
virtual directories, creating 183
Windows
ADSI client requirement 114
SADMIN password, changing 37
Windows Integrated Authentication 358
wireless communications, secure real time 28
workflow processes
activating (procedure) 222
custom business services, about 225
license agreement text, replacing 225
revising 225
seed data, revising 225
seed processes, about modifying 224
self-registration workflow views, table of 223
self-registration, activating processes 222
viewing 222

X

X.500 Object ID 114
X.509 authentication 19