Siebel

Security Guide

October 2026

Siebel
Security Guide

October 2026

F84292-15

Copyright © 1994, 2026, Oracle and/or its affiliates.

Author: Sukanya Mishra

Contents

Get Help i

1 What's New in This Release 1

What's New in This Release 1

2 Overview of Security for Siebel CRM 7

About Security for Siebel CRM 7
About This Guide 7
General Security Concepts 8
Industry Standards for Security 8
About Supported Security Products 9
Siebel Security Architecture 10
Web Sites with Security Information 17
Using Transport Layer Security with Siebel CRM 17
Supported TLS and SHA Versions 18
About Siebel Open UI 20
Roadmap for Configuring Security 21

3 Changing and Managing Passwords 23

Changing and Managing Passwords 23
About Managing and Changing Passwords 23
About Default Accounts 26
Changing Siebel Administrator Account Password 28
Changing the Anonymous User Password When a User Account is set to Anonymous User 36
Changing the Table Owner Password 36
Troubleshooting Password Changes By Checking for Failed Server Tasks 37
About Siebel Gateway Authentication Password 38
Encrypted Passwords in Siebel Application Interface Profile Configuration 39
Changing Encrypted Passwords Using the Siebel Management Console 39
About Encryption of Siebel Gateway Password Parameters 40
About the Object Manager's First Connection and LDAP User 41

4 Communications and Data Encryption 43
Communications and Data Encryption 43
Types of Encryption 43
About Certificates and Key Files Used for TLS Authentication 53
Process of Configuring Secure Communications 55
Installing Certificate Files 55
Configuring TLS Mutual Authentication for SHA-2 Certificates Using EAI HTTP Transport 60
About Configuring Encryption for Siebel Enterprise and Siebel Application Interface 62
About Key Exchange for TLS Encryption 62
Configuring TLS Encryption for a Siebel Enterprise or Siebel Server 62
Configuring TLS Encryption for Siebel Application Interface 65
Enabling SSL Acceleration for Application Interface/Enabling HTTP 66
About Configuring Encryption for Web Clients 68
Configuring Encryption for Mobile Web Client Synchronization 69
About Data Encryption 70
About Siebel Encryption 75
Configuring Encryption and Search on Encrypted Data 76
Encrypting Columns in a Business Component 78
Managing the Key File Using the Key Database Manager 79
Security Considerations for Unicode Support 83
About Encoding UI Values 83

5 Security Adapter Authentication 85
Security Adapter Authentication 85
About User Authentication 85
About Siebel Security Adapters 87
About Database Authentication 89
Implementing Database Authentication 90
About Authentication for LDAP Security Adapter 92
Process of Implementing LDAP Security Adapter Authentication 96
About Authentication for Siebel Gateway Access 109
About Authentication for Mobile Web Client Synchronization 113
Installing and Configuring Oracle LDAP Client Software 114
Configuring Security Adapters Using the Siebel Management Console 117
Migrating from Database to LDAP Authentication 119
Security Adapter Deployment Options 120
Security Adapters and the Siebel Developer Web Client 129

About Password Hashing 132
Process of Configuring User and Credentials Password Hashing 133
Running the Password Hashing Utility 137
Setting the ConfigLdapAuthTimeout Parameter 138
Setting the ConfigLdapFailoverTimeout Parameter 139

6 Single Sign-On Authentication 141
Single Sign-On Authentication 141
Supported Single Sign-On Solutions for Siebel Deployment 141
About Web Single Sign-On 142
About Implementing Web Single Sign-On 144
Web Single Sign-On Authentication Process 144
Requirements for Standards-Based Web Single Sign-On 146
Set up Tasks for Standards-Based Web Single Sign-On 146
Configuring the Session Timeout 147
Configuring Siebel CRM and Oracle Business Intelligence Enterprise Edition for Web Single Sign-On 148
Configuring Siebel Migration Application for Web Single Sign-On 149
Web Single Sign-On Authentication Process When Using Siebel REST and Web Services in Portal Application 150
About Implementing Federated Single Sign-On 152
Federated Single Sign-On Authentication Process for Interactive User Interfaces 153
Single Sign-On between Siebel and Identity Cloud Service through SSO or Open ID 154
Identity Provider-Initiated Single Sign-On Authentication Process 158
About Oracle API Gateway Role in Single Sign-On Authentication Process 160
Security Adapter Configuration When SSO is Enabled 160
Configuring Single Sign-On with a Database Security Adapter 161
Using OAuth with Siebel REST 167

7 Siebel Application Interface Security Features 187
Siebel Application Interface Security Features 187
About the Siebel Web Client and Using HTTPS 187
Implementing Secure Login 188
Logging Out of a Siebel Application 188
Login User Names and Passwords 188
Account Policies and Password Expiration 189
About Using Cookies with Siebel Business Applications 189
About Service Discovery Initiated by Trusted and Untrusted Sources in Siebel Application Interface 193

8 User Administration 195

User Administration 195
About User Registration 195
About Anonymous Browsing 196
Process of Implementing Anonymous Browsing 197
About Self-Registration 199
User Experience for Self-Registration 200
Process of Implementing Self-Registration 201
Identifying Disruptive Workflows 211
About Managing Forgotten Passwords 212
Internal Administration of Users 220
About Adding a User to the Siebel Database 220
Delegated Administration of Users 227
Maintaining a User Profile 231

9 Configuring Access Control 235

Configuring Access Control 235
About Access Control 235
Access Control Mechanisms 241
Planning for Access Control 250
Setting Up Divisions, Organizations, Positions, and Responsibilities 257
About View and Data Access Control 260
Listing the Views in an Application 261
Responsibilities and Access Control 261
Viewing Business Component View Modes 265
Configuring Access to Business Components from Scripting Interfaces 268
Viewing an Applet's Access Control Properties 270
Listing View Access Control Properties 271
Example of Flexible View Construction 275
About Implementing Access-Group Access Control 276
Implementing Access-Group Access Control 280
Managing Tab Layouts Through Responsibilities 286
Managing Tasks Through Responsibilities 289
Administering Access Control for Business Services 291
Administering Access Control for Business Processes 297
Clearing Cached Responsibilities 297
About Configuring Visibility of Pop-Up and Pick Applets 298

About Configuring Drilldown Visibility 300
Party Data Model 302

10 Troubleshooting Security Issues 315
Troubleshooting Security Issues 315
Troubleshooting User Authentication Issues 315
Troubleshooting User Registration Issues 316
Troubleshooting Access Control Issues 317

11 Authentication-Related Configuration Parameters 319
Authentication Related Configuration Parameters 319
Server Parameters for Siebel Gateway 319
Security Profile Configuration for Siebel Gateway 320
Parameters for Configuring Security Adapter Authentication 321
Authentication and Security-Related Parameters in the Enterprise Profile 328
Security-Related Parameters in the Server Profile 329
Siebel Application Interface Profile Parameters 329
Siebel Application Configuration Parameters 336

12 Predefined Data 341
Seed Data 341
Seed Employee 341
Seed Users 341
Seed Responsibilities 344

13 Siebel Security Hardening 347
Siebel Security Hardening 347
About This Chapter 347
Overview of Security Threats, Recommendations, and Standards 348
Securing the Network and Infrastructure 352
Securing the Operating Systems 376
Securing the Siebel Database 386
Securing Siebel Business Applications 388
Implementing Auditing 397
Performing Security Testing 399
Supported Security Standards 401

Default Port Allocations 404

Get Help

Preface

This preface introduces information sources that can help you use the application and this guide.

Using Oracle Applications

To find guides for Oracle Applications, go to the Oracle Help Center at *https://docs.oracle.com/*.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the *Oracle Accessibility Program website*.

Contacting Oracle

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit *My Oracle Support* or visit *Accessible Oracle Support* if you are hearing impaired.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send an email to: *oracle_fusion_applications_help_ww_grp@oracle.com*.

1 What's New in This Release

What's New in This Release

This chapter tracks the changes in the documentation. It includes the following topics:

- *What's New in Siebel Security Guide, Siebel CRM 26.10 Update*
- *What's New in Siebel Security Guide, Siebel CRM 26.5 Update*
- *What's New in Siebel Security Guide, Siebel CRM 26.4 Update*
- *What's New in Siebel Security Guide, Siebel CRM 25.10 Update*
- *What's New in Siebel Security Guide, Siebel CRM 23.9 Update*
- *What's New in Siebel Security Guide, Siebel CRM 22.12 Update*
- *What's New in Siebel Security Guide, Siebel CRM 22.3 Update*
- *What's New in Siebel Security Guide, Siebel CRM 21.7 Update*
- *What's New in Siebel Security Guide, Siebel CRM 21.5 Update*
- *What's New in Siebel Security Guide, Siebel CRM 21.3 Update*

What's New in Siebel Security Guide, Siebel CRM 26.10 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Restricting EAI File Transport File System Access	New topic. Added documentation for the EAI File Transport Business Service that now validates both read and write paths against the default and configured folder allowlist.

What's New in Siebel Security Guide, Siebel CRM 26.5 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Adding Custom HTTP Headers to Responses from Siebel	New topic. This topic describes how to add or update custom HTTP response headers in Siebel (version 26.5 and above) by configuring the **`GenericHeadersFilter`** in the Siebel **`web.xml`**, along with guidance to validate changes through thorough testing, especially for security-related headers.

What's New in Siebel Security Guide, Siebel CRM 26.4 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Certificate Requirements for Communications	Modified topic. This topic is updated to describe the industry change removing the Client Authentication EKU from publicly trusted certificates and the Siebel 26.3 requirement to use separate server and client certificates/keystores for HTTPS and mTLS.

What's New in Siebel Security Guide, Siebel CRM 25.10 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Inbound REST Requests and OAuth Scopes	New topic. Describes Inbound REST Requests and OAuth Scopes.

What's New in Siebel Security Guide, Siebel CRM 23.9 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Procedure to Modify Encryption Seed	New topic. The procedure to apply custom seed for encryption is applicable from Siebel release 23.6 and it is a non-mandatory post installation task. There is no need to re-apply customer seed in the subsequent patch once it is enabled in 23.6 or above updates.

What's New in Siebel Security Guide, Siebel CRM 22.12 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Changing Siebel Administrator Account Password on UNIX *Changing Siebel Administrator Account Password on Windows*	Modified topics. Steps 8-11 are new in these procedures (and apply to Siebel CRM 17.x Update and later releases).
About the Siebel Web Client and Using HTTPS	Modified topic. Added information about using HTTP/HTTPS with Siebel Application Interface and SES.
Using OAuth with Siebel REST	New topic. Describes the customizations required to use OAuth with Siebel REST.
Using OAuth with Siebel REST Inbound Web Services	New topic. Outlines the keynotes for using OAuth with Siebel REST inbound Web services.
Configuring OAuth Support for Siebel REST Outbound Connections (21.8 to 22.8)	New topics. Describes how to configure OAuth support for Siebel REST outbound connections for Siebel Update 21.8 to 22.8.

Topic	Description
• *Add Script for OAuth Support* • *Sample Script*	
Configuring OAuth Support for Siebel REST Outbound Connections (22.9+) • *Add Script for OAuth Support* • *Sample Script*	New topics. Describes how to configure OAuth support for Siebel REST outbound connections for Siebel Update 22.9 onwards.

What's New in Siebel Security Guide, Siebel CRM 22.3 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Certificate Requirements for Communications (second bullet and Step 1) *Modifying Server Keystore, Client Keystore and Truststore Files* (Step 2c) *Disabling Certificate Based Mutual Authentication* (Step 1 and Step 2) *Siebel Application Interface Profile Parameters* (very last line removed)	Modified topics. As of Siebel CRM 22.3 Update, Siebel Enterprise Cache is no longer supported.

What's New in Siebel Security Guide, Siebel CRM 21.7 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Centralizing the Location of the Key File	New topic. Depending on your requirements, you can optionally centralize the location of the key file (keyfile.bin, installed by default in the `SIEBSRVR_ROOT\admin` directory) for your Siebel CRM deployment, such as in the Siebel File System or in another secure repository.
Session Cookies with sameSiteCookies Set to Strict	New topic. Describes how to modify `sameSiteCookies="Strict"`.
Siebel Application Configuration Parameters	Modified topic. You can use LDAP authentication with Siebel Tools.
Managing Ciphers	Modified topic. Describes how to manage ciphers in Siebel CRM 17.0 and later. This topic was previously called *Disabling Weak Ciphers*.

What's New in Siebel Security Guide, Siebel CRM 21.5 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Disabling Weak Ciphers	New topic. This topic was renamed *Managing Ciphers* in Siebel CRM 21.7 Update.
Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode	Modified topic. This procedure shows how to create a Siebel Gateway security profile with Database Authentication Advanced mode for Single Sign-On (SSO) and non-SSO. When creating a Siebel Gateway security profile with Database Authentication Advance mode, the Database Connection can be one of the following: any SQL Style of Database, Oracle Data Guard, or Oracle RAC (Real Application Clusters).
Configuring Object Manager's Database Security Adapter in Advanced Mode	Modified topic. This topic is specific to SSO.

What's New in Siebel Security Guide, Siebel CRM 21.3 Update

The following table lists the changes in this revision of the documentation to support this release of the software.

Topic	Description
Enabling SSL Acceleration for Application Interface/Enabling HTTP	Modified topic. Describes how to configure SSL acceleration for communications between application interface traffic.
Updating siebel.cfg Before Running Key Database Manager	New topic. Describes the parameters to set in the siebel.cfg file before running the Key Database Manager utility.
Setting the ConfigLdapFailoverTimeout Parameter	New topic. Describes why and how to configure the ConfigLdapFailoverTimeout parameter, which is a new configuration parameter for the LdapSecAdpt subsystem available as of Siebel CRM 21.1 Update.
Configuring Object Manager's Database Security Adapter in Advanced Mode	Modified topic. The SecAdptMode parameter must be set to DBSSO (as of 21.3 Update) if you implement Single Sign-On (SSO) with a database security adapter.
Procedure to Configure Reverse Proxy	Modified topic. Shows how to modify the server.xml file to include separate connectors for internal and external users who are on the same application interface.
Multiple topics.	As of Siebel CRM 21.2 Update, the **`applicationcontainer`** directory has been replaced by two directories, as follows: • **`applicationcontainer_external`** (for Siebel Application Interface) • **`applicationcontainer_internal`** (for all other Siebel Enterprise components) In the Siebel Application Interface Installation, Web artifacts for application configurations, which were formerly located in **`applicationcontainer\webapps\siebel`**, now map to **`applicationcontainer_external\siebelwebroot`**. The **`siebelwebroot`** directory contains subdirectories such as **`files`**, **`fonts`**, **`htmltemplates`**, **`images`**, **`migration`**, **`scripts`**, and **`smc`**.

2 Overview of Security for Siebel CRM

About Security for Siebel CRM

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*
- *General Security Concepts*
- *Industry Standards for Security*
- *About Supported Security Products*
- *Siebel Security Architecture*
- *Web Sites with Security Information*
- *Using Transport Layer Security with Siebel CRM*
- *Supported TLS and SHA Versions*
- *About Siebel Open UI*
- *Roadmap for Configuring Security*

About This Guide

This guide provides recommendations for safeguarding your Siebel CRM 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 Siebel CRM data, you must secure both your Siebel Business Applications and the computing environment in which they run.

This guide provides the information you need to protect your Siebel CRM deployment:

- It describes the Siebel security architecture and security concepts.
- It outlines the security controls provided by Siebel CRM.
- It provides detailed procedural information on how to implement the security controls to secure your application.
- *Siebel Security Hardening* provides general recommendations for securing Siebel CRM and the deployment environment (network, operating system, database).
- *Siebel Security Hardening* provides detailed procedural information on implementing Siebel security controls only where such information isn't provided elsewhere in the Siebel Bookshelf.

Note: The Siebel Bookshelf is available on Oracle Help Center. 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:

- 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 nor 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 CRM. These services are intended to counter security attacks; they use one or more security mechanisms to provide the service.

Industry Standards for Security

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

Supported standards include:

- **Lightweight Directory Access Protocol (LDAP).** Siebel CRM provides preconfigured integration with LDAP for user authentication purposes. For more information, see *Security Adapters for LDAP Authentication* and *Security Adapter Authentication*.
- **Communications encryption.** Siebel CRM supports the use of Transport Layer Security (TLS) encryption and authentication for communications encryption.

  You can use TLS to protect communications between the following:
  - Siebel CRM 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 TLS for Web server and Siebel Web Client communications is transparent to Siebel CRM.
- Siebel Servers and Microsoft Exchange Server email servers.

For more information on configuring TLS, see the information in the following table.

Information Type	Topic
Configuring TLS for communication between Siebel Web clients and Siebel Application Interface.	*About the Siebel Web Client and Using HTTPS*
Configuring TLS for communication between Siebel components.	*Process of Configuring Secure Communications*
Using TLS to secure user login credentials	*Implementing Secure Login*
Using TLS to secure communications between Siebel Servers and directory servers.	*Configuring Secure Communications for Security Adapters*

- **SHA-2 password hashing.** Siebeluser passwords can be hashed using the SHA-2 algorithm. For more information, see *About Password Hashing*.
- **AES.** Siebeldata can be encrypted using Advanced Encryption Standard (AES). Multiple key lengths are supported for AES. For more information, see *Data Encryption*.

About Supported Security Products

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

https://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 CRM. For information on the Oracle Identity Management products, go to

https://www.oracle.com/middleware/identity-management/

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

> **Note:** For Siebel CRM, the system requirements and supported platform certifications are available from the Certification 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

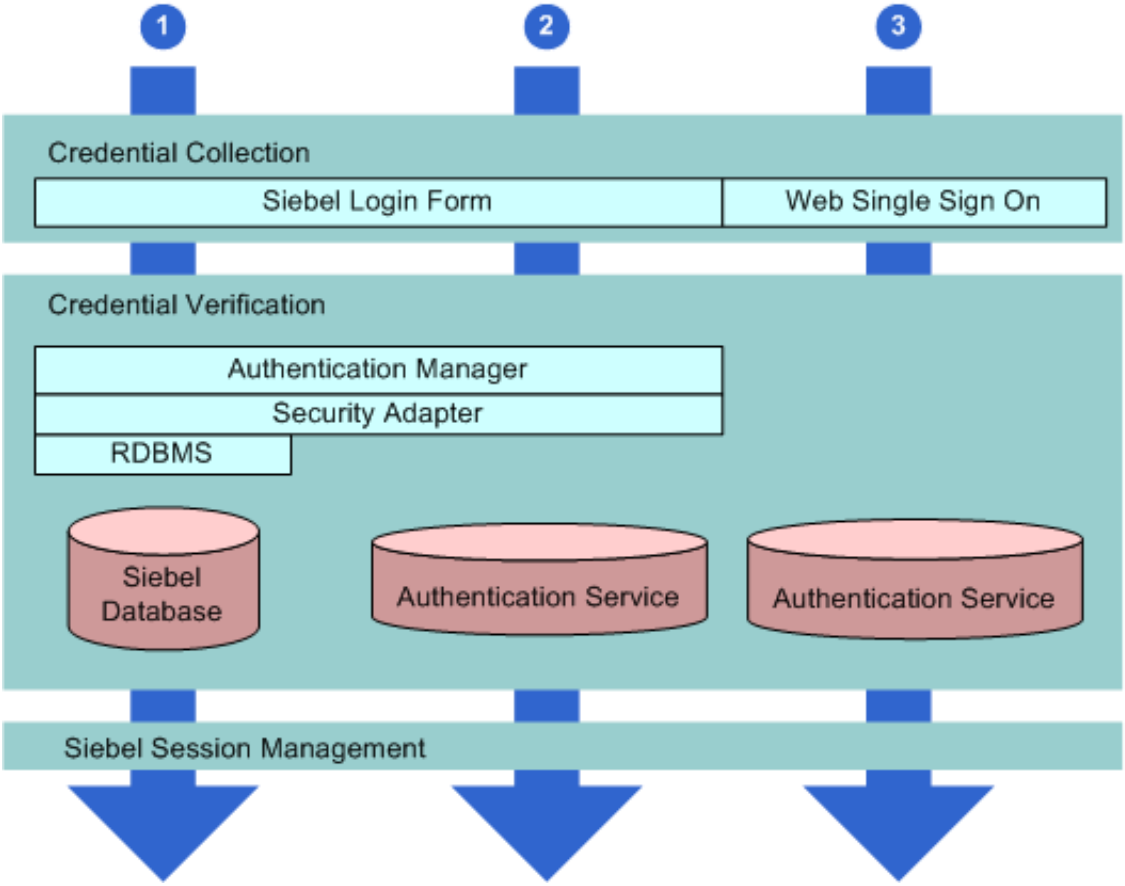
Siebel CRM provides an open authentication architecture that integrates with a customer's selected authentication infrastructure. For more information, see *Security Adapter Authentication* and *Single Sign-On Authentication*. Siebel CRM supports three types of user authentication. A logical view of each type of authentication is illustrated in the following figure, 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. For more information, see *Security Adapter for Database Authentication*.
2. **LDAP authentication.** LDAP security adapters are provided to support credential collection and verification of users in an LDAP-compliant directory. For more in formation, see *Security Adapters for LDAP Authentication*.
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. For more information, see *Web Single Sign-On*.

Customers can also develop custom security adapters using a security adapter SDK. For more information, see *Security Adapter SDK*.

The authentication mechanisms illustrated in the following figure apply whether users access Siebel CRM from within a LAN or WAN, or remotely.

> **Note:** When using multiple authentication mechanisms simultaneously, one application interface per authentication mechanism must be installed and configured. This applies to all Siebel versions using application interface.



Security Adapter for Database Authentication

Siebel CRM provides 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 CRM, such as workflow processes to support user self-registration or forgotten password scenarios (capabilities commonly used in customer applications), require authentication using LDAP 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 Authentication

For employee or customer applications, Siebel CRM includes a preconfigured security adapter interface to allow organizations to externalize credential verification in an LDAP-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 authentication, refer to the documentation from your vendor.

Siebel customers can therefore verify user credentials with security standards such as LDAP.

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.

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

Web Single Sign-On

Siebel CRM offers customers the capability of enabling a single login across multiple Web applications; this is known as Web Single Sign-On (SSO). Siebel CRM provides 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 CRM, 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 biometrics or smart cards.

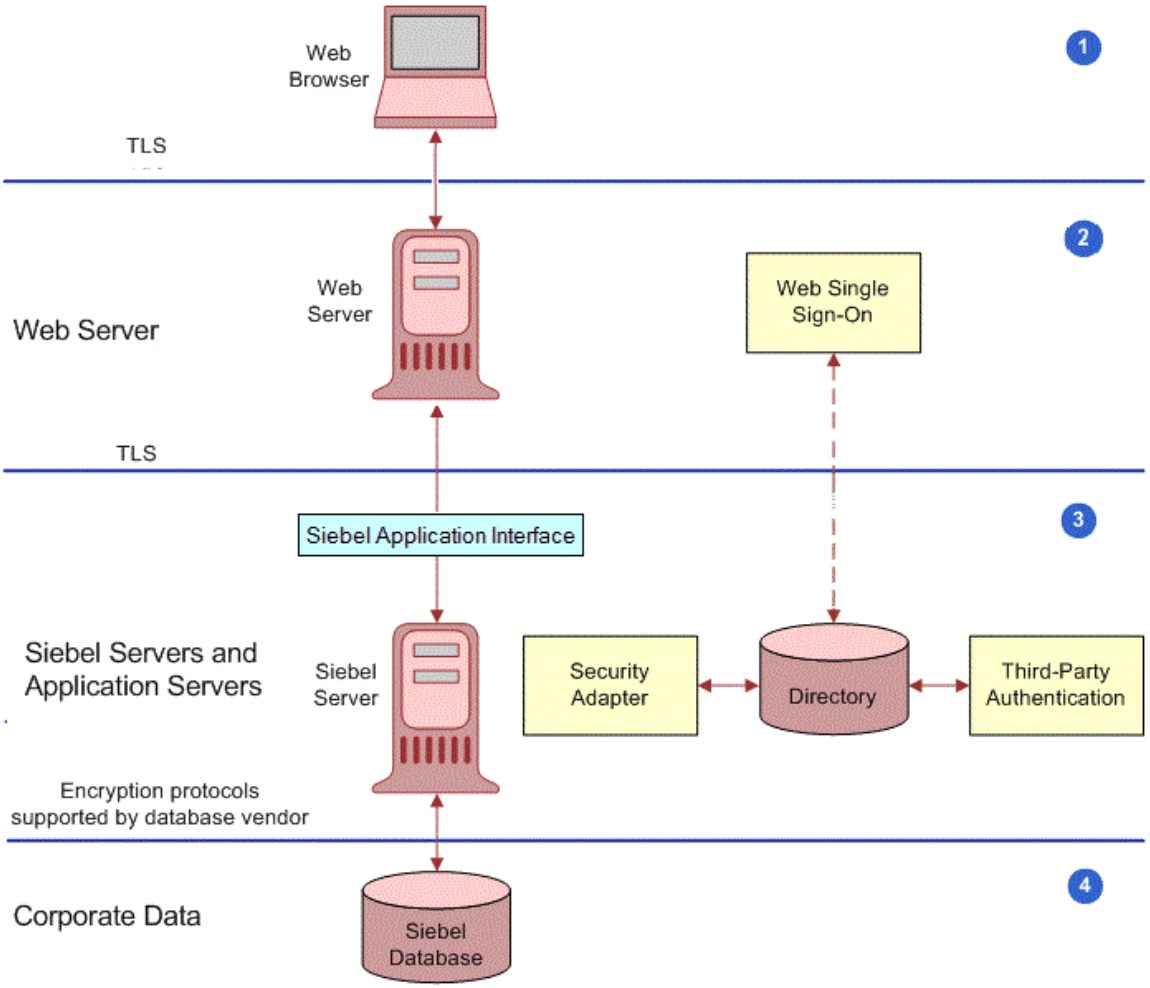
For example, a security adapter might be created for a portable device that provides users with a key that changes at frequent intervals. When a security adapter for this device is deployed, only by supplying both the currently displayed key and the user's password or other credentials can the user gain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

The security adapter interface is critical to the Siebel architecture because, for most Siebel 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.

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. The following figure shows the types of encryption available for communications within the Siebel environment.



This figure shows that communications encryption is available between the following:

1. **Client Browser to Web Server.** Siebel CRM runs 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 Siebel Application Interface 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 on the login view to protect password transmission. See *Implementing Secure Login*.
   - Use HTTPS for the entire application. See *About the Siebel Web Client and Using HTTPS*.

2. **Web Server to Siebel Server.** Siebel CRM components communicate over the network using Siebel TCP/IP using TLS. 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*.

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 CRM allows 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 CRM supports data encryption using AES algorithms. For more information, see *Data Encryption*.

About Controlling Access to Data

Authorization refers to the privileges or resources that a user is entitled to within Siebel CRM. Even among authenticated users, organizations generally want to restrict visibility to operating system data. Siebel CRM uses 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 *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 CRM, 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 Siebel CRM 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 CRM uses 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 CRM supports various degrees of auditing:

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

Secure Physical Deployment to Prevent Intrusion

Access to the physical devices that host Siebel CRM 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 CRM also supports and requires 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 CRM works 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 CRM 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*.

Security for Mobile Solutions

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

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

- For information about security issues when accessing Siebel CRM 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* and *About Authentication for Mobile Web Client Synchronization*. *Siebel Remote and Replication Manager Administration Guide* provides additional information on Mobile Web Client security measures.

Mobile Device User Authentication

Mobile devices themselves must be secure. If a mobile device falls into the wrong hands, then organizations need assurance that sensitive data will not be compromised. Siebel CRM is 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 CRM work in conjunction with security or other settings on the Web browser.

For information about the browser standards required for Siebel Open UI, see the Certifications tab on My Oracle Support and *About Siebel Open UI*. 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

  https://www.oracle.com/security/index.html
- 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 one of the preceding URLs is no longer active, then try using a Web search engine to find the new location.

Using Transport Layer Security with Siebel CRM

It is strongly recommended that you implement Transport Layer Security (TLS) encryption for all of the following services and communication paths in a Siebel CRM implementation:

Note: The use of Secure Sockets Layer (SSL) v3.0 encryption for environments with security requirements is not supported by Oracle for Siebel CRM as a result of security vulnerabilities discovered in the design of SSL v3.0.

- For communications between Siebel Web server and Siebel Web Client.
- For communications between Siebel Server and the Web server.
- For encryption of communications between Siebel Enterprise components, for example, communications between the Siebel Server to Siebel Web server (Siebel Application Interface), or between Siebel Servers.
- For communications between an LDAP security adapter and a directory server.
- For communications using Siebel CRM external interfaces (EAI), which use Web services to send and receive messages over HTTP.
- For communications between Siebel Server and an email server, including encryption for SMTP, IMAP, and POP3 sessions between Siebel Server and an email server.

For more information about configuring security in Siebel CRM, see *Roadmap for Configuring Security*.

Note: To ensure that you are using the highest level of security, download and install the current Siebel CRM Update release to enable the highest level of security and obtain the latest security-related patches. For more information about installing the current Siebel CRM Update release and about Siebel release types, see Siebel Installation Guide for the operating system you are using. For more information about installing Siebel Patchset releases, including new features, see *Siebel CRM Update Guide and Release Notes* on My Oracle Support, 23824315.1 (Article ID), for each applicable release.

Supported TLS and SHA Versions

This topic lists the level of support for TLS. Siebel implements TLS security for the services and communication paths listed in *Using Transport Layer Security with Siebel CRM*.

TLS Support

It is strongly recommended that you move the following services in Siebel to a more secure TLS configuration as follows:

- Siebel Application Interface to Client HTTPS traffic encrypted via TLS 1.2 or TLS 1.3.
- Siebel Server to Cloud Gateway internal traffic encrypted via TLS 1.2 or TLS 1.3.
- Siebel EAI/Web Services over HTTPS encrypted over TLS 1.2 or TLS 1.3.
- Siebel IMAP/POP encrypted over TLS 1.2 or TLS 1.3.
- Application Interface to Siebel Server Traffic encrypted over TLS 1.2 or TLS 1.3.
- Siebel Enterprise SISNAPI Traffic encrypted over TLS 1.2 or TLS 1.3.
- Siebel LDAPS client encrypted over TLS 1.2.
- Siebel Management Server/Agent Traffic encrypted over TLS 1.2 or TLS 1.3.
- Siebel (SSSE) to Exchange encrypted over TLS 1.2 or TLS 1.3.
- Siebel EAI JDB via TLS 1.2 or TLS 1.3.
- Siebel WebLogic Integrations (Such as BIP) over TLS 1.2 or TLS 1.3.

Application Interface HTTPS Traffic Using TLS 1.2 or TLS 1.3

Application Interface fully supports TLS 1.2 and TLS 1.3 encryption for client-side connections, including reverse proxy configuration. TLS configuration, including application interface and Web client encryption, for this part of the product is detailed in *Communications and Data Encryption*.

Application Interface always uses TLS to communicate with Siebel Gateway.

LDAPS (Encrypted) Over TLS 1.2

The LDAP service is usually hosted behind a secure firewall. Customers using Oracle LDAP client can encrypt traffic using TLS 1.2. This may require the latest patches of the Oracle Database Client certified for the product. Make sure that the latest security patches are installed for proper functionality.

Inbound EAI/Web Services Over HTTPS Encrypted Over TLS 1.2 or TLS 1.3

Siebel supports EAI inbound on all platforms using the native support for TLS 1.2 and the support of the Web Server.

Outbound EAI/Web Services Over HTTPS Encrypted Over TLS 1.2 or TLS 1.3

TLS 1.2 and TLS 1.3 are supported on all platforms. It is recommended that you host this service behind a secure firewall. *Communications and Data Encryption* describes how to configure TLS and components for secure communications.

The flow of message security protocols is:

Windows/Non-Windows(All platforms): **Siebel Object Manager (HTTP) →Config Agent Tomcat (HTTPS) →External Application**.

Siebel Message Queueing Support and JMS Over TLS 1.2 or TLS 1.3

You can encrypt this service using TLS 1.2. It is recommended that you host this service behind a secure firewall. *Communications and Data Encryption* describes how to configure TLS and components for secure communications. For encryption information, see *Configuring TLS Encryption for Siebel Enterprise or Siebel Server*.

Siebel EAI JDB via TLS 1.2 or TLS 1.3

Application Interface server communications always use TLS 1.2 or TLS 1.3 (if configured). Siebel EAI services via JDB standalone connect also use TLS 1.2 or TLS 1.3.

Siebel Management Server/Agent Traffic Encrypted Over TLS 1.2 or TLS 1.3

Communications and Data Encryption describes how to configure TLS and components for secure communications.

Email Response/IMAP/POP/SMTP Over TLS 1.2 or TLS 1.3

You can encrypt this service to varying degrees depending on technology. IMAP/POP3/SMTP can support TLS 1.2 or TLS 1.3. For information about TLS configuration for this part of the product and about email response and encryption, see *Siebel Email Administration Guide* . OpenSSL is an option for TLS 1.2 or TLS 1.3 connections with POP3. You can enable this by using the EnableOpenSSL parameter on the Mail component. OpenSSL v1.0 does support the "DHE-RSA-AES256-SHA" cipher. Use of IMAP with TLS 1.2 or TLS 1.3 requires the use of JavaMail 1.6.3 or higher.

Siebel WebLogic Integration (such as BIP)

You must enable TLS 1.2 or TLS 1.3 for WebLogic as follows:

- Log in to the WebLogic console.
- Click <Domain>, Environment, Servers, <Server>.
- Under Configuration and General, make sure the SSL Listen Port Enabled check box is selected.
- Go to the SSL tab, click Advanced, and make sure that the Use JSSE SSL check box is selected.

  Restart WebLogic for the changes to take effect.

Java Secure Socket Extension (JSSE) enablement sets WebLogic to use the TLS features of Java instead of its own SSL implementation. (WebLogic's internal SSL implementation is not compatible with the current TLS implementations in

modern browsers.) WebLogic 12.2.1.0.0 uses JSSE by default and does not have check boxes anymore to switch back to its own version of SSL. To force TLS 1.2 or TLS 1.3, set `weblogic.security.SSL.protocolVersion=TLSv1.2` in the WebLogic startup parameter in setDomainEnv.sh. This will reject any client that does not support TLS 1.2 or TLS 1.3.

Note: BI Publisher does not control TLS. BIP runs on WebLogic and depends on WebLogic's TLS/SSL environment.

SHA-2 and SHA-3 Support

Siebel implements SHA functions in a variety of use cases. The secure hashing algorithm supported is based on the certificate type implemented and the support level provided by Siebel. The level of support for SHA-2 and SHA-3 (including SHA-256, SHA-384, and SHA-512) is as follows:

- SHA-2 and SHA-3 (limited by third party used)
  - Web server to Web Client
  - MQ and JMS
- SHA-2
  - EAI SOAP Web services
  - EAI HTTP Transport business service
  - Email response IMAP/POP (OpenSSL can be used)
  - Oracle LDAP Client (may require the latest database clients)

About 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. In particular, note the following about Siebel Open UI:

- Siebel Open UI uses an open architecture that allows you to run Siebel CRM 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.
- The Siebel Open UI client is compatible with many 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, 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*.

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 the Tree navigation control option to access screens and views. However, you can choose to use the Tree navigation control if required. For more information about setting navigation options, see *Siebel Fundamentals Guide* .

Roadmap for Configuring Security

This topic provides a general overview of tasks you can perform to take advantage of security resources for Siebel CRM. 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 CRM. 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* .

To configure security, perform the following tasks:

1. During Siebel CRM installation, plan your Siebel Server and port usage for firewall access.

   For guidelines on implementing firewalls and port usage, see *Siebel Security Hardening*.
2. After you install Siebel CRM, change the passwords for Siebel accounts regularly.

   For more information, see *Changing and Managing Passwords*.
3. Make sure communications and important data is encrypted. See *Communications and Data Encryption*.
4. Implement security adapter authentication or Web Single Sign-On to validate users. For more information, see *Security Adapter Authentication* and *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 *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* 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*.

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

3 Changing and Managing Passwords

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*
- *About Default Accounts*
- *Changing Siebel Administrator Account Password*
- *Changing the Table Owner Password*
- *Troubleshooting Password Changes By Checking for Failed Server Tasks*
- *About Siebel Gateway Authentication Password*
- *Encrypted Passwords in Siebel Application Interface Profile Configuration*
- *Changing Encrypted Passwords Using the Siebel Management Console*
- *About Encryption of Siebel Gateway Password Parameters*
- *About the Object Manager's First Connection and LDAP User*

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*. For additional information on implementing password management policies, see *Defining Password Management Procedures*.

> **Note:** Use the Siebel Management Console installed with Siebel Business Applications to perform the initial configuration of Siebel Gateway, 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 Siebel Management Console 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) authentication, the underlying security mechanism must allow this functionality. See also *Requirements for the LDAP Directory*.

      In addition, the Propagate Change parameter must be TRUE for the LDAP security adapter. The default value is TRUE. For Siebel Developer Web Clients, the system preference, SecThickClientExtAuthent, must also be TRUE.
    - For an environment using database authentication, the Database Security Adapter Propagate Change parameter must be TRUE for the database security adapter. The default value is FALSE.

  For more information, see *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*.

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 (maximum length is 18 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 (#).

Unsupported Characters

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

Note: The LDAP security adapter used with Siebel Business Applications allows special characters in passwords, including characters not supported in Siebel passwords.

Character	Description	Hexadecimal
!	Exclamation point	21
"	Double quote	22
$	Dollar sign	24
%	Percent sign	25
&	Ampersand	26
'	Single quote	27
(	Open parenthesis	28
)	Close 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

Character	Description	Hexadecimal
=	Equal sign	3D
>	Greater-than sign	3E
?	Question mark	3F
@	At-sign	40
[	Open bracket	5B
\	Back slash	5C
]	Close bracket	5D
^	Caret	5E
_	Underscore	5F
`	Grave accent	60
{	Open brace	7B
|	Vertical bar	7C
}	Close 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 a non-DB2 database platform, 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 information on changing and managing the passwords for the SADMIN and database table owner accounts, see the following topics:

- *Changing Siebel Administrator Account Password on UNIX*
- *Changing Siebel Administrator Account Password on Windows*
- *Changing the Table Owner Password*
- *Troubleshooting Password Changes By Checking for Failed Server Tasks*

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

Note: A prerequisite to configuring and using DB2390 is that you must manually copy the db2jcc_license_cisuz.jar file (which is a DB2390-specific license jar file) from your DB2 client location to the following location: applicationcontainer_external/webapps/siebel/web-inf. You must also be licensed to use DB2390 and arrange a license for same. All other client drivers are licensed and packaged in the Siebel product.

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 Siebel/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 Siebel Application Interface profile (recommended) or by editing the Siebel Application Interface profile manually:

- **Anonymous User Name.** Set this parameter to the user ID of the anonymous user, for example, GUESTCST.
- **Anonymous User Password.** Set this parameter to the password associated with the anonymous user.

  The anonymous user password is written to the Siebel Application Interface profile in encrypted form by default if you add or change this value using the Siebel Management Console.

For more information on defining the anonymous user when you configure the Siebel Application Interface profile, see *Configuring the Anonymous User*, *Authentication Parameters in Siebel Application Interface Profile* and *Siebel Installation Guide* .

Changing Siebel Administrator Account Password

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 Siebel administrator account cannot be the same as the user name of the account. The password for the Siebel administration account must not exceed 18 characters - for more information, see *Characters Supported in Siebel Passwords*.

Note: It is strongly recommended not to change the name of the Siebel administrator account, SADMIN. This account must be created so that you can log in to Siebel applications as Siebel administrator. For more information about setting up the Siebel administrator account (SADMIN) for initial use, see *Siebel Installation Guide* .

Changing Siebel Administrator Account Password on UNIX

To increase the security of your Siebel implementation, it is recommended that you change the Siebel administrator account (SADMIN) password at regular intervals. For more information about setting up this account for initial use, see *Siebel Installation Guide* .

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

To change the Siebel administrator account (SADMIN) password on UNIX

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

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

   You must run this command on all Siebel Server computers to stop all servers in the Siebel Enterprise.
2. Use Server Manager to change the SADMIN password as follows:
   a. Log in at the Enterprise level:

      ```
      srvrmgr -g SiebelGatewayHostName:TLS_Port# -e EnterpriseServerName -u UserName -p Password
      ```

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

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

   If using this SADMIN user and password on another profile, such as the Application Interface or Migration profiles, then it will be revised for those profiles as well.
3. Change the password for SADMIN in the database. For more information, refer to your RDBMS documentation on changing passwords.

4. On each Siebel Server in your Siebel Enterprise, rename the existing Siebel Server system service (svc file) and then recreate the Siebel service with the new administrator database account password (SADMIN) as follows:

   > **CAUTION:** Do not edit the svc file manually as 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. Do not store the backup copy of the svc file in the same directory as the original file as this may interfere with normal server startup.

   a. To rename the existing Siebel service file, navigate to the `$siebsrvr/sys` directory and rename the file. To avoid issues when starting up the environment, store the renamed svc file in a different location to `$siebsrvr/sys`. The Siebel service file name is in a format similar to the following, where `siebsrvrname` is the name of the Siebel Server:

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

   b. To recreate the Siebel service file with the new SADMIN password, run the following command in the `$siebsrvr/bin` directory:

      ```
      siebctl -r "SIEBSRVR_ROOT" -S siebsrvr -i EnterpriseName:SiebelServerName -a -g "-g
       GatewayServerHostName:TLS_Port# -e EnterpriseName -s SiebelServerName -u sadmin" -e NewPassword -
      L ENU
      ```

      where:

      - `"SIEBSRVR_ROOT"` is the installation directory of the Siebel Server
      - `EnterpriseName` is the name of your Siebel Enterprise
      - `SiebelServerName` is the name of the Siebel Server
      - `GatewayServerHostname` is the name of the Siebel Gateway host
      - `TLS_Port#` is the port number of the Siebel Gateway
      - `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/ses/siebsrvr" -S siebsrvr -i ENTP_TRN:SIEBSRV2 -a -g "-g GTWNOVA04:2020 -
      e ENTP_TRN -s SIEBSRV2 -u sadmin" -e sadmin1 -L ENU
      ```

      The siebctl utility re-creates the Siebel service file (svc file) with the new encrypted password value. Make sure the Siebel service file is created without any errors.

5. Restart Siebel Gateway and Siebel Server system service (the application container for the Cloud Gateway should be running as well).

   - To stop and restart Siebel Gateway:

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

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

- To start the Siebel Server system service:
  i. On the Siebel Server, log in as the Siebel Service owner user.
  ii. Run the siebenv.sh or siebenv.csh script to set Siebel environment variables.
  iii. Run the ps command and check whether the application container for the Siebel Server is running. Start it if necessary.
  iv. Enter the following command, where siebel_server_name is the name of the Siebel Server:

```
start_server siebel_server_name
```

For further information on administering the Siebel Server system service on UNIX, see *Siebel System Administration Guide* .

6. Connect to the Server Manager (srvmgr) with the new password to verify the password change:

```
srvrmgr -g SiebelGatewayHostName:TLS_Port# -e EnterpriseServerName -s SiebelServerName -u SADMIN -p
 NewPassword
```

7. If Step 6 is successful, start Siebel Server. To restart all Siebel Servers:

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

> **Note:** The remaining steps in this procedure apply to Siebel CRM 17.x Update and later releases.

8. Update the AuthToken value in the applicationinterface.properties file as follows:
   a. Run the following command in any linux box:

```
echo -n 'sadmin:<newsadminpassword>' | base64
```

   Alternatively, use the online base64 encoding tool (*https://www.base64encode.org/*) to encode `'sadmin:<newsadminpassword>'`.
   b. Copy the output string. For example:

```
$AI/jre/bin/java -jar/siebel/sai/applicationcontainer/webapps/siebel/WEB-INF/lib/EncryptString.jar
$token
```

> **Note:** Even though you will still be able to access the application and srvrmgr if you do not update the AuthToken value, the SADMIN account will be locked out if the SADMIN profile at the database level is set with an *invalid password login attempt limit*.

9. Copy the output string from step 8 and update the encrypted string output in `$SAI/applicationcontainer/webapps/applicationinterface.properties`.
   Copy the value to all Application Interface nodes, for AuthToken Value, and restart all nodes.
10. Update the migration profile in Siebel Management Console if you are using SADMIN credentials in the migration profile:
    a. Undeploy the Application Interface and migration profile in Siebel Management Console.
    b. Stop the Application Interface container (tomcat).
    c. Remove the value set to the AuthToken parameter in the migration.properties file.
    d. Remove the value set to the MigrationProfile parameter in the migration.properties file.
    e. Start the Application Interface container and verify that the SADMIN password is not locked
    f. Log in to Siebel Management Console and redeploy the Application Interface Profile.

g. Restart the Application Interface container and check that the SADMIN password is not locked.
h. Log in to Siebel Management Console and redeploy the migration profile.
i. Restart the Application Interface container and check that the SADMIN password is not locked.

11. Recreate the Application Interface profile.

    Note the following:

    - Since the ZK node `/Config/Profiles/SWSM/<name>` will have the previous password hard coded as a base64 string, this will cause an invalid login and lead to the SADMIN account being locked.
    - To prevent this from happening, replace authtoken in applicationinterface.properties and update the value of GatewayIdentity:Authtoken in zookeeper with the modified password.
    - Either generate a new value (`echo 'SADMIN:<SADMINPASSWORD>' | base64`) and use zkui to manually update the `/Config/Profiles/SWSM/<name>` OR delete and recreate the `swsm/AI` profile using Siebel Management Console.

12. To validate application access, log in to Siebel as SADMIN (with the new Siebel administrator account password) and verify the password change.

> **Note:** Depending on how your Siebel administrator account (SADMIN) is configured, you may be locked out of your SADMIN account if you exceed a specified number of failed login attempts.

Changing Siebel Administrator Account Password on Windows

To increase the security of your Siebel implementation, it is recommended that you change the Siebel administrator account (SADMIN) 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 - see *Changing the Password for the Siebel Service Owner Account* . For more information about setting up these accounts for initial use, see *Siebel Installation Guide* .

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

To change the Siebel administrator account (SADMIN) password on Windows

1. End all client sessions and shut down Siebel Servers, for example, as follows:

    a. Go to Control Panel and double-click Computer Management.
    b. Expand Services and Applications in the Computer Management panel that appears, and then click Services.
    c. Right-click the Siebel Server system service that you want in the details panel, and then click Stop.

    Windows stops the Siebel Server system service. This operation might take a few seconds. Repeat these steps as required to stop all servers in the Siebel Enterprise.

2. Use Server Manager to change the SADMIN password as follows:

   a. Log in at the Enterprise level:

      ```
      srvrmgr -g SiebelGatewayHostName:TLS_Port# -e EnterpriseServerName -u UserName -p Password
      ```

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

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

   If using this SADMIN user and password on another profile, such as the Application Interface or Migration profiles, then it will be revised for those profiles as well.
3. Change the password for SADMIN 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 (svc file) and then re-create the Siebel service with the new administrator database account password (SADMIN) as follows:

   a. To delete the existing Siebel service file, go to `$ses\siesrvr\bin>` at the command prompt and enter the following command:

   ```
   siebctl -d -S siebsrvr -i "<SiebelServiceFileName>"
   ```

   For example:

   ```
   siebctl -d -S siebsrvr -i "ses_app01"
   ```

   b. To recreate the Siebel service file with the new SADMIN password, go to `siebsrvr\bin` and enter the following command:

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

   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 Siebel Gateway host
   - `TLS_Port#` is the port number of the Siebel Gateway
   - `sadmin` is the administrator user ID
   - `NewPassword` is the new Siebel administrator password in plaintext. The siebctl utility encrypts the password.
   - `NTAccount` is the Siebel service owner account name. For example: `companydomain\SADMIN`.

     It is recommended that the Siebel service owner account be part of a Windows domain (and not a local domain) so that services are operated under the same account on all the Windows servers. For more information on creating the Siebel service owner account, see *Siebel Installation Guide* .
   - `NTPassword` is the Siebel service owner account password

   For example:

   ```
   D:\ses\siebsrvr\BIN> siebctl -h "d:\siebel\ses\siebsrvr" -S siebsrvr -i "ENTP_TRN:SIEBSRV2" -a
    -g "-g GTWNOVA04:2020 -e ENTP_TRN -s SIEBSRV -u sadmin" -e sadmin1 -u companydomain\SADMIN -p
    xxxxxxxx
   ```

   The siebctl utility re-creates the Siebel service file (svc file) with the new encrypted password value. Make sure the Siebel service file is created without any errors.

5. Restart Siebel Gateway registry by starting the Siebel Gateway system service as follows (the application container for the Cloud Gateway should be running as well):

    a. Go to Control Panel and double-click Computer Management.
    b. Expand Services and Applications in the Computer Management panel that appears, and then click Services.
    c. Right-click the Siebel Gateway Name Server that you want in the details panel, and then click Start.

    Windows starts the Siebel Gateway Name Server system service. This operation might take a few seconds.
6. Connect to the Server Manager (srvmgr) with the new password to verify the password change:

```
srvrmgr -g SiebelGatewayHostName:TLS_Port# -e EnterpriseServerName -s SiebelServerName -u SADMIN -p
 NewPassword
```

7. If Step 6 is successful, start the Siebel Server system service:

    a. Go to Control Panel and double-click Computer Management.
    b. Expand Services and Applications in the Computer Management panel that appears, and then click Services.
    c. Right-click the Siebel Server system service that you want in the details panel (the enterprise name and Siebel Server name are indicated within brackets), and then click Start.

    Windows starts the Siebel Server system service. This operation might take a few seconds.

    For further information on administering the Siebel Server system service on Windows, see *Siebel System Administration Guide* .
8. Update the AuthToken value in the applicationinterface.properties file as follows:

    a. Run the following command (certutil is required):

```
certutil -encode pw.txt encoded.txt
```

    b. Copy the output string. For example:

```
$AI/jre/bin/java -jar/siebel/sai/applicationcontainer/webapps/siebel/WEB-INF/lib/EncryptString.jar
$token
```

> **Note:** Even though you will still be able to access the application and srvrmgr if you do not update the AuthToken value, the SADMIN account will be locked out if the SADMIN profile at the database level is set with an *invalid password login attempt limit*.

9. Copy the output string from step 8 and update the encrypted string output in `$SAI/applicationcontainer/webapps/applicationinterface.properties`.

    Copy the value to all Application Interface nodes, for AuthToken Value, and restart all nodes.

10. Update the migration profile in Siebel Management Console if you are using SADMIN credentials in the migration profile:
    a. Undeploy the Application Interface and migration profile in Siebel Management Console.
    b. Stop the Application Interface container (tomcat).
    c. Remove the value set to the AuthToken parameter in the migration.properties file.
    d. Remove the value set to the MigrationProfile parameter in the migration.properties file.
    e. Start the Application Interface container and verify that the SADMIN password is not locked
    f. Log in to Siebel Management Console and redeploy the Application Interface Profile.
    g. Restart the Application Interface container and check that the SADMIN password is not locked.
    h. Log in to Siebel Management Console and redeploy the migration profile.
    i. Restart the Application Interface container and check that the SADMIN password is not locked.
11. Recreate the Application Interface profile.

    Note the following:
    - Since the ZK node `/Config/Profiles/SWSM/<name>` will have the previous password hard coded as a base64 string, this will cause an invalid login and lead to the SADMIN account being locked.
    - To prevent this from happening, replace authtoken in applicationinterface.properties and update the value of GatewayIdentity:Authtoken in zookeeper with the modified password.
    - Either generate a new value (`echo 'SADMIN:<SADMINPASSWORD>' | base64`) and use zkui to manually update the `/Config/Profiles/SWSM/<name>` OR delete and recreate the `swsm/AI` profile using Siebel Management Console.
12. To validate application access, log in to Siebel as SADMIN (with the new Siebel administrator account password) and verify the password change.

> **Note:** Depending on how your Siebel administrator account (SADMIN) is configured, you may be locked out of your SADMIN account if you exceed a specified number of failed login attempts.

Changing the Password for the Siebel Service Owner Account

Use the following procedure to modify the password for the Siebel service owner account; 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 account 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 earlier in this procedure.

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

Changing the Anonymous User Password When a User Account is set to Anonymous User

The information in this topic applies to Microsoft Windows and UNIX.

If you set a Siebel user account, such as GUESTCST, with minimum responsibilities (for example, access to the login view) to Anonymous User Name, then you must also change the password (Anonymous User Password) associated with the anonymous user in the Siebel Application Interface profile. For more information, see *Changing Encrypted Passwords Using the Siebel Management Console*

> **CAUTION:** Never use the system administrator account (SADMIN) as the anonymous user account (Anonymous User Name) in a production environment. It is only acceptable to do so for development or test environments.

For more information about the anonymous user, see *Configuring the Anonymous User*.

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 (non-DB2). For information on creating the table owner account, see the *Siebel Installation Guide* . 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 (see *Parameters for Configuring Security Adapter Authentication*) 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 (example 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 Siebel Gateway Authentication Password

To make sure that only authorized users can make changes to the enterprise configuration parameters on Siebel Gateway, users connecting to the gateway must supply a valid authentication user name and password. Authentication user name and password values are verified by the security adapter specified for Siebel Gateway. The security adapter can be one of the following: database, LDAP, or custom.

The user account you use for Siebel Gateway 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.

You can choose to use the Siebel administrator account for Siebel Gateway 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 an LDAP or a custom security adapter, then you must also add the gateway authentication user name and password to the directory server.

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

Using Siebel Utilities to Access Siebel Gateway

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

You can pass the gateway 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.

Encrypted Passwords in Siebel Application Interface Profile Configuration

The AES algorithm encrypts passwords stored in the Siebel Application Interface profile with a 256-bit encryption key. Passwords are written in encrypted form when you configure the Siebel Application Interface profile. Values for the following parameters are subject to encryption in the Siebel Application Interface profile:

- Anonymous User Password
- Trust Token

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 Anonymous User Name 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 Siebel Application Interface profile. If you change the password for this account after setting up your system, then you must update the password stored in the Siebel Application Interface profile. For information about changing encrypted passwords, see *Changing Encrypted Passwords Using the Siebel Management Console*.

Changing Encrypted Passwords Using the Siebel Management Console

Using the Siebel Management Console to change an anonymous user password automatically saves the password in encrypted form.

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 Siebel Application Interface profile.

> **Note:** If you want to use different database accounts for the anonymous user for different applications, then you must manually update the Siebel Application Interface profile.

The following procedure describes how to change an encrypted password using the Siebel Management Console.

To change encrypted passwords using the Siebel Management Console

1. Log in to the Siebel Management Console.
2. Click Profiles in the navigation menu, and then click Application Interface.
   Existing application interface profiles are listed, if any.
3. Select the application interface profile that you want to modify, and then click Edit.

4. Go to the Basic Information section, click Authentication and change the Anonymous User Password.
5. To change the anonymous password specific to other applications (such as Siebel Call Center, EAI, or REST API), then do the following:

    a. Go to the Applications section, and select the check box next to the application you want to modify.
    b. Click Authentication, and change the Anonymous User Password as required.

About Encryption of Siebel Gateway Password Parameters

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

> **Note:** End user passwords aren't specified as parameter values for the gateway and aren't stored in the Siebel Gateway registry.

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

If you want, you can increase the encryption key length for encrypting passwords. If you do increase the encryption key length for encrypted passwords in the Siebel Gateway registry, then the passwords need to be encrypted again using the new key.

Upgrading to Siebel CRM

You must reset any passwords on the Siebel Gateway that were previously encrypted using RC4 encryption. In the current release, such passwords are encrypted using AES instead of RC4.

Furthermore, the Siebel Server system service and server components don't work after a migration installation until you have updated them to use AES password encryption. Make these changes in coordination, as described in *Siebel Installation Guide* .

> **Note:** When you upgrade to the current release, the Siebel Server system service password, which is required to connect the Siebel Server to the Siebel Gateway, is automatically reencrypted using AES encryption. The Siebel Gateway password parameter, which is set at the Siebel Enterprise level, is also automatically reencrypted. You don't have to reencrypt these passwords manually.

Determining Encrypted Parameters and Values in Siebel Gateway Registry

Passwords in the Siebel Gateway registry are encrypted using 128-bit AES encryption. If you have many components in your system and you want to obtain a list of the encrypted passwords including the encryption value for each password, then complete the following procedure.

> **Note:** This procedure assumes that Siebel Application Object Managers have been created for the components in your system.

Determine Encrypted Parameters and Values

Here's how to determine the encrypted parameters and values in Siebel Gateway registry:

1. Obtain the list of components and component types in your system.
2. For each component type, list the parameters for the component using the following srvrmgr commands:

   ```
   list params . . .
   list advanced params . . .
   list hidden params . . .
   ```

   In the list of parameters returned, the encrypted parameters and their associated values are preceded with an asterisk (*) symbol.
3. Re-encrypt the parameter values using srvrmgr if required.

About the Object Manager's First Connection and LDAP User

When using LDAP or LDAP with SSO and the Siebel Server is started, the Object Manager's first connection to load Runtime Repository (RR) tables will use the SADMIN Username/Password credentials (which are typically inherited from the Siebel Enterprise level setting). Customers that do not have an SADMIN user created in the LDAP server will, as a result, face performance issues because the RR tables cannot be loaded. In such cases, it is recommended that you do the following:

- Set new Username/Password parameters at the object manager component level, for another user.
- In the LDAP server, create the Username with Password defined (it does not have to be a Siebel application user).

4 Communications and Data Encryption

Communications and Data Encryption

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

- *Types of Encryption*
- *About Certificates and Key Files Used for TLS Authentication*
- *Process of Configuring Secure Communications*
- *Installing Certificate Files*
- *Configuring TLS Mutual Authentication for SHA-2 Certificates Using EAI HTTP Transport*
- *About Configuring Encryption for Siebel Enterprise and Siebel Application Interface*
- *About Key Exchange for TLS Encryption*
- *Configuring TLS Encryption for Siebel Enterprise or Siebel Server*
- *Configuring TLS Encryption for Siebel Application Interface*
- *Enabling SSL Acceleration for Application Interface/Enabling HTTP*
- *About Configuring Encryption for Web Clients*
- *Configuring Encryption for Mobile Web Client Synchronization*
- *Data Encryption*
- *Siebel Encryption*
- *Configuring Encryption and Search on Encrypted Data*
- *Encrypting Columns in a Business Component*
- *Managing the Key File Using the Key Database Manager*
- *Security Considerations for Unicode Support*
- *About Encoding UI Values*

Note: Application Interface server communications always use TLS 1.2 and Siebel EAI services via JDB standalone connect also use TLS 1.2.

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*

- *Certificate Requirements for Communications*
- *About Generating Server Keystore, Client Keystore and Truststore Files*
- *Modifying Server Keystore, Client Keystore and Truststore Files*
- *About Importing Certificates into Keystore and Truststore*
- *Disabling Certificate Based Mutual Authentication*

- *Data Encryption*

Communications Encryption

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

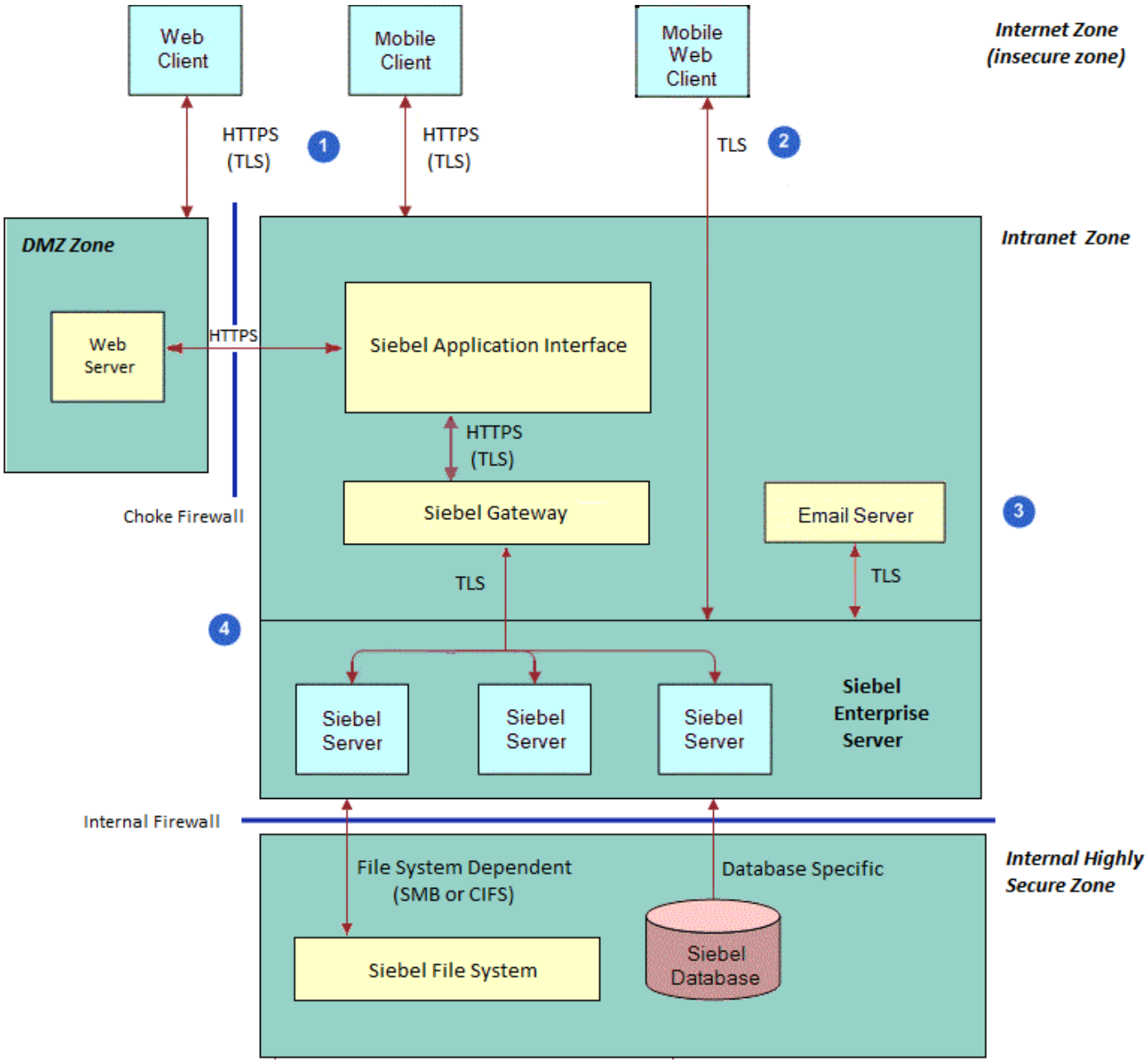
- **TLS encryption for Web client connections.** For data security over the Internet, Siebel Business Applications support the use of the Transport Layer Security (TLS) capabilities of supported Web servers to secure transmission of data between the Web browser and the Web server. The use of TLS for 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 or simply handle login requests under HTTPS. For more information, see *About the Siebel Web Client and Using HTTPS* and *Implementing Secure Login*.
- **Encryption for Siebel component connections (TLS).** Siebel administrators can enable encryption for communications between Siebel components. The Siebel communications protocol provides a security and compression mechanism for network communications based on TLS.

  By default, encryption based on TLS uses the AES algorithm with 256-bit encryption keys.

  TLS also supports certificate authentication between the Web server and the Siebel Server, or between Siebel Servers.
- **TLS encryption for connections to directory servers.** TLS encryption is supported for connections to certified LDAP directories.
- **TLS encryption for connections to email servers.** TLS encryption is supported for connections to email servers using Siebel Communications Server components. TLS encryption is supported for connections to Microsoft Exchange Server 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.

The following image shows some of the types of communications encryption available for Siebel Business Applications environment.



The encryption mechanisms illustrated in this image are as follows:

1. **Web client and mobile client connections.** TLS is used to secure transmission of data between the Web browser and the Web server in the DMZ.

   A reverse proxy should always be used for HTTP/HTTPS traffic in the DMZ. You can use any Web server to provide reverse proxy functionality and also any Siebel compatible SSO Web server plug-in on that Web server, provided the plug-in is supported by the Web server platform. Siebel Application Interface is expected to be

hosted inside a firewall. You can use any Web server to configure this. For more information on reverse proxies in the DMZ, consult your web server vendor documentation.

2. **Siebel Mobile Web Client connections.** You can use TLS encryption for Mobile Web Client communications with the Siebel Remote server.
3. **Email server connections.** TLS encryption for connections to email servers is supported.
4. **Siebel component connections.** Communications between Siebel components are based on TLS algorithms.

Certificate Requirements for Communications

Siebel installer for Siebel Business Applications enforces HTTPS during installation, as follows:

- Siebel Web Clients, Siebel Management Console and the Siebel Migration server all communicate with the Siebel Application Interface over HTTPS.
- All communication between Siebel services (Siebel Application Interface, Siebel Gateway, and Siebel Configuration Agent) are enforced over HTTPS by Siebel installer.
- Siebel Application Interface is an external interface accessing Siebel services. All other Siebel services are internal services and they are protected by client certificate based authentication.
- Any Siebel service-to-service access is over HTTPS with client certificate based authentication (for example, two-way SSL). Client certificates are used for service-to-service authentication.

The following figure illustrates the certificate requirements for communications as follows:

- Siebel Application Interface, Siebel Gateway, and Siebel Configuration Agent are hosted in application containers (Apache Tomcat).

  For information on configuring application containers, see *Siebel Installation Guide* . For information on starting and stopping application containers, see *Siebel System Administration Guide* .

- During Siebel installation (of the aforementioned components), the installer prompts you to specify valid Server Keystore, Client Keystore and truststore files, as follows:

  - **Server Keystore Name.** Specify a file (such as a JKS file) you have generated that will serve as the server keystore. Import the server authentication (serverAuth) certificate (and its private key/certificate chain) into this keystore using the Java Keytool utility. Use this keystore for Siebel server endpoints (for example, Tomcat connectors for External and Internal Application Interface and the Siebel Gateway TLS server configuration).
  - **Client Keystore Name.** Specify a file (such as a JKS file) you have generated that will serve as the client keystore. Import the client authentication (clientAuth) certificate (and its private key/certificate chain) into this keystore using the Java Keytool utility. Use this keystore for mutual TLS (mTLS) client certificate based authentication for Siebel service-to-service communication and for Java clients making HTTPS calls.

    > **Note:** Publicly trusted TLS/SSL certificates issued after the CA deadlines may not include the Client Authentication EKU and therefore cannot be used as mTLS client certificates. Use an internal/private CA (enterprise PKI) for the client keystore where client authentication is required.

- **Truststore Name.** Specify a file (such as a JKS file) you have generated that will serve as the truststore. For example, import the Certificate Authority (CA) certificate into truststore using the Java Keytool utility.

  The two scenarios during Siebel Update with respect to certificate selection are as follows:

  - Scenario #1: Updating pre-26.3 environment to 26.3 but still have old (both serverAuth and clientAuth EKU) combined hybrid certificates. No action required. It will continue to work till certificate expiry.

    > **Note:** If you are installing a fresh 26.3 environment but still using combined certificates (both serverAuth and clientAuth EKU). Specify the same keystore for both serverAuth and clientAuth during installation.

  - Scenario #2: Updating pre-26.3 environment to 26.3 but have separate certificates. Manually change the serverkeystore and clientkeystore details.

    > **Note:** If you are installing a fresh 26.3 environment with separate certificates. Follow the prompts and specify the correct keystores.

    - Changes required in `applicationcontainer_internal` and `applicationcontainer_external .. \conf\server.xml`:

      ```
      <Connector ...>
       <SSLHostConfig>
       <Certificate
       certificateKeystoreFile="z:\siebel\applicationcontainer_external\certs
      \siebelserverkeystore.jks"
       certificateKeystorePassword="siebel"
       certificateKeystoreType="JKS"
       />
       </SSLHostConfig>
      </Connector>
      ```

    - Changes required in `applicationcontainer_internal\webaps\gateway.properties`:

      ```
      KeyStoreType=JKS
      KeyStoreName=Z:\\siebel\\applicationcontainer_internal\\siebelcerts\
      \siebelclientkeystore.jks
      KeyStorePassword=<<value>>

      ServerKeyStoreType=JKS
      ServerKeyStoreName=Z:\\siebel\\applicationcontainer_internal\\siebelcerts\
      \siebelserverkeystore.jks
      ServerKeyStorePassword=<<value>>
      ```

    - Changes required in `applicationcontainer_external\webaps \applicationinterface.properties` and `applicationcontainer_external\webaps \migration.properties` files:

      ```
      KeyStoreType=JKS
      KeyStoreName=Z:\\siebel\\applicationcontainer_external\\siebelcerts\
      \siebelclientkeystore.jks
      KeyStorePassword=<<value>>
      ```

Since Siebel internal nodes are configured for client certificate based authentication, make sure that you use the correct client identity in the CN and Subject Alternate Name (SAN) fields. You can create certificates with the exact FQDN or IP address, or with a wildcard in the FQDN. For example, if you replace

`host.domain.subdomain.com` with `*.domain.subdomain.com`, then this eliminates the need to create separate client certificates for each machine.

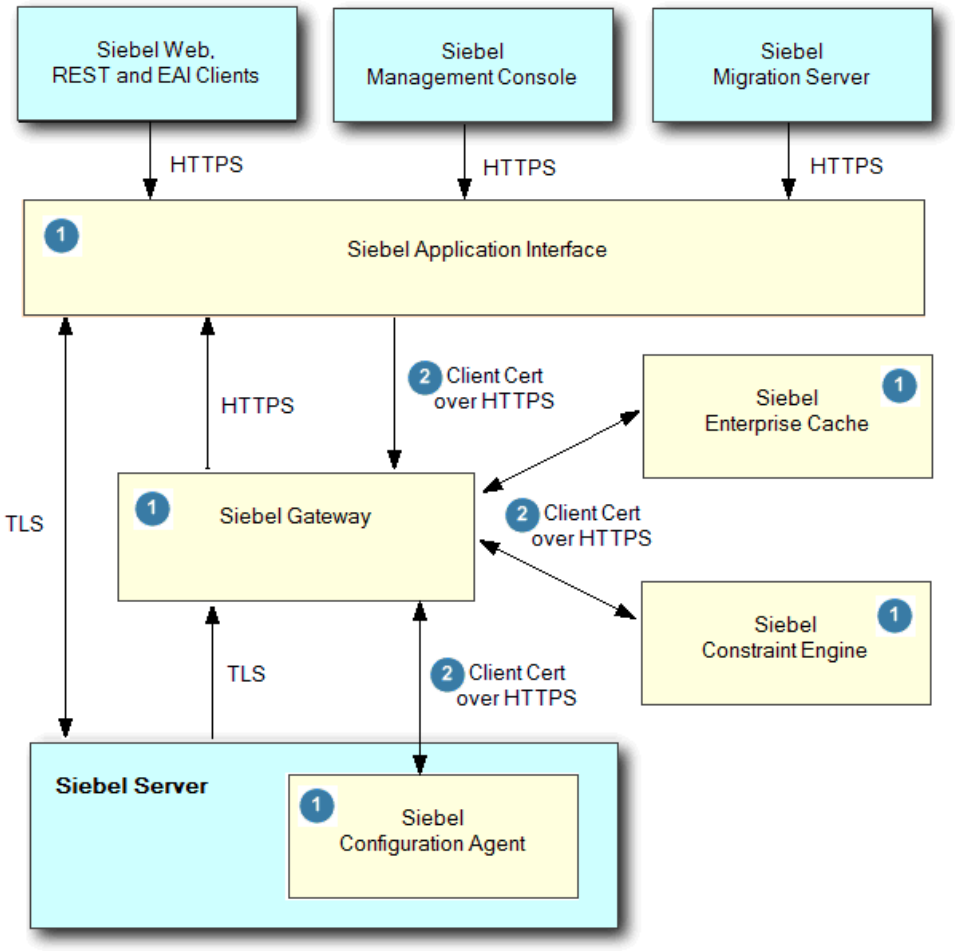
> **Note:** It is recommended that you use certificates provided by a Certificate Authority (CA) rather than self-signed certificates for server certificates and use internal CA signed or self signed certificates for client certificates used for mTLS. For production environments, you must create a certificate request and get it signed either by your internal CA (for employee-only environments) or an external CA (for customer, consumer, or partner environments). Self-signed certificates are suitable for development environments, for example, where you can provide instructions to users to import the self-signed certificate, since clients will not trust such a certificate unless it is manually installed into the certificate store.

For more information, see *About Generating Server Keystore, Client Keystore and Truststore Files* and *Modifying Server Keystore, Client Keystore and Truststore Files*.

- **Password.** Specify the password for the specified keystore and truststore files.
- **Confirm Password.** Confirm the password for the specified keystore and truststore files.

> **Note:** The Siebel Gateway requires that client connections from the Siebel Application Interface be authenticated using a client certificate (mutual authentication). As such, the SSL certificate on the Application Interface must have two certificates, client certificate for client authentication and server certificate for server authentication.. When requesting the certificate, ensure that it will include `"clientAuth"` for client certificate and `"serverAuth"` for server certificate Extended Key Usage Attributes. These are typically included in certificates issued by commercial Certificate Authorities, but may or may not be included by default in certificates issued by an internal CA.

For more information about certificate files, see *About Importing Certificates into Keystore and Truststore* and *Installing Certificate Files*.



About Generating Keystore and Truststore Files

The Server Keystore, Client Keystore and truststore files are JKS files containing certificates. These files are necessary for the application container to be able to use secure two-way communications when connecting with other Siebel modules, as occurs during Siebel Management Console configuration and in normal operation.

> **Note:** Siebel supports only JKS storetype. It is expected to explicitly pass store type while creating JKS file using keytool using the option "-storetype JKS".

Important points about generating the Server Keystore, Client Keystore and truststore files:

- The Server Keystore and Client Keystore files must contain the server certificate chain and an imported CA certificate.
- Generate your files so that the keystore file references both the private key and the public key, while the truststore file references the public key only.
- Generate your certificates using the Java Runtime Environment (JRE) provided with your release.
- Specify the password that was previously configured to open the certificate files.

- Use the fully qualified domain names rather than IP addresses.

> **Note:** If you use IP address instead of FQDN, then certificates must be created with both FQDN and IP address as two separate SAN entries and in such cases, the Siebel Server fails. As a result, it is recommended that you use the FQDN rather than IP address.

If you do not configure the Server Keystore, Client Keystore and truststore files correctly, then you will not be able to configure the Siebel Business Applications, as described in *Configuring Security Adapters Using the Siebel Management Console*, *Authentication Related Configuration Parameters* and *Siebel Installation Guide* .

Modifying Keystore and Truststore Files

In cases where it is necessary to modify the Server Keystore, Client Keystore and truststore file details, complete the steps in the following procedure.

To modify Server Keystore, Client Keystore and truststore files

1. Go to the location where the Server Keystore, Client Keystore and truststore files are stored.

   This location is specific to Siebel Application Interface, Siebel Gateway, Siebel Configuration Agent, or any other component.
2. Use the Java Keytool commands to edit the Server Keystore, Client Keystore and truststore file details as required.

   Do the following to change the details in the properties and server.xml files:

   a. Encrypt the password using the encryptstring.jar utility

   ```
   $<javahome>\bin>java - jar
   $<siebelhome>\siebel\classes\original\encryptstring.jar <<plaintext>>
   ```

   b. Go to the corresponding properties file and update the KeyStorePassword with clientkeystore password, ServerKeyStorePassword with serverkeystore password and TrustStorePassword with the encrypted value.

   You must update the encrypted password in the applicationinterface.properties file, which is located on the Siebel Application Interface in the `applicationcontainer_external\webapps` folder.

   c. Go to the corresponding server.xml file (located under `..\conf`) and update the truststorepass and keystorepass with serverkeystore password.

   - To change the password, update the truststorepass and keystorepass in the `\conf\server.xml` file for Siebel Application Interface, Siebel Gateway, and Siebel Configuration Agent.
   - Update truststorepass and keystorepass under the HTTP connector.
   - Update the plain text password here:

   ```
   $<javahome>\bin>java - jar <connector port="<https port>" ... .
   keystorepass="xxx" ... . truststorepass="xxx"/>
   ```

3. Restart the application containers for all components where you made changes. For details, see *Siebel System Administration Guide* .

Note: Alternatively, in the event where you previously installed Siebel CRM 17.0 or later using the keystore file test.jks but used incorrect domain name or hostname credentials when creating the jks file, then do the following to use the newly created certificate (provided the password is the same) without re-installing Siebel CRM:

- Copy the new JKS file (with the same password, but with different domain name and hostname) to the siebcerts folder under Siebel Application Interface, Siebel Gateway, Siebel Configuration Agent, or any other component.
- Restart the application containers. For details, see *Siebel System Administration Guide* .

About Importing Certificates into Keystore and Truststore

When you import your certificate into the keystore or truststore, you typically give it an alias (for example, `–alias server`) as follows:

```
keytool -import -trustcacerts -alias server -file your_site_name.p7b -keystore your_site_name.jks
```

Then in your server.xml file, you must declare the same alias (for example, `keyAlias="server"`) as follows:

```
<Connector port="443" maxHttpHeaderSize="8192" maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
 enableLookups="false" disableUploadTimeout="true" acceptCount="100" scheme="https" secure="true"
 SSLEnabled="true" clientAuth="false" sslProtocol="TLSv1.2" keyAlias="server" keystoreFile="/home/user_name/
your_site_name.jks" keystorePass="your_keystore_password" />
```

Disabling Certificate Based Mutual Authentication

You can disable certificate based authentication and run all components over HTTPS, however, this action is not recommended for security reasons. The following procedure shows you how to disable certificate based authentication.

To disable certificate based authentication

1. Set `certificateVerification="none"` in the `conf\server.xml` file for Siebel Gateway and Siebel Configuration Agent to disable certificate based mutual authentication.

   For example, set the HTTPS connector as follows to keep all communication over HTTPS without client certificate authentication:

```
<Connector
 port="xxxx"
 protocol="org.apache.coyote.http11.Http11NioProtocol"
 maxThreads="150"
 SSLEnabled="true"
 maxParameterCount="1000"
 scheme="https"
 secure="true"
 relaxedQueryChars="&#x20;&#x22;&#x3C;&#x3E;&#x5B;&#x5C;&#x5D;&#x5E;&#x60;&#x7B;&#x7C;&#x7D;"
 relaxedPathChars="&#x20;&#x22;&#x3C;&#x3E;&#x5B;&#x5C;&#x5D;&#x5E;&#x60;&#x7B;&#x7C;&#x7D;"
>
 <SSLHostConfig
 truststoreFile="xxxx"
 truststorePassword="xxxx"
 truststoreType="JKS"
 protocols="TLSv1.2+TLSv1.3"
 ciphers="...."
 certificateVerification="none"
 >
 <Certificate
 certificateKeystoreFile="xxxx"
 certificateKeystorePassword="xxxx"
 certificateKeystoreType="JKS"
```

```
 certificateKeyAlias="xxxx"
 />
 </SSLHostConfig>
</Connector>
```

2. Restart the application containers for all components: Siebel Application Interface, Siebel Gateway, and Siebel Configuration Agent.

   For information on starting and stopping application containers, see *Siebel System Administration Guide* .
3. Access the UI using the following address: `HTTPS://<hostname>:https_port/`.

Managing Ciphers

The following procedure shows how to manage ciphers in Siebel Application Interface for Siebel CRM.

To manage ciphers

1. In the server.xml file (located in the `ai\applicationcontainer\conf\` folder) for Siebel Application Interface, go to the following SSL/TLS Connector container attribute:

```
<Connector
 port="xxxx"
 protocol="org.apache.coyote.http11.Http11NioProtocol"
 maxThreads="150"
 SSLEnabled="true"
 maxParameterCount="1000"
 scheme="https"
 secure="true"
 relaxedQueryChars="&#x20;&#x22;&#x3C;&#x3E;&#x5B;&#x5C;&#x5D;&#x5E;&#x60;&#x7B;&#x7C;&#x7D;"
 relaxedPathChars="&#x20;&#x22;&#x3C;&#x3E;&#x5B;&#x5C;&#x5D;&#x5E;&#x60;&#x7B;&#x7C;&#x7D;"
>
 <SSLHostConfig
 truststoreFile="xxxx"
 truststorePassword="xxxx"
 truststoreType="JKS"
 protocols="TLSv1.2+TLSv1.3"
 ciphers="...."
 certificateVerification="none"
 >
 <Certificate
 certificateKeystoreFile="xxxx"
 certificateKeystorePassword="xxxx"
 certificateKeystoreType="JKS"
 certificateKeyAlias="xxxx"
 />
 </SSLHostConfig>
</Connector>
```

2. Add ciphers to this list (or remove ciphers from this list) as required.
3. Restart the application container for Siebel Application Interface.

   For information on starting and stopping application containers, see *Siebel System Administration Guide* .

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 *Data Encryption*.

  Siebel Business Applications also use AES encryption to encrypt passwords stored in the Siebel Gateway registry. The Siebel Gateway registry stores information required by the gateway. For more information about encrypted passwords in the Siebel Gateway registry, see *About Encryption of Siebel Gateway Password Parameters*.
- **SHA-2 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 SHA-2. (The previous mangle algorithm is still available for existing customers.)

  The Siebel administrator password is stored for Siebel Gateway in the Siebel Gateway registry, and is not hashed; passwords in the Siebel Gateway registry 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*.
- **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*.

About Certificates and Key Files Used for TLS Authentication

When you configure TLS authentication for a Siebel Enterprise, Siebel Server, or Siebel Application Interface, 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. 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 Enable Peer Authentication parameter 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 in the Certificate Authority (CA) Certificate File Name parameter when you configure 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 TLS, such as the Siebel Server or Siebel Application Interface. 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*.

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 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.

For TLS authentication in a Siebel Enterprise, Siebel Server, or Siebel Application Interface, Siebel Business Applications support certificates that use an encryption key size of 1024 bits by default. You can use a higher encryption key size, such as 2048 or 4096 bits, as well.

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

TLS Communication Type	Supported Key Size
TLS communications between the Siebel Server and the Web server (Siebel Application Interface), and between Siebel Servers.	1024-bit certificate keys are supported by default. Certificate key sizes larger than 1024 bits, such as 2048-bit or 4096-bit keys, are also supported.
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.
TLS communications between developer clients (including Siebel Tools) and components in the Siebel environment.	1024-bit certificate keys only are supported.

TLS Communication Type	Supported Key Size
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.
TLS communications between Siebel security adapters and external directory servers.	These connections can support larger bit sizes for certificate keys.
TLS communications for Web services.	Web services support up to 4096-bit certificate keys.

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*
- *Configuring TLS Mutual Authentication for SHA-2 Certificates Using EAI HTTP Transport*
- *Configuring TLS Encryption for Siebel Enterprise or Siebel Server*
- *Configuring TLS Encryption for Siebel Application Interface*
- *Enabling SSL Acceleration for Application Interface/Enabling HTTP*
- *Configuring Encryption for Mobile Web Client Synchronization*

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

Installing Certificate Files

This topic includes information about the following:

- *Installing Certificate Files*
- *Installing Certificate Files on Servers*
- *Installing Certificate Files on UNIX for Client Authentication*
- *Setting HTTP Proxy for UNIX Using the mwcontrol Utility*

This task is a step in *Process of Configuring Secure Communications*.

About Installing Certificate Files

The use of a trusted root CA (for example, a commercial certificate or one signed by a trusted internal corporate CA) is strongly recommended for the certificate used by Siebel components, such as the Application Interface, Siebel Server, and Siebel Gateway.

- If forced to use a self-signed certificate, then the client will need to explicitly trust the certificate. Check with your browser and operating system supplier for information on how to do this.
- When migrating data from a source (development) into another target environment (QA or production), the truststore on the source must include the CA that signed the certificate on the target. If that CA is trusted, the source also trusts any valid certificate signed by that authority.

In summary, the typical steps to obtain and install certificate files are as follows:

1. Generate a certificate signing request, for example, as follows and send the request off to a Certificate Authority (CA).

   ```
   keytool -certreq -alias siebel -keystore siebelkeystore.jks - file siebel.csr
   ```

   The following table explains these parameters:

Parameter	Example Value	Description
-certreq	NA	Indicates that you want to generate a certificate request.
-alias	Siebel	This tells keytool which key to use to generate the certificate.
-keystore	siebelkeystore.jks	The name of the keystore file (you'll be prompted to enter the same password used when the file was created).
-file	siebel.csr	The name of the file in which to put the certificate signing request.

2. As long as the CA decides that you're allowed to have a certificate, the CA will issue a certificate, sign it, and return the certificate to you.

   Note: This signed certificate, which contains information about the CA, is what will allow your browser to determine whether to trust the certificate. For example, is the certificate issued by a CA who's defined in your browser's Trust Store?

3. Import the trusted root CA into the Key Store, which is used by the web server to provide the certificate to browsers. For example:

```
keytool -import -alias a_demo_ca -file ca_root.cer -keystore siebelkeystore.jks
```

This table explains these parameters:

Parameter	Example Value	Description
-import	NA	Indicates that you want to import the signed certificate.
-alias	a_demo_ca	The name of the root certificate authority.
-file	ca_root.cer	The CA's certificate (which the CA provides).
-keystore	siebelkeystore.jks	The name of the keystore file (you'll be prompted to enter the same password used when the file was created).

4. If an intermediary CA certificate is required, import it using the same syntax as that used for importing the trusted root CA, except specify the intermediate CA's certificate. For example:

```
keytool -import -alias name_of_intermediary CA -file ca_int.cer -keystore siebelkeystore.jks
```

Note: The Certificate Authority will tell you if an intermediary certificate is required.

5. Import the signed certificate using the following syntax:

```
keytool -import -alias siebel -keystore siebelkeystore.jks -file siebel.cer
```

6. Create the Trust Store by importing the root CA into a new keystore as follows:

```
keytool -import -alias a-demo-ca -file ca_root.cer -keystore truststore.jks
```

The following table explains these parameters:

Parameter	Example Value	Description
-import	NA	Indicates that you want to import the signed certificate.
-alias	a_demo_ca	The name of the root certificate authority.
-file	ca_root.cer	The CA's certificate (which the CA provides).

Parameter	Example Value	Description
-keystore	truststore.jks	The name of the keystore file (you will be prompted to enter the same password used when the file was created).

For more information about certificate files, see the following topics:

- *Certificate Requirements for Communications*
- *About Importing Certificates into Keystore and Truststore*
- *About Certificates and Key Files Used for TLS Authentication*

Installing Certificate Files on Servers

If you're using a UNIX operating system, then see the following for information on obtaining certificate authority files and certificate files:

- **TLS Encryption for Siebel component connections.** Obtain the required certificate files and find them on a local volume; they don't have to be installed.
- **TLS encryption for connections to LDAP directories.** The LDAP security adapter uses Oracle Wallet Manager to handle the installation of certificates.
- **Communications encryption between the Siebel Server and the Database Server.** See your third-party RDBMS supplier 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 TLS protocol, you might have to install certificate files, for example, if you want to enable client authentication. For information on client authentication, see *Configuring TLS Mutual Authentication for SHA-2 Certificates Using EAI HTTP Transport*.

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 the certificate authority and certificate files required when using EAI HTTP Transport with TLS.

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. Run the mwcontrol utility on each Siebel Server and Siebel Application Interface 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, run the following command:

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

   where $SIEBSRVR_ROOT is the Siebel Server 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.
10. Configure the DockConnString parameter in the [LOCAL_SE] section of your application's configuration file as required, then save the changes and exit the file.

    > **Note:** As of Siebel CRM 20.8 Update, Oracle Database SE2 has replaced Oracle Database XE for the local database for Siebel Mobile Web Client. For more information, see *Siebel Installation Guide* .

    The DockConnString parameter specifies the name of the Siebel Server used to synchronize with the client and the type of encryption to use during synchronization, and it has the following format:

```
siebel_server_name::sync_port_number:encryption
```

    Example values for the DockConnString parameter follow. For more information about configuring the DockConnString parameter, see *Configuring Encryption for Mobile Web Client Synchronization*.
    - If using TCP-IP: `APPSRV::40400`
    - If using TLS: `APPSRV::40400:TLS`
11. Restart the Siebel Server or Siebel Application Interface computer on which you installed the certificate file.

Setting HTTP Proxy for UNIX Using the mwcontrol Utility

The following procedure shows you how to set HTTP proxy for UNIX using the mwcontrol utility. A proxy server is a computer that acts as an intermediary between a user's computer and the Internet. A proxy server allows client computers to make indirect network connections to other network services.

To set HTTP proxy for UNIX using the mwcontrol utility

1. Change directory to Siebel root bin as follows:

   ```
   cd $SIEBEL_ROOT/mw/bin
   ```

2. Enter the following command:

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

   The Internet Properties window opens.
3. In the Internet Properties window, click the Connections tab, and then enter the proxy server address and port, for example, as follows:

   Address: `www.` proxyservername `.com`

   Port: 80

   Proxy server details are specific to an organization.

Configuring TLS Mutual Authentication for SHA-2 Certificates Using EAI HTTP Transport

Mutual authentication is a process in which a connection between two parties is established only after each party has authenticated the other. In TLS mutual authentication, the client is authenticated to the server and the server is authenticated to the client during the TLS handshake.

Siebel supports server authentication. Client authentication is supported for TLS-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. In previous releases, client authentication is supported on SHA-2 (that is, TLS v1.2).

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*.

To configure client authentication with SHA-2 certificates using EAI HTTP Transport

1. Obtain the following files, according to the operating system you are using, and install them on Siebel Server:

- For Microsoft Windows operating systems:
  - A certificate authority file.
  - A client certificate file that is in PKCS#12 format.
- For non-windows operating systems:
  - Import the client certificate into the keystore JKS file.
  - Import the CA certificate in to the truststore JKS file.

    For information on how to import certificates into JKS files, see *Siebel Installation Guide* .
  - Make sure that the CONTAINERURL parameter for the OUTBOUNDSHA2 named subsystem has the correct HTTP port number of the application container running on Siebel Server, using the command:

    ```
    list parameter for the named subsystem OUTBOUNDSHA2
    ```

    For example:

    ```
    CONTAINERURL value http://localhost:9001/siebel/outboundeai
    ```
  - Assign the subsystem name to the EAIOutboundSubSys parameter of the component used, using the following command for example:

    ```
    change param EAIOutboundSubSys=OUTBOUNDSHA2 for comp eaiObjMgr_enu
    ```
  - Restart Siebel Server before testing SHA-2 using EAI HTTP Transport.

    For information on installing certificate files, see *Installing Certificate Files*.

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* .

About Configuring Encryption for Siebel Enterprise and Siebel Application Interface

When you configure your Siebel Enterprise or Siebel Application Interface profile after installation using the Siebel Management Console, you specify the encryption type to use for communications between the Siebel Server and Web server (Siebel Application Interface), and between Siebel Servers.

The Encryption Type parameter setting determines how encryption is defined within generated connect strings for Siebel Business Applications. The Encryption Type parameter options for configuring the encryption type are:

- **Without Encryption.**
- **Using TLS 1.2.** TLS encryption is supported on Siebel Server at the server and component level; TLS works for Siebel Remote and Mobile Web Client connections. For information on configuring TLS, see the following topics:
  - *Configuring TLS Encryption for Siebel Enterprise or Siebel Server*
  - *Configuring TLS Encryption for Siebel Application Interface*

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.

For information about running the Siebel Management Console, see the *Siebel Installation Guide* .

About Key Exchange for TLS Encryption

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

Configuring TLS Encryption for a Siebel Enterprise or Siebel Server

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

This task is a step in *Process of Configuring Secure Communications*.

Configuring TLS communications between Siebel Servers and the Web server also requires that you configure the Siebel Application Interface to use TLS. When configuring TLS for Siebel Server and the Siebel Application Interface, 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 TLS encryption involves the following tasks:

1. Run the Siebel Management Console for the Siebel Enterprise or Siebel Server and select the appropriate option to deploy TLS.

   This task is described in *Deploying TLS for Siebel Enterprise or Siebel Server*.
2. For each Application Object Manager that is to use TLS, set the Communication Type (CommType) parameter to TLS as appropriate.

   This task is described in *Setting Additional Parameters for Siebel Server TLS*.

Deploying TLS for a Siebel Enterprise or Siebel Server

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

> **Note:** If you configure 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 Management Console 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 TLS for your Siebel Servers, you must run this utility.

To deploy 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 TLS authentication.

2. Depending on whether you are enabling TLS encryption for the Siebel Enterprise or for the Siebel Server, do one of the following:
   - If you are running the Siebel Management Console to configure the Siebel Enterprise, then do the following:
     i. Start the Siebel Management Console and configure values for the Enterprise.

        For information on this task, see *Siebel Installation Guide* .
     ii. When the Additional Tasks for Configuring the Enterprise screen appears, select the Enterprise Network Security Encryption Type option.
     iii. On the Security Encryption Level or Type screen, select the following option: SISNAPI to use TLS 1.2.
   - To run the Siebel Management Console directly on a Siebel Server computer, do the following:
     i. Start the Siebel Server Management Console directly and configure values for the Siebel Server.

        For information on this task, see *Siebel Installation Guide* .
     ii. When the Additional Tasks for Configuring the Siebel Server screen is displayed, select the Server-Specific Security Encryption Settings option.
     iii. On the Security Encryption Level or Type screen, select the following option: SISNAPI to use TLS 1.2.

   Note: If you change to a different Siebel Management Console, then you might need to redeploy the profile. The easiest way to do this is to create a new profile and apply it to the required server using Siebel Management Console (or Siebel Server Manager, although this is harder).

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

   The parameters to configure in the Siebel Gateway are:
   - Certificate File Name (CertFileName)
   - Certificate Authority (CA) Certificate File Name

   For more information about these parameters, see *Parameters for Configuring Security Adapter Authentication*.
4. 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 parameters to configure in the Siebel Gateway are:
   - Private Key File Name
   - Private Key File Password

   For more information about these parameters, see *Parameters for Configuring Security Adapter Authentication*.
5. Specify whether or not you want to enable peer authentication.

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

   The peer authentication parameter is ignored if TLS is not deployed between the Siebel Server and the client (either the Siebel Application Interface or another Siebel Server). If peer authentication is enabled (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

TLS is deployed and the Siebel Application Interface has a certificate, then it is recommended that you enable peer authentication on both the Siebel Server and the Siebel Application Interface to obtain maximum security.

The parameter to configure in the Siebel Gateway is Enable Peer Authentication.

6. 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 parameter to configure in the Siebel Gateway is Validate Peer Certificate.

   Depending on whether you are running Siebel Management Console for Siebel Enterprise or Siebel Server, return to either the Siebel Enterprise or the Siebel Server configuration process.
7. Continue to configure values for the Siebel Enterprise or Siebel Server, then review the settings, finish configuration, and restart the server (which is required only if you are reconfiguring TLS encryption for Siebel Enterprise or Siebel Server).
8. Perform the tasks in *Setting Additional Parameters for Siebel Server TLS*.
9. Repeat this procedure for each Siebel Server in your environment, as necessary.
10. Make sure you also configure each Siebel Application Interface in your environment. For information, see *Configuring TLS Encryption for Siebel Application Interface*.

Setting Additional Parameters for Siebel Server TLS

After configuring TLS for a Siebel Server, you must set additional server parameters (on the gateway) to enable TLS for the Siebel Server as described in the following procedure.

To set additional parameters for Siebel Server TLS

1. Using Siebel Server Manager, set the Communication Type (alias CommType) parameter to TLS as appropriate for each Application Object Manager that is to use TLS (TCP/IP is used by default). For information on using Siebel Server Manager, see *Siebel System Administration Guide* .
2. If you previously used RSA encryption, then using Siebel Server Manager, set the Encryption Type (alias Crypt) parameter to NONE for the Siebel Enterprise.

Configuring TLS Encryption for Siebel Application Interface

This topic describes how to configure the Siebel Application Interface to use TLS encryption and, optionally, authentication for communications with Siebel Servers. Configuring TLS communications between Siebel Servers and the Web server also requires that you configure a Siebel Enterprise or Siebel Server to use TLS. For information on this task, see *Configuring TLS Encryption for Siebel Enterprise or Siebel Server*.

This task is a step in *Process of Configuring Secure Communications*.

Note: The information in this topic describes how to implement TLS for communications between Siebel Application Interface and Siebel Servers. For information on implementing TLS for communications between Siebel Web Client and Siebel Application Interface, see *About the Siebel Web Client and Using HTTPS*.

You must include TLS-related parameters in the applicationinterface.properties file if you are using TLS to encrypt communications between the Web server and the Siebel Server.

To configure TLS encryption for Siebel Application Interface

1. Ensure that the following parameters are set in the applicationinterface.properties file by the Siebel installer:
   - TrustStoreName
   - KeyStoreName
   - TrustStorePassword
   - TrustStoreType=JKS
   - KeystoreType=JKS

   KeyStore and TrustStore with valid certificate, are a prerequisite for the application interface component installer to pick and use.

   The applicationinterface.properties file is located on the Siebel Application Interface in the `applicationcontainer_external\webapps` folder.
2. In addition to these parameters, set the following parameter in the setenv.bat file located on the Siebel Application Interface in the `applicationcontainer_external\bin` folder:

   ```
   set CATALINA_OPTS=-Djavax.net.ssl.keyStoreAlias=<<keystore alias name>>
   ```

Enabling SSL Acceleration for Application Interface/ Enabling HTTP

This topic describes how to configure SSL acceleration for communications between application interface traffic. The instructions in this topic apply to all channels (UI and EAI).

This task is a step in *Process of Configuring Secure Communications*.

If you are using a third party HTTP-based load balancer for Siebel Application Interface load balancing and you want to off-load the processing of SSL 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 SSL is used to encrypt URLs. EnforceSSL is False by default. To enforce the use of SSL acceleration, you change the EnforceSSL parameter for an Application Object Manager to True.

To enable SSL acceleration for application interface/enable HTTP

1. Enable HTTP for Object Manager-based applications:
   a. Set the Application Object Manager parameter, EnforceSSL, to TRUE as follows:
      - Navigate to the Administration - Server Configuration screen, then the Servers view.
      - In the Siebel Servers list, select the Siebel Server of interest.
      - Click the Components view tab.
      - In the Components list, select the Application Object Manager of interest such as Call Center Object Manager (ENU).
      - Click the Parameters subview tab.
      - In the Parameter field, perform a case-sensitive query on EnforceSSL.
      - Click the Value in the Restart field and type TRUE.
   b. Set the SecureLogin and SecureBrowse server parameters to FALSE for the Application Object Manager (see Step 1.1 for details).
   c. Set the `<transport-guarantee>` value to NONE (instead of CONFIDENTIAL) in the web.xml file located in the following directory:

```
<Siebel Home Directory of Application Interface>\applicationcontainer_external\webapps\siebel\WEB-INF
<security-constraint>
 <web-resource-collection>
 <web-resource-name>securedapp</web-resource-name>
 <url-pattern>/*</url-pattern>
 </web-resource-collection>
 <user-data-constraint>
 <transport-guarantee>NONE</transport-guarantee>
 </user-data-constraint>
</security-constraint>
```

2. Enable HTTP for the Siebel Management Console Application and Siebel Migration Application.

   To do this, set the `<transport-guarantee>` value to NONE (instead of CONFIDENTIAL) in the web.xml file located in the following directories:

```
// Siebel Management Console Application:
<Siebel Home Directory of Application Interface>\applicationcontainer_external\siebelwebroot\smc\WEB-INF

// Siebel Migration Application:
```

```
<Siebel Home Directory of Application Interface>\applicationcontainer_external\siebelwebroot\migration
\WEB-INF
```

> **Note:** When enabling HTTP for the application interface, the implementer must take full responsibility for ensuring overall security of the deployment. When enabling HTTP, protecting intranet ports preservation of secure function involves the following:
>
> - A reverse proxy must always be implemented in front of all application interfaces in the DMZ to secure the intranet ports behind the DMZ.
> - Adjustments to HTTP in linked Web applications to avoid mixed content errors may be needed (if supported). This may require reverse proxies and/or a new security design for any impacted UI based integrations.

3. Restart Siebel Application Interface and 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 set for the Siebel Application Interface 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 *About the Siebel Web Client and Using HTTPS*.

- **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 TLS encryption for Mobile Web Client synchronization.

  For information on setting encryption for transmissions between the Mobile Web Client and Siebel Remote Server, see *Configuring Encryption for Mobile Web Client Synchronization*. 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. 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 Siebel Mobile Web Client synchronization. During this synchronization, DX files are transferred between the Siebel Server and Mobile Web Clients. DX files use messages to transfer information between the Siebel Server and Mobile Web Clients.

This task is a step in *Process of Configuring Secure Communications*.

The Siebel Mobile Web Client reads configuration parameters in the Siebel application configuration file to determine the type of encryption to use during synchronization. Encryption options are defined as one of the elements in the `DockConnString` parameter.

> **Note:** TLS is the supported encryption method for the Siebel Developer Web Client and 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*. For general information on configuring encryption for Web clients, see *About Configuring Encryption for Web Clients*. 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 configure encryption for Mobile Web Client synchronization

1. Open the Siebel application configuration file that you want to edit.

   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 (siebel.cfg is used for Siebel Sales). For more information about working with Siebel application configuration files, see *Siebel System Administration Guide* .

   > **Note:** You can use any plain text editor to edit configuration files. However, when you edit configuration files, do not use a text editor that adds additional, nontext characters to the file.

2. Locate the DockConnString parameter in the [LOCAL_SE] section of the configuration file and modify it as required.

   > **Note:** As of Siebel CRM 20.8 Update, Oracle Database SE2 has replaced Oracle Database XE for the local database for Siebel Mobile Web Client. For more information, see *Siebel Installation Guide* .

   The DockConnString parameter specifies the name of the Siebel Server used to synchronize with the client and the type of encryption to use during synchronization, and it has the following format:

   ```
   siebel_server_name::sync_port_number:encryption
   ```

   where:

   - siebel_server_name is the logical network address of the Siebel Server that the remote client uses to connect and synchronize
   - sync_port_number is the TLS or TCP/IP port number that Siebel Remote uses for the Synchronization Manager. If you do not specify any value, then the default value is 40400.
   - encryption (optional) is the type of encryption used during synchronization. As of Siebel CRM 19.6 Update, Siebel Remote supports TLS for synchronization, where the necessary configuration has been done on the server and the clients. If you do not specify TLS, then no encryption is used.

   Example values for the DockConnString parameter are:

   - If using TCP-IP: `APPSRV::40400`
   - If using TLS: `APPSRV::40400:TLS`

3. 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* .
4. Deploy SHA-2 certificate files on the Siebel Server and remote clients. This is required to use TLS encryption. For more information, see the topic about configuring TLS encryption in *Siebel Remote and Replication Manager Administration Guide* .

About Data Encryption

You can encrypt sensitive data in the Siebel database using AES encryption. It's recommended that you implement AES encryption for increased data security.

See the following topics for information about data encryption:

- *How Data Encryption Works*
- *Requirements for Data Encryption*
- *Encrypted Database Columns*
- *Procedure to Modify Encryption Seed*
- *Upgrade Issues for Data Encryption*

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

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's 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*.

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*.

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

Requirements for Data Encryption

You must follow specific 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's truly sensitive, such as credit card numbers and social security numbers.
- Siebel Assignment Manager doesn't 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 primary 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 can't create the association between the two business components. For detailed information on configuring links, see *Configuring Siebel Business Applications* .
- Data that's moved into or out of the Siebel database using Siebel EIM isn't encrypted or decrypted by EIM.

  For more information on encrypting EIM data after it's imported into an encrypted column, see .
- 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.

- You can only apply AES encryption to data in database columns that are at least 32 bytes long. You can't 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 SHA-2 algorithm.
- Field-level AES encryption isn't supported for Siebel Developer Web Clients.
- Encryption isn't supported for List of Values (LOV) columns or multilingual LOV (MLOV) columns.
- Encryption isn't 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*.

Encrypted Database Columns

Siebel Business Applications provide a number of database columns that are encrypted by default. The following table shows 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*.

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

Table	Table Column
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
S_USER	CHALLENGE_ANSWER
	CHALLENGE_QUESTION
T_DETAIL	ENCRPTD_COL

The CC_NUMBER and CC_NUM columns listed in the table 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.

Procedure to Modify Encryption Seed

The procedure to apply custom seed for encryption is applicable from Siebel release 23.6 and it is a **non-mandatory post installation** task. There is no need to re-apply customer seed in the subsequent patch once it is enabled in 23.6 or above updates.

Note: Though not required, it is recommend to use custom seed for secure Siebel implementations.

1. Make sure to take backup of files specified in Table 1 before making any updates.

2. Create a new Environment variable by the name **SBL_FS_CONST** and value as required seed. Seed expects alphanumeric characters and length should be of 44-50 characters long for strong encryption. If the seed length is not between 44 to 50 characters, then the encrypt string utility will give an error.

   For example: set SBL_FS_CONST=j0dfbjtfhkdbjbkbnjb83h7y7fsfdbfjh66dhfkbjhh=

   Steps to be followed in Windows

   a. Go to **System Properties → Open Environment Variables**.
   b. Create a new Environment variable with a name **SBL_FS_CONST** and value as required seed.

   Steps to be followed in Non Windows

   a. Go to **Home Directory**
   b. Export `SBL_FS_CONST=VALUE`

      for example :

      ```
      export SBL_FS_CONST=j0dfbjtfhkdbjbkbn
      jb83h7y7fsfdbfjh66dhfkbjhh=
      ```

   c. To verify :

      ```
      echo $SBL_FS_CONST
      ```

3. Re-encrypt the passwords saved in various places (detailed in Table 1) manually using EncryptString.jar. Run EncryptString.jar from the environment where custom seed is set via the environment variable SBL_FS_CONST and update them back at the same place.
4. Follow this step if LDAP security adapter is configured.

   Edit LDAP security profile via SMC safe mode and re-enter LDAP password.

   a. Login to smc in safe mode (../smc/safemode.html)
   b. Select LDAP Authentication to update its password and save it.
   c. Log out from SMC
5. Restart all the containers (AI, Migration, CG and SES containers) where re-encrypted passwords are updated.

Below is Table 1 describing specified backup files.

SN	LOCATION	FILE	VARIABLE NAMES
1	applicationcontainer_internal\webapps	configagent.properties	KeyStorePassword TrustStorePassword
		gateway.properties	KeyStorePassword TrustStorePassword registrypassword
2	applicationcontainer_external\webapps	applicationinterface.properties	Password KeyStorePassword TrustStorePassword

SN	LOCATION	FILE	VARIABLE NAMES
		migration.properties	KeyStorePassword TrustStorePassword
3	**It is applicable only where Event Pub-Sub feature is enabled.** In addition to above changes, follow this in AI Side car - applicationcontainer_external(copy)\webapps	applicationinterface.properties	AIEgressServerKeyStorePassword KafkaKeyStorePassword KafkaTrustStorePassword KafkaPassword
		aieventconfig.txt	Update all the instances of **Password**

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 25.10 and later release.

Application developers enable data encryption by encrypting columns in database tables. All fields in the encrypted columns are encrypted.

When you upgrade from an earlier release 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 using AES 256-bit encryption .

If data encryption is to work in the current release, then the encrypted column and the key index column must reside in the same database table. For information on encrypting database columns in Siebel 25.10 and later releases, see the following topics:

- *Configuring Encryption and Search on Encrypted Data*
- *Encrypting Columns in a Business Component*

About Siebel Encryption

Siebel encryption provides 256-bit encryption. Siebel encryption provides AES encryption, using AES Encryptor. AES encryption for data is provided as a Siebel business service and is configured using Siebel Tools.

Siebel provides:

- AES encryption, using AES Encryptor
- The files in the following table for AES data encryption.

File	Purpose
sslcrsa256.dll (Windows)	Provides AES 192-bit or 256-bit data encryption.

File	Purpose
libsslcrsa256.so (UNIX)	
sslcnapi128.dll (Windows) sslcnapi128.so (UNIX)	Supports 2048-bit or 4096-bit data encryption.

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*.

Configuring Encryption and Search on Encrypted Data

You use Siebel Tools to enable encryption for a column in a database table and to enable search on the encrypted column. 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 SHA-2 algorithm to the plain text value of the encrypted data. Search can be case-sensitive or case-insensitive depending on how you configure search.

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

This procedure explains how to encrypt data and, optionally, enable searching on the encrypted data. Before you begin, note the following:

- 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 can't encrypt a column that has a denormalized column, because this feature isn't 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*.

Note: All encryption that's upgraded is upgraded to a minimum of 256 bits in Siebel CRM.

Encrypt a Column and Enable Search

Here's how 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 the previous step:

- 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 *Data Encryption*.
- Encrypt Key Specifier. Specify the column that stores the index number to the key file.

4. To allow search on encrypted data, create another column with a name of your choice or with the following name format: `C_HASH_NAME`. Where `Name` is the name of the column you selected earlier in this procedure.

   `C_HASH_NAME` stores the value that results from applying the SHA-2 algorithm to the plain text values of the column you selected earlier in this procedure.

   The following table shows the syntax for several 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 the next step of this procedure.

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.

   This step is mandatory for successful Siebel CRM upgrade, otherwise encrypted data with the old hash value will not be readable.

6. Update the repository and deliver the updates.
   Note that tables can be published using the Apply/DDL button or the siebdev.exe utility in Siebel Tools (Windows environment). For more information on publishing tables, see *Using Siebel Tools*.

Encrypting Columns in a Business Component

The following example procedure shows you how to create a new encrypted field/column named *Password* for the *Account* business component. Note the following requirements:

- The encrypted column must be larger than the largest value you want to encrypt. That is, (4x +10) times larger where x is the longest password allowed. If you allow a 20 character password, then you need 90 characters (4*20+10) for the encrypted field/column.
- For encryption to work, a minimum of two columns are required as follows:
  - The column that you want to encrypt (in the following example, this is PASSWORD).
  - A second column, which stores the Encryption Key Specifier, or the index number to the key file (PASSWORD_ENCRYPKEY_REF).

To encrypt a column in the Account BusComp

1. Locate the base table where data is stored for the Account BusComp.
   Since Account BusComp is an S_PARTY BusComp, use the Inner Join Extension Table 1 (S_ORG_EXT).
2. Navigate to S_ORG_EXT and extend it to include the following new columns:
   a. **PASSWORD_ENCRYPKEY_REF.** This column stores information about the key file that is used to encrypt the password field (of size VARCHAR(30)).
   b. **PASSWORD.** This column stores the encrypted password and contains the following attributes:
      - The VARCHAR size must be (4x +10) times larger than the longest possible password.
      - The Computation Expression is `SiebelEncrypt.AES([PASSWORD])`.
      - The Encrypt Key Specifier is `PASSWORD_ENCRPKEY_REF`.
   c. **C_HASH_PASSWORD** (Optional). This column allows case-sensitive searches against the encrypted column:
      - The VARCHAR must be the same size as PASSWORD.
      - Set the Computation Expression to `SiebelHash.SHA1 ([C_PASSWORD])`.
   d. **C_HASH_PASSWORD_CI** (Optional). This column allows case-insensitive searches against the encrypted column:
      - The VARCHAR must be the same size as PASSWORD.
      - Set the Computation Expression to `SiebelHash.SHA1CI ([C_PASSWORD])`.
3. Return to the Account Business Component and add new fields based on the columns created earlier in this procedure.
4. To partially show a field in the UI (for example, to show a partial credit card number as xxxxxxxxxxx1234), perform the following configuration steps:
   a. Create a new field named `"Field Name - Display"`.

b. Mark it as a Calculated Field with no Calculated Value attribute.

c. Create the following Field User Properties for the calculated field.

- Encrypt Source Field. The name of the field that stores the actual encrypted field (for example: "Password").
- Display Mask Char. The character to be used to mask part of the encrypted string (for example: "x").

d. Add the calculated field to the appropriate applets.

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 key file is encrypted with the key file password, which is supplied by the Admin user. The key file password is encrypted with the default key from keyfile.bin and default AES-256 encryption; the encrypted password is stored in the Siebel database. The AES Encryptor uses the key in the key file to encrypt new data.

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.

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: Before starting a migration installation for Siebel Enterprise Server, you must make a copy of the original key file (keyfile.bin). You must do this because when data encryption is enabled, the migration process creates a new key file overwriting your existing keyfile.bin. After the migration installation, copy back the original key file. For more information about Siebel migration installation, see *Siebel Installation Guide* .

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 the table in this topic.
3. When prompted, enter the key file password:
   - To add a new encryption key, see *Adding New Encryption Keys*.
   - To change the key file password, see *Changing the Key File Password*.
4. To exit the utility, enter 3.

5. Restart any server components that were shut down in the first step of this procedure.
   For information on starting server components, see *Siebel System Administration Guide* .

The following table lists the flags and parameters for the Key Database Manager utility.

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 (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*
- *Changing the Key File Password*

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*.
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 impossible to recover encrypted data without a backup key file.

7. Restart any server components that were shut down in the first step of this procedure.

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

Changing the Key File Password

The key file is encrypted with the key file password, which is supplied by the Admin user. 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*.
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 the first step of this procedure.

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

Updating siebel.cfg Before Running Key Database Manager

You must set the following configuration parameters, in the siebel.cfg file, before running the Key Database Manager utility. The Key Database Manager utility is used to maintain the key file (keyfile.bin).

1. **[ServerDataSrc] section.** Set all parameters correctly in this section. For more information about the parameters in this section, see *Siebel System Administration Guide* .

   Failure to set all the parameters correctly in this section might result in an error similar to the following: *An internal error has occurred within the authentication subsystem for the Siebel application. Please contact your system administrator for assistance. (SBL-DAT-00565)*
2. **[InfraSecMgr] section.** Set the following parameters:

   - SecAdptName: Set to `DBSecAdpt` (the default value).
   - SecAdptMode: Set to `DB` (the default value).

   Failure to set these parameters correctly might result in an error similar to the following: *An error occurred loading the Siebel authentication subsystem configuration from the configuration store. More specifically, <?> Please contact your system administrator for assistance. (SBL-DAT-00561)*
3. **[DBSecAdpt] section.** Set the following parameter:

   - DataSourceName : Set to `ServerDataSrc` (change the default `Local` value to `ServerDataSrc`).

   Failure to set this parameter correctly might result in an error similar to the following: *An internal error has occurred within the authentication subsystem for the Siebel application. Please contact your system administrator for assistance. (SBL-DAT-00565)*

Centralizing the Location of the Key File

The key file, keyfile.bin, is installed by default in the `SIEBSRVR_ROOT\admin` directory. Depending on your requirements, you can optionally centralize the location of the key file for your Siebel CRM deployment, such as in the Siebel File System or in another secure repository. Doing so requires that you create a symbolic link to the central location in the `SIEBSRVR_ROOT/admin` directory for each installed Siebel Server.

To centralize the location of the key file

1. Shut down the Siebel Server where you will create the symbolic link.
2. For the first Siebel Server, move the latest keyfile.bin file from this Siebel Server (`SIEBSRVR_ROOT\admin`) to the centralized location. This step does not apply for additional Siebel Servers on which you perform this step.
3. (Windows) Create a symbolic link to the centralized keyfile.bin in each Siebel Server, as follows:

   - Navigate to `SIEBSRVR_ROOT\admin`.
   - Open a Command Prompt as an Administrator.
   - Enter a command like the following:

   ```
   mklink /h <absolute path of centralized location>\keyfile.bin keyfile.bin
   ```

4. (UNIX) Create a symbolic link to the centralized keyfile.bin in each Siebel Server as follows:
    - Navigate to `SIEBSRVR_ROOT/admin`.
    - Enter a command like the following:

      ```
      ln -s <absolute path of centralized location>\keyfile.bin keyfile.bin
      ```
5. Delete the physical key file from `SIEBSRVR_ROOT/admin`.
6. Start the Siebel Server.
7. Repeat steps 1 to 6, as required, on each additional (installed) Siebel Server.

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. For more information, see *Data Encryption*.

About Encoding UI Values

You can use the control user property Encode to encode (or not encode) values in the UI as follows:

- Set the control user property Encode to False to skip or ignore HTML encoding for control values.

  All control values that come from trusted sources, set Encode to False by default.

- Set the control user property Encode to True to encode all control values.

  For customized or newly introduced controls, all control values are encoded if Encode is set to True. True is the default value for Encode.

Siebel distinguishes the source for the calculated field value by taking the value from one of the following:

- The Business Component fields.

  Field values are user-entered, un-trusted, and are not provided to the browser for execution to avoid cross site scripting flaws.

- The hard coded value, provided in the Siebel repository.

  Hard coded values are from a trusted source and do not require encoding.

5 Security Adapter Authentication

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*
- *About Siebel Security Adapters*
- *About Database Authentication*
- *Implementing Database Authentication*
- *About Authentication for LDAP Security Adapter*
- *Process of Implementing LDAP Security Adapter Authentication*
- *About Authentication for Siebel Gateway Access*
- *About Authentication for Mobile Web Client Synchronization*
- *Installing and Configuring Oracle LDAP Client Software*
- *Configuring Security Adapters Using the Siebel Management Console*
- *Migrating from Database to LDAP Authentication*
- *Security Adapter Deployment Options*
- *About Password Hashing*
- *Process of Configuring User and Credentials Password Hashing*
- *Running the Password Hashing Utility*
- *Setting the ConfigLdapAuthTimeout Parameter*
- *Setting the ConfigLdapFailoverTimeout Parameter*

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 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). For more information, see *About Database Authentication* and *Implementing Database Authentication*.

> **Note:** Database authentication is supported for development environments only, it is not supported for production environments.

  - **Lightweight Directory Access Protocol (LDAP) 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 LDAP Security Adapter to authenticate against directory servers. For more information, see *About Authentication for LDAP Security Adapter* and *Process of Implementing LDAP Security Adapter Authentication*.
  - **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*.

- **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 *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 *Authentication Related Configuration Parameters* For information about the seed data related to authentication, user registration, and user access that is installed with Siebel Business Applications, see *Seed Data*.

Issues for Mobile Web Clients

The following special issue applies for authentication for deployments using Mobile Web Client:

- 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

The following table highlights the capabilities of each authentication method 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.

Functionality	Database Security Adapter	LDAP Security Adapter	Web SSO
Requires additional infrastructure components.	No	Yes	Yes
Centralizes storage of user credentials and roles.	No	Yes	Yes

Functionality	Database Security Adapter	LDAP Security Adapter	Web SSO
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.
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

https://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 (selected by default). For more information, see *About Database Authentication*.
- LDAP (Lightweight Directory Access Protocol) security adapter. For more information, see *About Authentication for LDAP 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*.

You can implement LDAP authentication for application object manager components and for EAI components. Do not use the LDAP security adapter to authenticate access for 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 security adapter.

Authentication Directories

An LDAP 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 CRM* 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 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's identity is verified.
- 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 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.

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* . For more information about configuring the log events for Siebel Mobile applications and saving the log information, see *Siebel Mobile Guide: Disconnected* .

About Database Authentication

If you do not use LDAP 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 Application Interface 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 Hash User Password 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 on the database server by adding 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.

When creating a profile using Siebel Management Console, the database security adapter is selected by default, indicating to use database authentication, but you can change this and select to use an LDAP or a custom security adapter as required.

> **Note:** Database authentication is supported for development environments only, it is not supported for production environments.It is strongly recommended that you use TLS for database authentication.

About Implementing the Database Security Adapter

You implement the database security adapter using the Enterprise Security Authentication Profile (Security Adapter Mode) parameter and the Security Adapter Name (named subsystem) parameter. You can set these parameters for the Siebel Gateway, 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).

> **Note:** To configure an individual Siebel Server or component to use LDAP at a later time, then you must configure the Enterprise Security Authentication Profile (Security Adapter Mode) and the Security Adapter Name (named subsystem) parameters as shown in Step 1 of the following procedure.

You can configure the Security Adapter Mode and Security Adapter Name parameters using the Siebel Management Console.

> **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.
   b. Set the Security Adapter Name parameter to DBSecAdpt, 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 *Authentication Related Configuration Parameters*.

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*.

   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*.

4. If you are implementing database authentication with an MS SQL Server database, then perform the task described in *Implementing Database Authentication with Microsoft SQL Server*.

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 Microsoft 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*.

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 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 Microsoft SQL Server

1. On the Siebel Server computer, 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 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 Authentication for LDAP Security Adapter

Siebel Business Applications include security adapters that are based on LDAP standards, allowing customers to use LDAP directory products for user authentication. LDAP 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.

Before implementing security adapter authentication for LDAP security adapters, note the following:

- You must install the Oracle Database Client, which contains the Oracle LDAP Client, on the Siebel Server or Siebel Gateway computer if you choose the LDAP security adapter.
- How you configure communications encryption between the Siebel security adapter and the directory server differs depending on the security adapter you use. TLS encryption is supported with the LDAP security adapter. For more information, see *Configuring Secure Communications for Security Adapters*.

For more information about LDAP security adapter authentication, see the following topics:

- *LDAP Security Adapter Authentication Process*
- *Directory Servers Supported by Siebel CRM*
- *Administering the Directory through Siebel Business Applications*
- *Communicating with More Than One Authentication Server*
- *Requirements for the LDAP Directory*

LDAP Security Adapter Authentication Process

In an implementation using LDAP 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 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 email address or telephone number. The user credentials are passed to the Siebel Application Interface 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 LDAP security adapter used with Siebel Business Applications allows special characters in passwords. Be aware, however, that only a limited number of special characters are supported for use in Siebel passwords. Passwords are also subject to the requirements and limitations imposed by the external directory service. For additional information, see *Characters Supported in Siebel Passwords*.
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 security adapters. Siebel CRM supports the following directory servers:

- **LDAP directory servers.** Siebel CRM supports 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.

Administering the Directory through Siebel Business Applications

If you choose to administer the LDAP directory through Siebel Business Applications, then be aware that in large implementations timeout issues can occur. 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.

Communicating with More Than One Authentication Server

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 that enable LDAP security adapters to communicate with multiple LDAP-compliant directories. For information on Oracle Virtual Directory, go to

  http://www.oracle.com/technetwork/testcontent/index-093158.html

Requirements for the LDAP Directory

If you implement LDAP 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), 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.

About Setting Up the LDAP Directory

To provide user access to a Siebel application implementing an LDAP 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 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 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 instead of in an attribute value for the directory entry. For more information, see *Configuring the Shared Database Account*.

  > **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.** Stores a user's login password for the LDAP server. 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 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 *Server Parameters for Siebel Gateway*.

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*.

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 (*https://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*.

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*.

Process of Implementing LDAP Security Adapter Authentication

This topic describes the tasks involved in implementing LDAP 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 an LDAP 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*. For information about special considerations in implementing user authentication, see *Troubleshooting User Authentication Issues*.

> **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*. 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 security adapter authentication architecture:

1. Verify that all requirements are met. For information on the requirements, see *Requirements for Implementing an LDAP Authentication Environment for Oracle LDAP Client Installation*.
2. Review *About Creating a Database Login for Externally Authenticated Users*.
3. Set up the attributes for users in the directory. See *Setting Up the LDAP Directory*.
4. Create users in the directory: a regular user, the anonymous user, and the application user. See *Creating Users in the LDAP Directory*.
5. Add user records in the Siebel database corresponding to the users in the directory. See *Adding User Records in the Siebel Database*.

6. Edit parameters related to security adapter authentication in the Siebel Application Interface profile. See *LDAP Security Adapter Authentication Parameters in the Siebel Application Interface Profile*.
7. Select the security adapter you want to use (LDAP or Custom) and then configure parameters for the selected security adapter. Use one of the following methods:
    - Use Siebel Management Console

      Start the Siebel Management Console, select the security adapter you want to use (LDAP or Custom), and then specify the appropriate values for the following parameters:

        - Enterprise Security Authentication Profile (Security Adapter Mode)
        - Security Adapter Name (named subsystem)

      For more information, see *Configuring Security Adapters Using the Siebel Management Console*.
    - Edit the parameters directly for Siebel Gateway

      You can select the security adapter you want to use, and then configure the parameters for the security adapter by editing the parameters directly using Siebel Server Manager. For more information, see *Configuring Security Adapter Parameters for Siebel Gateway*.
    - Edit the application configuration file (Developer Web Clients only)

      For Developer Web Clients only, you configure parameters for the security adapter in the application configuration file. For more information, see *Configuring Security Adapter Parameters for Developer Web Clients*.
8. (Developer Web Client only) *Setting a System Preference for Developer Web Clients*.
9. *Restarting Servers*.
10. *Testing the LDAP Authentication System*.

Requirements for Implementing an LDAP Authentication Environment for Oracle LDAP Client Installation

This topic describes the requirements for implementing an LDAP authentication environment. The Siebel default authentication method is database authentication but if you want to implement LDAP authentication instead, then verify that the requirements outlined in this topic are in place.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication* and *Installing and Configuring Oracle LDAP Client Software*.

You must complete the following tasks before you can configure an LDAP security adapter for your environment and install Oracle LDAP Client software:

- Install the Web server.
- Install the LDAP directory.
- Install the Siebel Enterprise Server components (Siebel Gateway, Siebel Server, and Database Configuration Utilities).

  For information on this task, see *Siebel Installation Guide* .
- Review *Requirements for the LDAP Directory*.

  To implement LDAP 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) If using LDAP authentication for non-Oracle Database deployments and for deployments with Oracle Database, then you must install the Oracle Database Client, which contains the Oracle LDAP Client software.

  Consider the following requirements for the Oracle LDAP Client installation in a Siebel environment:

  - The Oracle LDAP Client must be installed on each Siebel Server or Siebel Gateway computer for which LDAP authentication is to be supported using the LDAP security adapter. For deployments with Oracle Database, the Oracle LDAP Client software can be installed either before or after you install the Siebel Server.
  - Oracle Wallet Manager, which is required if you are supporting TLS, is an application you use to generate wallets. Wallets 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.
  - For deployments with Oracle Database, Siebel Developer Web Client deployments only support database authentication.

  For more information about the requirements for installing the Oracle LDAP Client, see *Siebel Installation Guide* .

  > **Note:** If you are using LDAP security adapter authentication, then you must download and install the latest Oracle Database Client (which contains the Oracle LDAP Client) from Oracle Software Delivery Cloud, even if you are using Siebel Business Applications with an Oracle Database and have previously installed the Oracle LDAP Client. Be aware that only one Oracle LDAP Client can be used in a Siebel CRM implementation, so if you download and install the latest Oracle Database Client (containing the Oracle LDAP Client) from Oracle Software Delivery Cloud to enable LDAP authentication, then you must also use this client to connect to your Oracle Database.

- 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 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 Security Adapter Authentication*.

A database login is created for externally authenticated users during the Siebel installation process. If you are using an Oracle or Microsoft/Azure SQL Database Server, 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* .

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

When you implement LDAP 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 Security Adapter Authentication*.

The following procedure describes how to set up the LDAP directory. For more information about setting up the directory, review *About Setting Up the LDAP Directory*.

To set up the LDAP directory

1. Determine the Base Distinguished Name, that is, the location in the directory in which to store users. For details, see the Base Distinguished Name (DN) parameter description in *Server Parameters for Siebel Gateway*.

   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.
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.
   - **Database account.** Suggested attribute: dbaccount.
   - **Password.** Suggested attribute (for LDAP only): userPassword.

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

Creating Users in the LDAP Directory

This topic describes the users you must create in the LDAP directory to implement LDAP security adapter authentication.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

When you use LDAP 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*.
- **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*.
- **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 security adapter profiles. For more information, see *Configuring the Shared Database Account*.

Create users in the directory using values similar to those shown in the following table. Store information for users in the directory attributes indicated in *Setting Up the LDAP Directory*. Optionally, complete other attribute entries for each user.

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 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*.

The example directory entries in the table in this topic 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*. The P symbol represents the password for that database account. For additional information, see *Configuring the Shared Database Account*.

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*.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

You must confirm that the seed data record exists for the anonymous user for your Siebel customer or partner application, as described in *Seed Data*. This record must also match the anonymous user you created in *Creating Users in the LDAP Directory*.

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, 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*.

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 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.
User ID Example: TESTUSER	Required. This entry must match the uid (LDAP) 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*. You can complete other fields, but they are not required.

LDAP Security Adapter Authentication Parameters in the Siebel Application Interface Profile

This topic describes the parameters you must configure in the Siebel Application Interface profile when you implement LDAP security adapter authentication.

Configure the Siebel Application Interface profile parameters using values similar to those shown in the following table. Specify values for Anonymous User Name and Anonymous User Password in the Basic Information - Authentication section of the application interface profile if you are configuring LDAP authentication for all your Siebel Business Applications. If you are implementing LDAP authentication for a single application, then specify these parameters in the Applications section of the application interface profile. For more information, see *Siebel Application Interface Profile Parameters*.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

Section in Siebel Management Console	Parameter	Guideline

Basic Information - Authentication section under Application Interface Profiles, OR Applications section under Application Interface Profiles.
 	
That is, the section that is specific to your application, such as one of the following, where /enu is the language code for U.S. English:
 	
`[/eservice/enu]`
 	
`[/callcenter/enu]`
	Anonymous User Name	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) entry for the anonymous user record in the directory. For example, enter **`GUESTCST`** for Siebel eService.

	Anonymous User Password	Enter the password you created in the directory for the anonymous user. For information on this parameter, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*.

Configuring Security Adapter Parameters for Siebel Gateway

This topic describes the security-related configuration parameters you use for configuring an LDAP security adapter that are defined in the Siebel Gateway.

You can modify some Siebel Gateway configuration parameters (such as, enterprise profile and object manager parameters) using either Siebel Server Manager or the Siebel Management Console, but others can only be modified using the Siebel Management console. For example, you cannot modify security profile parameters using Siebel Server Manager, you must use the Siebel Management Console to set security profile parameters. For information on using Siebel Server Manager to edit parameters on the gateway, see *Siebel System Administration Guide* . For information on editing parameters using the Siebel Management Console, see *Configuring Security Adapters Using the Siebel Management Console*.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

You can set security adapter parameters for Siebel Gateway for the following:

- *Parameters for Enterprise, Siebel Servers, or Components*

- *Parameters for Application Object Manager Components*
- *Parameters for Security Adapter (Profile/Named Subsystem)*

Set security adapter parameters as described in each of these topics. For more information about these parameters, see *Server Parameters for Siebel Gateway*.

Parameters for Enterprise, Siebel Servers, or Components

This topic describes the security adapter parameters you can set at the Siebel Gateway 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 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 the following table.

Subsystem	Parameter	Guideline
Security Manager	SecAdptMode For more information about setting this parameter, see the Enterprise Security Authentication Profile (Security Adapter Mode) parameter in the table in *Parameters for Configuring Security Adapter Authentication*.	The security adapter mode in which to operate. For LDAP, specify **LDAP**.
Security Manager	SecAdptName For more information about setting this parameter, see the Security Adapter Name (named subsystem) parameter in the table in *Parameters for Configuring Security Adapter Authentication*.	The name of the security adapter. For LDAP, specify **LDAPSecAdpt** 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 describes the parameters you set for the Application Object Manager component when implementing LDAP authentication for a single Siebel application.

To implement LDAP 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 the following table.

Subsystem	Parameter	Guideline
InfraUIFramework	AllowAnonUsers	Enter **TRUE** for LDAP. 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**.

Subsystem	Parameter	Guideline
Object Manager	OM - Username BC Field (UsernameBCField)	You can leave this parameter empty.

Note: These parameters (AllowAnonUsers, ProxyName, and UsernameBCField) are server parameters, and they are not available in the Siebel Management Console.

Parameters for Security Adapter (Profile/Named Subsystem)

This topic describes the parameters you set for the enterprise profile (named subsystem) for the specific security adapter you are configuring.

To implement LDAP authentication for a single Siebel application, configure parameters for the LDAP Security Adapter (defined as enterprise profile or named subsystem). Typically, the alias for this adapter is LDAPSecAdpt.

Set the security adapter parameters using values similar to those shown in the following table.

Parameter	Guideline
Security Adapter Dll Name (SecAdptDllName)	For LDAP, enter sscforacleldap.dll 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	Enter the name of the computer on which the LDAP directory server runs.
Port	For LDAP, an example entry is 389. Typically, use port 389 for standard transmission or port 636 for secure transmission.
Base Distinguished Name (DN)	The Base Distinguished Name is the root of the tree under which users are stored. Users can be added directly or indirectly after 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.
User Name Attribute Type	LDAP example entry is uid If you use a different attribute in the directory for the Siebel user ID, then enter that attribute name.
Password Attribute Type	The LDAP entry must be userPassword.

Parameter	Guideline
Credentials Attribute	If you are using an LDAP security adapter, an example entry is **mail**. If you used a different attribute in the directory for the database account, then enter that attribute name.
Application User Distinguished Name (DN)	LDAP example entry: **uid=APPUSER, ou=people, o=domainname** 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	For LDAP, enter **APPUSERPW** or the password assigned to the application user.
Shared Database Account Distinguished Name (fully qualified domain name)	LDAP example entry: **uid=shared database account user User ID, ou=people, o=domainname** For example: **uid=SharedDBUser, ou=people, o=example.com**

Configuring LDAP Authentication for Developer Web Clients

This topic describes the tasks you must perform if you want to implement LDAP security adapter authentication for Developer Web Clients. This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

To configure LDAP authentication for Developer Web Clients, perform the following tasks:

- *Configuring Security Adapter Parameters for Developer Web Clients*
- *Setting a System Preference for Developer Web Clients*

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 security adapter authentication rather than in the gateway.

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 parameters (for Siebel Gateway) listed in the tables in the following topics:

- *Parameters for Enterprise, Siebel Servers, or Components*
- *Parameters for Application Object Manager Components*
- *Parameters for Security Adapter (Profile/Named Subsystem)*

To configure a security adapter for the Developer Web Client, provide parameter values, as indicated by the guidelines in the following table, in the configuration for the Siebel application for which you are implementing LDAP security adapter authentication.

You can use a text editor to make changes to an application's configuration, or you can do so using the Siebel Management Console. For more information about editing an application's configuration and about the purposes for the parameters, see *Siebel Application Configuration Parameters*. For a list of Siebel application configuration files, see *Siebel System Administration Guide* .

Section	Parameter
[InfraUIFramework]	AllowAnonUsers For the AllowAnonUsers parameter, enter **TRUE** for LDAP. 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. Note that AllowAnonUsers is a server parameter, and it is not available in the Siebel Management Console.
[InfraSecMgr]	SecAdptMode For the SecAdptMode parameter, specify **LDAP** for LDAP. For more information about setting this parameter, see the Enterprise Security Authentication Profile (Security Adapter Mode) parameter in the table in *Parameters for Configuring Security Adapter Authentication*.
[InfraSecMgr]	SecAdptName For the SecAdptName parameter, specify **LDAPSecAdpt** or another name of your choice for LDAP. For more information about setting this parameter, see the Security Adapter Name (named subsystem) parameter in the table in *Parameters for Configuring Security Adapter Authentication*.
[LDAPSecAdpt]	For parameters, see *Configuring Security Adapter Parameters for Siebel Gateway* or *Authentication Related Configuration Parameters*.

Setting a System Preference for Developer Web Clients

If you are configuring LDAP 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 security adapter authentication.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

Stop and restart the following services:

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

Testing the LDAP Authentication System

After performing all the tasks required to implement LDAP security adapter authentication, you can verify your implementation using the procedure in this topic.

This task is a step in *Process of Implementing LDAP Security Adapter Authentication*.

The tests outlined in this topic allow you to confirm that the security adapter provided with Siebel Business Applications, your LDAP 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 authentication implementation, perform the following procedure.

To test your LDAP authentication system

1. In a Web browser, enter the URL to your Siebel application, for example:

   ```
   http://<siebel_AI_host><port_num>/siebel/app/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 the first step of this procedure 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 in the following table, and then submit the form. You can complete other fields, but they are not required.

Field	Description
Last Name	Required. Enter any name.
First Name	Required. Enter any name.
User ID	Required. Enter a simple contiguous user ID, which must be unique for each user. Typically, the user provides this user ID to log in. Depending on how you configure authentication, the user might or might not log in with this identifier.
Password	Optional (required for some authentication implementations). Enter a simple contiguous login password. The password must conform to the syntax requirements of your authentication system, but it is not checked for conformity in this form. For LDAP 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 earlier in this procedure.

   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 Authentication for Siebel Gateway Access

The Siebel Gateway registry serves as the dynamic registry for Siebel servers and components. The gateway 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, user access to the gateway is authenticated. Authentication is not implemented for starting the gateway, only for connecting to it.

Siebel Gateway authorization is required whether you use the Siebel Management Console, Siebel Server Manager, or other utilities to access the gateway. In each case, you must specify a valid gateway authentication user name and password. For information on the gateway authentication credentials, see *About Siebel Gateway Authentication Password*.

Authentication Mechanisms

You can choose to use database authentication, LDAP authentication, or custom authentication for the Siebel Gateway and Enterprise.

When you configure Siebel Gateway (first time running Siebel Management Console) or create a profile subsequently, the database security adapter is selected by default, indicating to use database authentication, but you can change this and select to use an LDAP or a custom security adapter as required.

The enterprise profile that you define when configuring the Siebel Enterprise Server using the Siebel Management Console contains the Enterprise Security Authentication Profile (Security Adapter Mode) parameter, the Security Adapter Name (named subsystem) parameter and the Primary Language parameter. You use these parameters to choose the type of authentication to use for the Enterprise.

For information on implementing LDAP authentication for Siebel Gateway, see *Implementing LDAP Authentication for Siebel Gateway*.

Security Profile Configuration

The security profile, which is centrally stored in the registry, contains the configuration parameters that determine how access to Siebel Gateway is authenticated. When a user attempts to log in to the gateway, the user's credentials are passed by the server to the authentication provider specified in the security profile, which checks that the user has the required administrator privileges to access the gateway. If it has, the gateway starts to process service requests.

> **Note:** Authentication is not required for starting the gateway, only for connecting to it.

You configure the security profile using the Siebel Management Console. For more information on the authentication configuration parameters that you must set for the gateway, see *Configuring Security Adapters Using the Siebel Management Console* and *Parameters for Configuring Security Adapter Authentication*.

Updating the Security Profile for Siebel Gateway

As of Siebel CRM 19.11 Update, administrators can update the security profile for Siebel Gateway in the event of a planned or unplanned back-end system (DB/LDAP) outage. Prior to this, it was not possible to update the security profile once the gateway was configured in Siebel Management Console since any change in database/LDAP instance would block a re-login and all other configuration activity.

To update the security profile for Siebel Gateway in Siebel CRM 19.11 Update and later releases, administrators must do the following:

1. First configure a safe mode user to enable login to Siebel Management Console in safe mode. You can only update the security profile in Siebel Management Console safe mode. There is no out-of-the box safe mode user.
2. Then log in to Siebel Management Console in safe mode and update the security profile for Siebel Gateway using the safe mode user credentials.

To update the security profile for Siebel Gateway

1. Determine the safe mode user credentials for Siebel Gateway as follows:
   - Log in to Siebel Management Console and go to the Settings screen.
   - If the safe mode user has already been set, then make a note of the details in the Gateway Safe Mode Credentials section of the Settings screen.
   - If the safe mode user has not been set, then see *Configuring the Siebel Management Console Safe Mode User*.
2. Start Siebel Management Console in safe mode using the following URL format:

   ```
   https://<host-name>:<port-number>/siebel/smc/safemode.html
   ```

3. Log in to Siebel Management Console in safe mode using the safe mode user credentials, which you obtained in Step 1.

   Note that logging in to Siebel Management Console in safe mode is not possible without first configuring the safe mode user.
4. On the Set Up Gateway - Create Security Profile form that appears, modify the security profile details:
   - In the Profile field, enter the name of the security profile. For example: `ORA127`.
   - In the Data Sources section, click the plus (+) icon to add the name of the data source. For example: `ORA127`.
   - Specify the Type of authentication, the Host Name, and the Port number for the data source.

   For more information about these parameters, see *Parameters for Configuring Security Adapter Authentication*.
5. Click Save to save the updated security profile.

   Upon save, the Siebel Management Console safe session automatically logs the administrator out and prompts a re-login to Siebel Management Console in normal mode using the new security profile credentials you specified in Step 4:

   ```
   https://<host-name>:<port-number>/siebel/smc/
   ```

Configuring the Siebel Management Console Safe Mode User

You must configure a safe mode user if you want to log in to Siebel Management Console in safe mode and subsequently update the security profile for Siebel Gateway using the safe mode user credentials. This feature is available in Siebel CRM 19.11 Update and later releases.

- For new deployments, it is recommended that you specify the safe mode user when you first configure the Siebel Gateway.
- For existing deployments, you must specify the safe mode user if you want to be able to update the security profile.

Any administrator can become or create, modify or delete the Siebel Management Console safe mode user. There is no out-of-the-box safe mode user.

To configure the Siebel Management Console safe mode user

1. Log in to Siebel Management Console and go to the Settings screen.
2. For initial creation or for new deployments, create the safe mode user as follows :
   a. Click Edit (the pencil icon) in the Gateway Safe Mode Credentials section.
   b. Click OK when prompted with the following message: Do you want to make yourself the Gateway Safe Mode user?

   Your user ID and Password are now the credentials for the safe mode user.
3. To update the existing safe mode user where the logged in user and the safe mode user are the same:
   a. Click Edit (the pencil icon) in the Gateway Safe Mode Credentials section.
   b. Update the password in the Password and Confirm Password fields. Note that you will not be able to modify the User ID.
   c. Click Submit to save the changes.
4. To update the existing safe mode user where the logged in user and the safe mode user are not the same:
   a. Click Edit (the pencil icon) in the Gateway Safe Mode Credentials section.
   b. Click OK when prompted with the following message: Do you want to remove the existing Safe Mode user and make yourself the new Safe Mode user?
   c. Enter the password in the Password and Confirm Password fields.
   d. Click Submit to save the changes.
5. To delete an existing safe mode user:
   a. Click Delete in the Gateway Safe Mode Credentials section.
   b. Click OK when prompted with the following message: Do you want to permanently remove the Gateway Safe Mode user?
6. Click Refresh, as required, to retrieve the latest information about the safe mode user from the server.

For more information about safe mode for Siebel Management Console, see *Siebel Installation Guide* .

Implementing LDAP Authentication for Siebel Gateway

This topic describes how to implement LDAP authentication for Siebel Gateway. This involves configuring the Siebel Enterprise Server for LDAP authentication using the Siebel Management Console, then adding parameters to the gateway security profile and the LDAP directory. These tasks are described in the following procedure.

To implement LDAP authentication for Siebel Gateway

1. Using the Siebel Management Console, configure your Siebel Enterprise to use the LDAP security adapter provided with Siebel Business Applications.

   For information on this task, see *Configuring Security Adapters Using the Siebel Management Console*.
2. Add the following parameters to the gateway security profile to specify the security adapter you want to implement.

Section Under Security Profiles	Parameter	Value
Basic Information [InfraSecMgr]	Enterprise Security Authentication Profile (Security Adapter Mode)	The security adapter mode to operate in: o For LDAP, specify LDAP.
Basic Information [InfraSecMgr]	Security Adapter Name (named subsystem)	The name of the security adapter. o For LDAP, specify LDAPSecAdpt or another name of your choice.
Data Sources [LDAPSecAdpt]	Roles Attribute	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:
   - The user name and password for gateway authentication.
   - For the gateway 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. Specify Siebel Administrator as the default role.

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. Start Siebel 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. Start Siebel 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. 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* and subsequent topics, earlier in this chapter.

Installing and Configuring Oracle LDAP Client Software

Install the Oracle LDAP Client, which is part of the Oracle Database Client, only for non-Oracle Database deployments and if there is no external or existing Oracle LDAP Client installed on your machine.

To install the Oracle LDAP Client software (which includes Oracle Wallet Manager) and to configure it for your environment, perform the following tasks:

> **Note:** If you install the Oracle LDAP Client with a Siebel Enterprise Server that connects to an Oracle Database, then this installation resets the existing Oracle Home defined for the Oracle LDAP Client to the new Oracle LDAP Client. Consequently, Siebel Business Applications will be unable to connect to the database.

1. Review *Requirements for Implementing an LDAP Authentication Environment for Oracle LDAP Client Installation*
2. Review *Considerations if Using LDAP Authentication with TLS*

Considerations if Using LDAP Authentication with TLS

This topic provides information on using LDAP authentication with TLS. The Oracle LDAP Client requires that Oracle Wallet Manager is installed if TLS must be supported. The LDAP libraries and utilities provided with the Oracle LDAP Client use the TLS libraries provided with Oracle Wallet Manager.

This task is a step in *Installing and Configuring Oracle LDAP Client Software*.

- If Oracle Wallet Manager is installed, then the LDAP libraries dynamically load the TLS libraries and use them to enable TLS, when TLS is configured.
- If Oracle Wallet Manager is not installed and the TLS libraries are not available, then the LDAP library is fully functional, with the exception of TLS support.

By using TLS 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, TLS provides data confidentiality (encryption) on connections protected by TLS. Authentication of servers to clients is accomplished with X.509 certificates.

It is assumed that TLS 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 TLS will never be turned on for Siebel LDAP authentication, then you do not have to install Oracle Wallet Manager.

Creating an Oracle Wallet

To enable TLS 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. Before creating an Oracle Wallet, note that you must be logged in to Siebel as the same user that the Siebel Server service runs under and the wallet must be located in the default location for that user.

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 TLS for clients and servers. You can save the wallet to a different directory if required.

4. Import the CA certificate that you copied to the computer earlier in this procedure 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 TLS for the Siebel LDAP Security Adapter

Use the following procedure to configure TLS for the Siebel LDAP security adapter. For more information about LDAP security adapter configuration, see *Configuring Security Adapters Using the Siebel Management Console*.

To enable TLS for the Siebel LDAP security adapter

1. Copy the wallet you created in *Creating an Oracle Wallet* 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 *Creating an Oracle Wallet*. 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 TLS port is configurable for the LDAP server. Verify the actual port number the LDAP server is using for TLS and specify that value. The default value is 636.
SSL	Select this check box to enable Secure Sockets Layer for socket connections to the host.
Enable SSL	Select this check box to use TLS for communications between the LDAP security adapter and the directory. Note the following: o The wallet file (ewallet.p12) must be stored in the **`keystore/truststore`** central location configured for Siebel Gateway, Siebel Application Interface, and other nodes. o Oracle LDAP client libraries are required to decipher the ewallet file, which is used to make secure connections (LDAPS) to the LDAP server. o The required Oracle LDAP client library files are: oraclepki.jar, osdt_core.jar, and osdt_cert.jar These library files must be located in the **`WEB-INF/lib`** directory for the Siebel Web application.
Wallet Password	wallet_password Specify the password you assigned to the wallet when creating the wallet.

   For information on configuring parameters for the LDAP security adapter, see *Configuring Security Adapters Using the Siebel Management Console* and *Parameters for Configuring Security Adapter Authentication*.
4. Restart the Siebel Server (if you are configuring LDAP on a Siebel Server).

Configuring Security Adapters Using the Siebel Management Console

This topic describes how to configure a Database, LDAP, or Custom security adapter using the Siebel Management Console after you have installed Siebel Business Applications. For information on installing and configuring Siebel Business Applications, see *Siebel Installation Guide* .

Note: When creating a security profile using the Siebel Management Console, the database security adapter is selected by default, indicating to use database authentication, but you can change this and select to use an LDAP or a custom security adapter as required. Database authentication is supported for development environments only, it is not supported for production environments.

You use the Siebel Management Console to do the following:

- Configure the parameters that set security adapter values. When you configure these parameters, the gateway must be running.
- Configure security adapter settings for gateway access authentication.
- Configure authentication parameters for Siebel application configuration, when configuring a Siebel Developer Web Client.

The Siebel Management Console sets authentication-related configuration parameters for Siebel Business Applications and Siebel Gateway authentication, but does not make changes to the LDAP directory. Make sure the configuration information you enter is compatible with your directory server.

When you specify LDAP as the security adapter type using the Siebel Management Console, the setting you specify provides the value for the Enterprise Security Authentication Profile (Security Adapter Mode) parameter. The Security Adapter Mode and Security Adapter Name (named subsystem) parameters can be set for Siebel Gateway, Siebel Enterprise Server, for a particular Siebel Server, for an individual Application Object Manager component, or for the Synchronization Manager component (for Siebel Remote).

When you specify LDAP as the security adapter mode, additional configuration parameters are defined for the particular LDAP security adapter. For example, the Security Adapter DLL Name (SecAdptDllName) parameter is automatically set when you specify LDAP as the security adapter mode.

CAUTION: If you want to configure a server component or a Siebel Server to use different LDAP authentication settings to those already configured at a higher level (that is, configured for the Siebel Enterprise or Siebel Server), then you must create a new LDAP security adapter. Otherwise, the settings you make reconfigure the existing security adapter wherever it is used.

The following procedure describes how to use the Siebel Management Console to configure security adapters (security profile) provided with Siebel Business Applications.

Note: You can set Enterprise (profile) parameters and Object Manager (Siebel Application Interface profile) parameters on Siebel Gateway using Siebel Server Manager or Siebel Management Console. However, you cannot set security profile parameters using Siebel Server Manager, you must use Siebel Management Console to set security profile parameters.For information about using Siebel Server Manager to edit parameters on Siebel Gateway, see *Siebel System Administration Guide* . For information about editing parameters on Siebel Gateway using the Siebel Management Console, see the following procedure.

To configure your security adapter using Siebel Management Console

1. Log in to the Siebel Management Console.
2. Click Profiles in the navigation menu, and then click Security.

   Existing security profiles are listed, if any.
3. Click Add (the plus (+) icon) to add a new security profile, or click the Clone button to clone an existing profile.

4. Specify a name for the profile.

   The security profile that is created on first login is named Gateway.
5. Click Add (the plus (+) icon) next to Data Sources to add a new data source.
6. Click Datasource, and configure your security adapter.
   - To configure a security adapter of type Database Authentication Basic mode:
     - Select the following option: Database Authentication (Basic mode for development only).
     - Specify the settings for the selected data source, as shown in *Parameters for Configuring Security Adapter Authentication*.
     - Click Next when prompted.
   - To configure a security adapter of type Database Authentication Advanced mode:
     - Select the following option: Database Authentication (Advanced mode).
     - Specify the settings for the selected data source, as shown in *Parameters for Configuring Security Adapter Authentication*.
     - Click Next when prompted.
   - To configure a security adapter of type LDAP:
     - Select the following option: Lightweight Directory Access Protocol (LDAP) Authentication.
     - Specify the settings for the selected data source, as shown in *Parameters for Configuring Security Adapter Authentication*.
     - Click Next when prompted.
   - To configure a security adapter of type Custom:
     - Select the following option: Custom Security Authentication (using Security SDK).
     - Specify the settings for the selected data source, as shown in *Parameters for Configuring Security Adapter Authentication*.
     - Click Next when prompted.
7. When you have specified all applicable settings, click Submit and save your changes to the profile.

Migrating from Database to LDAP Authentication

After you install Siebel Business Applications, the security adapter options provided for user authentication are a database security adapter, an LDAP security adapter, and a custom security adapter. If you want to implement LDAP 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 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*

- *About Siebel Security Adapters*
- *Features Not Available for Database Authentication*
- *About Authentication for LDAP Security Adapter*

Migrating from Database to LDAP Authentication

The steps to migrate a Siebel application from database authentication to LDAP authentication are outlined in *Process of Implementing LDAP Security Adapter Authentication*. 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 authentication from the Siebel database. Do not archive the following database accounts:
    - The default Siebel administrator account, SYSADMIN.
    - The default database account, for example, LDAPUSER, that is used by Siebel LDAP security adapter 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 security adapter and by adapters that comply with the Siebel Security Adapter Software Developer's Kit (SDK) version 3.0.

Depending on your security adapter or Web SSO implementation, you might have to configure the following:

- *Configuring the Application User*
- *Configuring Checksum Validation*
- *Configuring Secure Communications for Security Adapters*
- *Configuring the Shared Database Account*
- *Configuring Adapter-Defined User Name*
- *Configuring the Anonymous User*
- *Configuring Roles Defined in the Directory*

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. 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, 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 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.
- 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*). 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.

     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*.
3. For your Siebel security adapter, define the following parameter values for the security adapter's enterprise profile (such as LDAPSecAdpt) on the Siebel Gateway.

   - **Application User Distinguished Name (DN).** 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
     ```

- **Application Password.** Enter the application user password (unencrypted).

For more information on setting these parameters, see *Parameters for Configuring Security Adapter Authentication*. For Siebel Gateway authentication, define these parameters in the security profile. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

Application User and Password Expiration Policies

Typically, user administration in an LDAP 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 *Account Policies and Password Expiration*.

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, 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 a custom security adapter.

2. For the security adapter you are using, set the CRC Checksum parameter to the checksum value that is calculated earlier in this procedure.

   For information on setting configuration parameters, see *Parameters for Configuring Security Adapter Authentication*. For Siebel Gateway authentication, define these parameters in the security profile. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

   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 TLS to transmit data between a security adapter provided with Siebel Business Applications and an LDAP directory. Secure communications for the Siebel security adapter can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, custom (not database authentication)
- Web SSO authentication

Configuring TLS for the LDAP Security Adapter

This procedure describes how to configure TLS 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's used by the directory server.
2. Set the Wallet Password parameter for the LDAP security adapter (LDAPSecAdpt) to the password assigned to the Oracle wallet.

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, 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 security adapter as follows:

- The shared database account credentials can be specified in an attribute 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*.
- The shared database account credentials can be specified as profile parameters (Shared DB User Name and Shared DB Password) for the LDAP 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*.

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.
- Or, do the following:
  - Implement LDAP authentication for the gateway.
  - 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: Siebel Administrator is the default role.

The following topics describe in more detail how the LDAP server uses 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 the LDAP security adapter.

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*.
3. For each security adapter that implements this shared database account, specify values for the parameters shown in the following table.

Parameter	Value
Credentials Attribute	Enter the attribute in which the database account is stored in the directory, for example, `dbaccount`.
Shared Database Account Distinguished Name (fully qualified domain name)	Enter the distinguished name (including quotes) for the designated entry, such as: `"uid=SHAREDENTRY, ou=people, o=example.com"`

For information on setting configuration parameters, see *Configuring Security Adapters Using the Siebel Management Console* and *Parameters for Configuring Security Adapter Authentication*. For Siebel Gateway authentication, define these parameters in the security profile. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

Storing Shared Database Account Credentials as Profile Parameters

This topic describes how to configure a shared database account for an LDAP directory and how to store the database credentials for the account as parameters of the LDAP 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 the LDAPSecAdpt profile.

3. Configure the parameters shown in the following table for the LDAPSecAdpt profile.

Parameter	Value
Shared DB User Name	Enter the user name to connect to the Siebel database.
Shared DB Password	Enter the password to connect to the Siebel database

Note: You must specify a valid Siebel user name and password for the Shared DB User Name and Shared DB Password parameters. For more information about setting these parameters, see *Parameters for Configuring Security Adapter Authentication*.

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, 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 User Name Attribute Type 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 User Name Attribute Type.

Even if other requirements to administer user attributes in the directory through the Siebel client are met, you must also set the User Name Attribute Type 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 User Name Attribute Type 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
Security Adapter Mapped User Name	Select this check box.
Siebel Username Attribute	The attribute in which you store the Siebel user ID, such as uid (LDAP).
User Name Attribute Type	The attribute in which you store the adapter-defined user name, such as `telephonenumber`.

For information on setting Siebel Gateway configuration parameters, see *Server Parameters for Siebel Gateway*. For Siebel Gateway authentication, define these parameters in the security profile. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

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

   The Application Object Manager parameter to be populated is OM - Username BC Field.

   For information on working with Siebel business components, see *Configuring Siebel Business Applications* . For information on 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 User Name Attribute Type 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 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*.

The following procedure describes how to configure the anonymous user. The anonymous user for employee applications must be associated with an appropriate position and responsibility.

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 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.
3. Specify values for the following parameters, either when configuring the Siebel Application Interface profile (recommended) or by editing the application interface profile manually:
    - **Anonymous User Name.** 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`.
    - **Anonymous User Password.** Enter the password associated with the anonymous user.

    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.
4. If you use one anonymous user for most or all of your applications, then define the anonymous user in the Authentication section of the application interface profile. To override the default value for an individual application, list the Anonymous User Name and Anonymous User Password parameters in the Application section of the application interface profile, 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 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, 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 Roles Attribute parameter for the LDAP security adapter. For example, for the LDAP security adapter, define the following parameter:

   ```
   RolesAttributeType= attribute_in_which_roles_are_stored
   ```

   For information on setting configuration parameters for Siebel Gateway, see *Configuring Security Adapters Using the Siebel Management Console* and *Parameters for Configuring Security Adapter Authentication*. For Siebel Gateway authentication, define these parameters in the security profile. For Developer Web Client, define these parameters in the corresponding section in the application configuration file, such as uagent.cfg for Siebel Call Center.

Security Adapters and the Siebel Developer Web Client

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

- Application Object Manager (through the siebel.exe program)
- Application configuration file
- Authentication manager and security adapter
- Oracle LDAP Client (where applicable)

> **Note:** Siebel Business Applications support for the Siebel Developer Web Client is restricted to administration, development, and troubleshooting usage scenarios only. Siebel Business Applications does not support the deployment of this client to end users.

When you implement security adapter authentication for Siebel Developer Web Clients, observe the following principles:

- It is recommended to use the remote configuration option, which can help you make sure that all clients use the same configuration settings. This option is described later in this topic.
- Authentication-related configuration parameters stored in application configuration files on client computers, or stored in remote configuration files, must generally contain the same values as the corresponding parameters in the Siebel Gateway (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 Parameters*.
- 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*.
- In a security adapter authentication implementation, you must set the security adapter configuration parameter Propagate Change 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. (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 Parameters* and *Configuring LDAP Authentication for Developer Web Clients*.
- 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 IntegratedSecurity parameter 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*.

  > **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* and the *Siebel System Administration Guide* .

Sample LDAP Configuration

The following sample is an example of LDAP configuration information generated by the Siebel Management Console when you configure an LDAP security adapter for Developer Web Clients. For more information, see *Configuring Security Adapters Using the Siebel Management Console*. For information about setting Siebel configuration parameters, see *Siebel Application Configuration Parameters*.

```
[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 only to the Siebel Developer Web Client. The remote configuration option can be implemented in the following authentication strategies:

- Security adapter authentication: LDAP, 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]`, 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 following examples 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 in the preceding example. 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 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. 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 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 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 Salt User Password parameter is ignored if the Configure Web Single Sign-On 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 Salt User Password parameter, see *Parameters for Configuring Security Adapter Authentication*.
- **Database credentials password hashing.** When you are using security adapter authentication other than database authentication (LDAP 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 SHA-2 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.

For information about managing encrypted passwords in Siebel Application Interface configuration, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*. 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 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 authentication environment:
        - The authentication manager passes the user credentials, including the hashed password, to the LDAP security adapter.
        - The LDAP 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

Running the Password Hashing Utility

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 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*
2. Perform either or both of the following tasks, as appropriate:
   - *Configuring User Password Hashing*
   - *Configuring Password Hashing of Database Credentials*

   > **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 Management Console.

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*.

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 or LDAP 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 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, SHA-2) 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*.
- 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* and *Siebel Application Configuration Parameters*.

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*.

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*.
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 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. Create a Gateway security profile with the hash password enabled and SHA1 as the hash algorithm. For more information, see *Configuring Security Adapters Using the Siebel Management Console*.

5. 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).
   - For the LDAP security adapter (typically, LDAPSecAdpt):
     - Set the Hash User Password parameter to `TRUE`.
     - Set the Hash Algorithm parameter to `RSASHA1` (this is the default value).
     - (Optional) Set the Salt User Password parameter to `TRUE` to specify that salt values can be added to user passwords.
     - (Optional) Set the Salt Attribute Type parameter to specify the attribute that is to store the salt value.
6. Provide each user with the user name and the clear-text password for logging in.

Related Topics

About Password Hashing

Configuring Password Hashing of Database Credentials

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*.

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*.
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, 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 Security Adapter profile.

For information about required attributes in the directory, see *Requirements for the LDAP Directory*. 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 security adapter:
    - Set the Hash DB Password parameter to `TRUE`.
    - The hash algorithm is based on the setting you previously made for the Hash Algorithm parameter when you configured user password hashing.

Related Topics

About Password Hashing

Configuring User Password Hashing

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).

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*. For information about the password hashing options mentioned in the procedures in this topic, see *About Password Hashing*.

You can hash passwords using the SHA2 hashing algorithm. The following procedure describes how to hash passwords using the SHA-2 algorithm.

Hashing Passwords Using the SHA-2 Algorithm

The following procedure describes how to run the hashpwd.exe utility using the default password hashing algorithm, SHA-2.

To hash passwords using the SHA-2 algorithm

- To hash a password using the SHA-2 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
  ```

Setting the ConfigLdapAuthTimeout Parameter

The following procedures describe how to set the Configuration LDAP Authentication Timeout parameter (ConfigLdapAuthTimeout). You should configure this parameter to avoid an internal error being returned in the event of a return delay in the LDAP authentication response (that is, if the LDAP authentication response is not returned within 10 seconds). You can set ConfigLdapAuthTimeout at both server and component levels. The value set at the component level overrides the value set at the server level.

Note: The ConfigLdapAuthTimeout parameter is available in Siebel CRM 20.11 Update and later releases.

To set ConfigLdapAuthTimeout at the component level

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. Go to the Components subview and select the component that you want.
3. Go to the Parameters subview and query for the Configuration LDAP Authentication Timeout parameter (ConfigLdapAuthTimeout).
4. Change the value of ConfigLdapAuthTimeout from 10 seconds (which is the default value) to, for example, 200 seconds.
5. Restart the component for the changes to take effect.

To set ConfigLdapAuthTimeout at the server level

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. Go to the Parameters subview.
3. Query for the Configuration LDAP Authentication Timeout parameter (ConfigLdapAuthTimeout).
4. Change the value of ConfigLdapAuthTimeout from 10 seconds (which is the default value) to, for example, 200 seconds.
5. Restart the server for the changes to take effect.

To set ConfigLdapAuthTimeout parameter from the Server Manager

- Use the following command format to set the ConfigLdapAuthTimeout parameter from the Server Manager:

```
<Srvrmgr> change param ConfigLdapAuthTimeout = <value in seconds> for comp <component_name>
```

Setting the ConfigLdapFailoverTimeout Parameter

The following procedures describe how to set the Configuration LDAP Failover Timeout parameter (ConfigLdapFailoverTimeout). You should configure this parameter only if you have multiple LDAP servers configured to avoid a login delay in the event of an LDAP failover. You can set ConfigLdapFailoverTimeout at both server and component levels. The value set at the component level overrides the value set at the server level.

Note: The ConfigLdapFailoverTimeout parameter is available in Siebel CRM 21.1 Update and later releases.

To set ConfigLdapFailoverTimeout at the component level

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. Go to the Components subview and select the component that you want.
3. Go to the Parameters subview and query for the Configuration LDAP Failover Timeout parameter (ConfigLdapFailoverTimeout).
4. Change the value of ConfigLdapFailoverTimeout from 15 seconds (which is the default value) to, for example, 3 seconds.
5. Restart the component for the changes to take effect.

To set ConfigLdapFailoverTimeout at the server level

1. Navigate to the Administration - Server Configuration screen, then the Servers view.
2. Go to the Parameters subview.
3. Query for the Configuration LDAP Failover Timeout parameter (ConfigLdapFailoverTimeout).
4. Change the value of ConfigLdapFailoverTimeout from 15 seconds (which is the default value) to, for example, 3 seconds.
5. Restart the server for the changes to take effect.

To set ConfigLdapFailoverTimeout parameter from the Server Manager

- Use the following command format to set the ConfigLdapFailoverTimeout parameter from the Server Manager:

```
<Srvrmgr:Set Sevrer> change param ConfigLdapFailoverTimeout = <value in sec> for comp <component_name>
```

6 Single Sign-On Authentication

Single Sign-On Authentication

This chapter describes how to implement Web Single Sign-On (Web SSO) and Federated Single Sign-On (Federated SSO) for user authentication. It includes the following topics:

- *Supported Single Sign-On Solutions for Siebel Deployment*
- *About Web Single Sign-On*
- *About Implementing Web Single Sign-On*
- *Web Single Sign-On Authentication Process*
- *Requirements for Standards-Based Web Single Sign-On*
- *Set up Tasks for Standards-Based Web Single Sign-On*
- *Configuring the Session Timeout*
- *Configuring Siebel CRM and Oracle Business Intelligence Enterprise Edition for Web Single Sign-On*
- *Configuring Siebel Migration Application for Web Single Sign-On*
- *Web Single Sign-On Authentication Process When Using Siebel REST and Web Services in Portal Application*
- *About Implementing Federated Single Sign-On*
- *Federated Single Sign-On Authentication Process for Interactive User Interfaces*
- *Identity Provider-Initiated Single Sign-On Authentication Process*
- *About Oracle API Gateway Role in Single Sign-On Authentication Process*
- *Security Adapter Configuration When Single Sign-On is Enabled*
- *Configuring Single Sign-On with a Database Security Adapter*
- *Using OAuth with Siebel REST*

Note: If you are using the Siebel Self-Service Applications then see *Siebel Self-Service Application Deployment Guide* for additional information on Web Single Sign-On user authentication.

Supported Single Sign-On Solutions for Siebel Deployment

Siebel supports three types of HTTP access through which Siebel-provided services and data can be accessed: interactive user interfaces, Web services, and REST API.

Siebel deployment supports the following single sign-on (SSO) solutions:

1. **Web Single Sign-On (Web SSO).** This solution includes the following use case:
    - **Web SSO for interactive user interfaces.** See the following topics:

- *About Web Single Sign-On*
- *About Implementing Web Single Sign-On*
- *Web Single Sign-On Authentication Process*
- *Requirements for Standards-Based Web Single Sign-On*
- *Set up Tasks for Standards-Based Web Single Sign-On*
- *Configuring the Session Timeout*
- *Configuring Siebel CRM and Oracle Business Intelligence Enterprise Edition for Web Single Sign-On*

2. **Federated Single Sign-On with Security Assertion Markup Language (SAML).** In this solution, the user's single authentication token is trusted across multiple applications. For more information, see *About Implementing Federated Single Sign-On*. This solution includes the following use cases:

> **Note:** These use cases use Oracle Access Manager (OAM) and Oracle Access Gateway (OAG) for demonstration purposes only. Any equivalent solution from other vendors can also be used.

   - **SSO with SAML for interactive user interfaces.** For more information, see the following topics:
     - *Federated Single Sign-On Authentication Process for Interactive User Interfaces*
     - *About Oracle API Gateway Role in Single Sign-On Authentication Process*
   - **SSO when Siebel REST and Siebel Web services are used in a portal application.** For more information, see the following topics:
     - *Web Single Sign-On Authentication Process When Using Siebel REST and Web Services in Portal Application*
     - *About Oracle API Gateway Role in Single Sign-On Authentication Process*
   - **Identity provider-initiated SSO.** In this case, the portal application links to Siebel REST and Web services. The portal acts as an Identity Provider (IdP) and initiates federation. For more information, see the following topics:
     - *Identity Provider-Initiated Single Sign-On Authentication Process*
     - *About Oracle API Gateway Role in Single Sign-On Authentication Process*

> **Note:** For Siebel REST, you can use any Identity Provider (IdP) or gateway solution from any vendor. For more information, see *Siebel REST API Guide*

> **Note:** Siebel Open UI provides standards-based Single Sign-On (Web SSO and SAML based). Windows Integrated Authentication (WIA) is not supported.

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 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* .

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.

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 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*.

Web Single Sign-On and Silent Login

Silent login is typically not supported in Web SSO deployments where you want to start Siebel from an external application and both Siebel and the external application have different SSO credentials. In this case, there must be a Siebel session open for the external application to work with Siebel in SSO mode. However, if Siebel and the external application are both configured with the same SSO credentials, then silent login is supported and you will be able to start Siebel from the external application without being prompted for login credentials.

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 standards-based Web SSO solutions that meet the requirements listed in *Requirements for Standards-Based Web Single Sign-On*.

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:

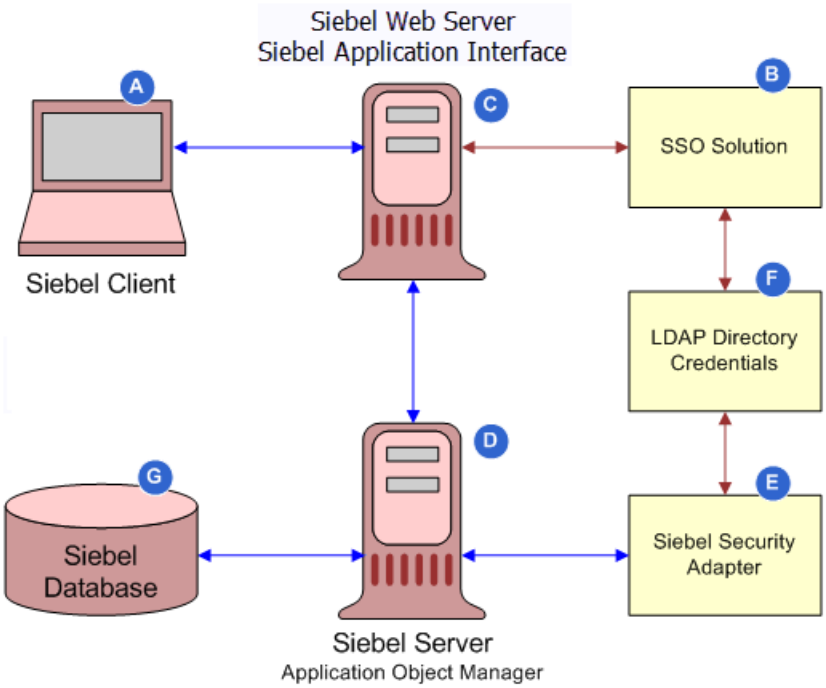
- **User specification source.** You must specify the source from which the Siebel Web Engine derives the user's identity key: a Web server environment variable or an HTTP request header variable.
- In addition, many options identified in *Security Adapter Deployment Options* can be implemented for Web SSO.

Related Topic

Requirements for Standards-Based Web Single Sign-On

Web Single Sign-On Authentication Process

The following image illustrates the user authentication process in a Web SSO environment.



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 (B) intercepts the user request and determines if the Siebel resource is protected.
    - If the resource is protected, the SSO authentication service checks for the user's session cookie.
    - 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 (B) 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 Application Interface on the Web server (C).

    Note: For LDAP standards-based Web SSO, a header variable must be used.

6. The Siebel Application Interface (C) passes the authenticated user's user name and the value for the Trust Token parameter to the security adapter (E). The user name can be the Siebel user ID or another attribute.
7. The security adapter (E) provides the authenticated user's user name to a directory (F), from which the user's Siebel user ID, a database account, and, optionally, roles are returned to the security adapter.
   In addition, the security adapter (E) compares the Trust Token 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 Siebel Application Interface; that is, from a trusted Web server (C).
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.

Related Topic

About Web Single Sign-On

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. 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 Siebel Application Interface 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 Application Interface.
- 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 Siebel Application Interface configuration, the fully qualified domain name and the port number for the application interface 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 User Specification parameter in the Siebel Application Interface profile. 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.
- The following parameters must be set in the Siebel Application Interface profile:
  - Configure Web Single Sign-On must be set to TRUE to implement SSO.
  - Trust Token must be set to HELLO, or another contiguous string of your choice.

    In 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 Siebel Application Interface configuration. In this case, you must specify the encrypted value. For more information, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*.

  - User Specification must be set to, for example, OAM_REMOTE_USER.

    > **Note:** OAM_REMOTE_USER is the header which carries the Siebel ID set by the SSO process.

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 Active Session Timeout Value (in seconds) parameter, see *About the Active Session Timeout Value Parameter*.

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 application interface configuration located in the AI_ROOT `\BIN` directory.
   b. Set the value of the Active Session Timeout Value 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 the previous step.

   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 steps 2 through 5 of this procedure for the Web server you have implemented.

For information about Federated or Security Assertion Markup Language-based SSO, see *About Implementing Federated Single Sign-On*.

Configuring Siebel CRM and Oracle Business Intelligence Enterprise Edition for Web Single Sign-On

Siebel CRM and Oracle Business Intelligence Enterprise Edition must be set up to use the same Web SSO and authentication server. Oracle Business Intelligence Enterprise Edition does not require credentials.

The Symbolic URL arguments that are required are shown in the following table.

Argument Name	Argument Required?	Argument Type	Argument Value	Append As Argument?	Sequence	Comment
IFrameLogin:Cmd	Y	Constant	Login	Y	1	None
Cmd	Y	Constant	Answers	Y	2	This argument indicates to display the *Answers* tool page in Oracle Business Intelligence Enterprise Edition.
PostRequest	Y	Command	PostRequest	Y	3	None
Style	Y	Command	IFramestyle="height: 768px; width: 1024px;"	Y	4	This argument is for determining the size of the iframe in Siebel Open UI.

Configuring Siebel Migration Application for Web Single Sign-On

Siebel Migration supports header based SSO and SAML assertion based SSO authentication. Several parameters must be configured in Siebel Management Console for Siebel Migration application to use Web SSO, SSO with SAML, or basic authentication. The required parameters are described in the following table. For more information about creating and deploying a Siebel Migration profile, see the *Siebel Installation Guide* .

Setting in Siebel Management Console	Section (Under Create Profile)	Comment or Description
Host Name	Database Information	Specify the host name for the database. Siebel Migration application uses this host name to establish the database connection. For example: `Host Name = <database_hostname>.FQDN`
Port Number	Database Information	Specify the port number of the database.
Authentication Type	Authentication	Specify the authentication type for the Siebel Migration application. Specify one of the following: • Basic Authentication • Single Sign-On
Authentication Host	Authentication	Specify the Siebel authentication host for authenticating the Siebel Migration application user. Siebel Migration application uses this URI to authenticate users

Setting in Siebel Management Console	Section (Under Create Profile)	Comment or Description
		when they log in to the application. The value will be the REST URI of the Siebel application. For example: `Authentication Host = https://<ApplicationInterface_hostname>.FQDN:<AI_https_port>`
User Specification	Authentication This option appears if you selected Single Sign-On Authentication.	Provide the user specification for SSO authentication. **Note:** This is the name of the http header which carries the identity for header based SSO. If you need only header based authentication, then set the appropriate value in this field. If you need SAML assertion based SSO, then set a dummy value in this field.
Assertion Specification	Authentication This option appears if you selected Single Sign-On Authentication.	Provide the assertion specification for SSO authentication. **Note:** This is the name of the http header, which carries the SAML assertion, when SAML based SSO is configured.
Identity Provider Logoff URL	Authentication This option appears if you selected Single Sign-On Authentication.	Provide the identity provider logoff URL for SSO authentication. **Note:** This is the Identity Provider Logoff URL that will be invoked when the user logs off from the application.
Parameter Name for Identity Provider Logoff Return URL	Authentication This option appears if you selected Single Sign-On Authentication.	Provide the parameter name for the identity provider logoff return URL for SSO authentication. **Note:** This is the Siebel Migration URL to navigate to, after logout.
Siebel Application Name for Data Administration	Other Information	Specify the Siebel application name that needs to be embedded in the Siebel Migration application.
Language	Other Information	Specify the language of the Siebel application that needs to be embedded in the Siebel Migration application.

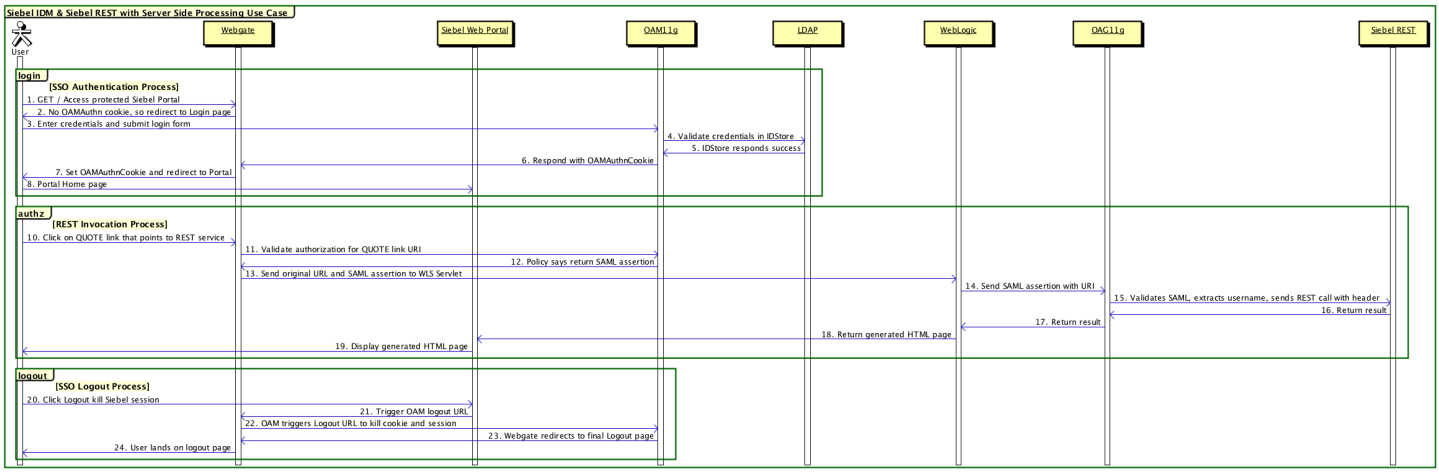
Web Single Sign-On Authentication Process When Using Siebel REST and Web Services in Portal Application

The figures in this topic show the typical steps in a Web SSO authentication process when Siebel REST and Web Services are invoked by a server that is part of a portal application. The process uses Oracle WebLogic server with Oracle Access Manager and Oracle API Gateway for *illustrative purposes*, but you can use any other Web application server with a SAML (Security Assertion Markup Language) identity provider solution and a Service Provider Gateway.

There are three parts in the Web SSO authentication process, which is shown in the following figures:

- SSO authentication process, see Steps 1 through 9.
- REST invocation process, see Steps 10 through 18.
- SSO logout process, see Steps 19 through 24.

The following image shows the Web SSO authentication process when using Siebel REST and Web Services in a portal application.



The steps in the Web SSO authentication process shown in this image (using Oracle WebLogic server with Oracle Access Manager and Oracle API Gateway for illustrative purposes) are:

1. **GET/Access protected Siebel Portal.** A non-authenticated user requests access to a protected Siebel Web Portal.
2. **Redirect to Login page.** There is no OAMAuthn cookie, so the user is redirected to the login page.
3. **Enter credentials and submit login form.** The user enters their credentials and submits the login form.
4. **Validate credentials in IDStore.** Oracle Access Manager validates the user credentials in the IDStore (Oracle LDAP or Oracle Unified Directory installed with Identity Store).
5. **IDStore responds success.** The IDStore returns success to Oracle Access Manager.
6. **Respond with OAMAuthnCookie.** Oracle Access Manager forwards the OAMAuthnCookie to Oracle Webgate.
7. **Set OAMAuthnCookie and redirect to Portal.** Oracle Webgate sets the OAMAuthnCookie and redirects the user to the portal.
8. **Portal Home page.** The user accesses the portal home page.
9. There is no step 9 in the Web SSO authentication process shown in the figures in this topic.
10. **Click on QUOTE link that points to REST service.** The user initiates the REST invocation process by clicking the QUOTE link, which points to the REST service.
11. **Validate authorization for QUOTE link URI.** Oracle Webgate invokes Oracle Access Manager to validate authorization for the QUOTE link URI.
12. **Return SAML assertion.** Oracle Access Manager returns SAML assertion to Oracle Webgate.
13. **Send original URL and SAML assertion to Oracle WebLogic Server.** Oracle Webgate sends the original URL and SAML assertion to the servlets hosted in the Oracle WebLogic server.
14. **Send SAML assertion with URI.** Oracle WebLogic server sends the URL with SAML assertion to the Oracle API Gateway.
15. **Validate SAML assertion.** Oracle API Gateway validates SAML assertion, extracts the user ID, sets the user ID in the request header, and sends a REST call with the user ID header.
16. **Return result.** Siebel REST returns the result to the Oracle API Gateway.
17. **Return result.** Oracle API Gateway returns the result to the Oracle WebLogic server.
18. **Return generated HTML page.** Oracle WebLogic server returns the generated HTML page to the portal.
19. **Display generated HTML page.** Siebel Web portal displays the generated HTML page to the user.

20. **Click Logout to terminate Siebel session** The user clicks Logout to terminate the Siebel session.
21. **Trigger Oracle Access Manager logout URL.** Siebel Web Portal invokes the Oracle Access Manager logout URL.
22. **Oracle Access Manager triggers logout URL to terminate the cookie and session.** Oracle Webgate invokes the Oracle Access Manager Logout URL to terminate the cookie and the session.
23. **Oracle Webgate redirects to final logout page.** Oracle Access Manager redirects Oracle Webgate to the final logout page.
24. **User lands on logout page.** The user lands on the logout page.

For more information about each step in this process, consult the supporting documentation for Oracle WebLogic, Oracle Access Manager, and Oracle API Gateway. For information about using OAuth with Siebel REST, see *Using OAuth with Siebel REST* and *Siebel REST API Guide* .

About Implementing Federated Single Sign-On

Browser based applications are suited to using single sign-on (SSO) authentication, which is cookie based. All configurations related to SSO (SSO cookie or Security Assertion Markup Language (SAML) token) must be performed outside Siebel. Siebel expects SSO authentication to be performed before the request reaches Siebel and looks at the HTTP request header injection for the subject. The Identity Provider (IdP) vendor must review this functional requirement. For SAML deployments, note that Siebel does not currently have a SAML validator or Assertion Consumer Service built into the product.

For customer use cases where multiple applications are federated in one SSO solution, the IdP, which acts as a service provider, validates the user credentials and passes SAML assertion to Siebel. If the request is directly sent to Siebel with a SAML token, Siebel currently does not have any way to validate it internally. This is required when Siebel has a SAML assertion consumer service by default.

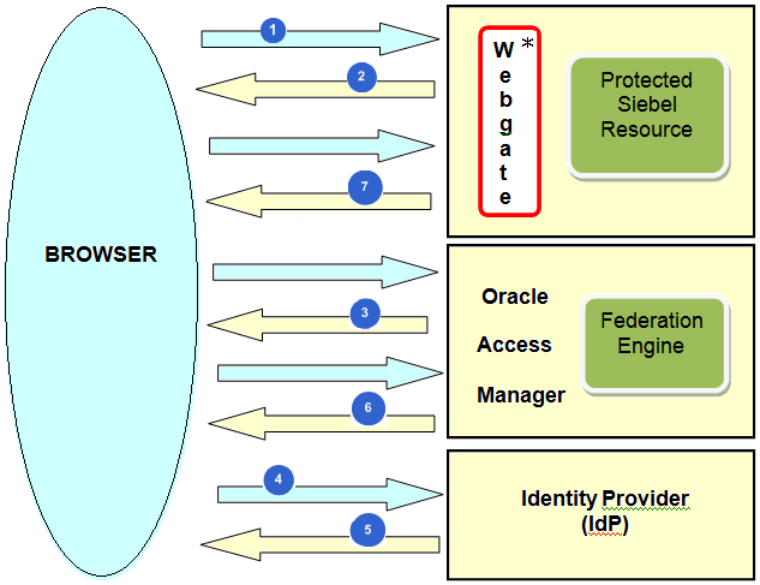
The SAML solution vendor can provide the external service provider or the service provider can be procured from open source solutions (for example: custom servlet). The implemented solution can use an external gateway to validate the SAML token/ID token/access token, and relay the request to Siebel (when successful) with the subject (part of the token) set in the request header. Solutions similar to this rely on the IdP and the use case that is to be implemented.

An example of an open source SAML authentication module, which can be implemented by customers, is the mod_auth_mellon module. This module provides the service provider and authentication function when used with Apache HTTPD. The mod_auth_mellon module is available only for Linux. For non-Linux platforms, such as Windows, the module must be compiled. The mod_auth_mellon module authenticates users against a SAML 2.0 IdP solution and grants access to directories depending on the attributes received from the IdP. For more information about the mod_auth_mellon module, see *https://github.com/Uninett/mod_auth_mellon*.

Note: The mod_auth_mellon module is not supported by Oracle.

Federated Single Sign-On Authentication Process for Interactive User Interfaces

The following image shows the user authentication process in a federated environment for interactive user interfaces. The process uses Oracle Access Manager (identity management solution) and Oracle Webgate (gateway) for *illustrative purposes*, but you can use any identity management solution and gateway.



* Oracle Access Manager-specific

The steps in the federated SSO authentication process shown in this image (using Oracle Access Manager and Oracle Webgate for illustrative purposes) are:

1. A non-authenticated user requests a Siebel interactive UI protected by Oracle Webgate.
2. Oracle Webgate intercepts the request and redirects the user to Oracle Access Manager for authentication.
3. The user enters their credentials, Oracle Access Manager determines whether the federation SSO should occur and invokes the federation engine to create a SAML AuthN request.

   Oracle Access Manager redirects the user to the tenant's identity provider (IdP) with the SAML AuthN request.
4. The tenant's IdP processes the SAML AuthN request and authenticates the user if required.
5. The user's IdP creates an assertion containing the user data and session data, and redirects the user with an assertion to Oracle Access Manager.
6. Oracle Access Manager invokes the federation engine to validate the assertion and map it to a local user record. Oracle Access Manager creates a local session for the user, performs authorization policy evaluation and redirects the user to the protected resource.
7. If the user is authorized by Oracle Access Manager, then Oracle Webgate grants access to the protected resource.

About Configuring Interactive User Interfaces for Federated Single Sign-On

The following prerequisites are required on the Siebel side before configuring identity federation. You must install and set up the components to suit your own business needs. Consult the supporting documentation of your chosen components (for example, Oracle Access Manager and Oracle API Gateway) for more information.

- Siebel Object Manager configured for SSO.
- The following parameters must be set in the Siebel Application Interface profile:
  - Configure Web Single Sign-On must be set to TRUE to implement SSO.
  - Trust Token must be set to HELLO, or another contiguous string of your choice.

    In 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 Siebel Application Interface configuration. In this case, you must specify the encrypted value. For more information, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*.

  - User Specification must be set to, for example, OAM_REMOTE_USER.

    > **Note:** OAM_REMOTE_USER is the header which carries the Siebel ID set by the SSO process.

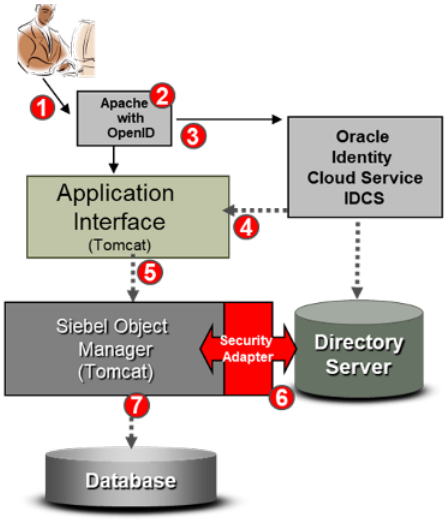
Single Sign-On between Siebel and Identity Cloud Service through SSO or Open ID

To support Siebel mainly as an on-premise application, to integrate with cloud applications, you need to authenticate Siebel and cloud application users one time, to allow them to access the on-premise or cloud applications in a seamless manner. To support such a single sign-on mechanism, you can use Oracle's Identity Cloud Service or other SSO services supporting OAuth. Other identity providers follow similar patterns to IDCS.

Siebel IP Integration with IDCS

The following figure describes the architecture for Siebel CRM integration with IDCS.

The Siebel CRM integration with IDCS architecture has this workflow:



1. A user tries to access the application.
2. The Apache reverse proxy with Open ID module intercepts the request (HTTPS/HTTP).
3. OpenID checks for the existence of a session cookie on the user's computer. If a valid cookie exists, then the OpenID populates the header variable and the UserID is passed to Siebel.
4. If no cookie exists, then the user is prompted for credentials using the IDCS form. The user enters the credentials which are passed to the Identity Cloud Service.
5. If the credentials are authenticated, then the IDCS session cookie is set and the OpenID sets the header variable and redirects the request to Siebel.
6. Siebel security adapter retrieves the database account and role information from the directory server.
7. Siebel session is started with the appropriate responsibilities.

Set Up the Apache Server

At the end of this setup, make sure that navigating to a protected directory prompts the user with credentials from IDCS, and, after providing valid credentials in IDCS, the user can access the protected URL.

Siebel Object Manager and User Requirements

Two object managers – one with database authentication and one for configuring single sign-on (IDCS in our example) – are needed for the setup process. As an example, enable Siebel CME Component Group and use ecommunications/enu for database authentication and eCommunicationsWireless/enu as IDCS authentication.

Note: The URLs are case sensitive.

To enable single sign-on for an object manager, the object manager must be configured for LDAP authentication. See *LDAP Configuration for Siebel CRM* for the high-level configuration for LDAP.

Note:

- Make sure that you have Siebel Administrator SADMIN privilege to access server administration screens.
- The environment should have GUESTCST configured with the appropriate responsibility to give the minimum number of views.
- GUESTCST should be configured in LDAP along with a database user account that can fetch information from user before the actual user logs into Siebel.

Configure Apache HTTP Server 2.x Server as Reverse Proxy

Note: To use this setup in a production environment, TLS is required for security, which requires certificates.

1. Modify apache24\conf\httpd.conf file using the changes in this procedure. Configure Apache to listen on SSL port 16660. Siebel server and Apache are configured on two separate machines.

   ```
   Listen10.248.120.16:16660
   ```
2. Enable reverse proxy by uncommenting the following lines in the httpd.conf file:

   ```
   LoadModule proxy_module modules/mod_proxy.so
   LoadModule proxy_html_module modules/mod_proxy_html.so
   LoadModule proxy_http_module modules/mod_proxy_http.so
   LoadModule proxy_http2_module modules/mod_proxy_http2.so
   ```
3. Enable `LoadModule xml2enc_module modules/mod_xml2enc.so`
4. Add the following lines before the protected directory:

   ```
   ProxyPass "/siebel" "http://<host>:16660/siebel"
   ProxyPassReverse "/siebel" "http://<host>:16660/siebel"
   ```
5. The protected URL should be eCommunicationsWireless/enu URL instead of the protected URL.

   ```
   #<Location /eCommunicationsWireless_enu>
   <Location /siebel> AuthType openid-connect Require valid-user
   </Location>
   Working httpd.conf with IP 2018
   ```

Configure Application Interface from Siebel Management Console (SMC)

1. Sign in on to `https://Siebel_Server:HTTPS_Port/siebel/smc`.
2. Go to **Profiles** > **Application Interface**.
3. Select the active profile in **Application Interface Profiles**.
4. Select **Applications** from the second tab in the Applications area.
5. Expand the **eCommunicationsWireless(enu)** tab.
6. Expand the **Enhanced Authentication** tab.
7. Select the **ConfigureWeb Single Sign-On (Web SSO)** checkbox and enter these values:
   - **TrustToken**: IDCSSIEBEL (This value must match the value in the Security adapter of the Siebel Enterprise Profile).
   - **UserSpec**: OIDC_CLAIM_sub (This is the HTTP header variable in which the OIDC passes the user name to Siebel).

Configure Object Manager to Enable LDAP Security Adapter

1. Go to **Administration** > **Server Configuration** > **Enterprises** > **Component Definition** using eCommunications_enu object manager.
2. Query for the Alias **eCommWirelessObjMgr_enu**
3. Change the values of the following parameters in **Component parameters**.
    - **Security Adapter Mode (SecAdptMode)**: LDAP (old value DB)
    - **Security Adapter Name (LDAPSecAdpt)**: LDAPSecAdpt (old value DBSecAdpt)
    - **EnforceSSL**: True

Set Up Security Adapter

1. Go to **Administration** > **Server Configuration** > **Enterprises** > **Profile Configuration** using eCommunications_enu object manager.
2. Query for the Profile **LDAP Security Adapter**.
3. Set the following parameters:
    - **Single sign-on**: True
    - **Trust Token**: IDCSSIEBEL (this value must match the value given in eapps.cfg file).

Siebel ships with HTTPS enabled. You need to provide SSL certificates. Ina production environment, we recommend using the HTTPS protocol.

Test the Configuration

Bounce the Siebel server, refresh application interface and start the httpd server whenever any changes are done to relevant components.

Known Issues in Siebel IDCS Integration

When a user is logged out, the cookie on the user's machine should be invalidated through scripting and the user should be navigated to the IDCS sign in page. By default, users are taken to Siebel's sign in page.

LDAP Configuration for Siebel CRM

Here's how to configure LDAP for Siebel:

1. Connect to Siebel server machine and launch the server manager (`srvrmgr` command in the console or terminal).
2. Execute the following commands on the server manager console. Servername parameter is the LDAP server name and port is LDAP port.

```
change param servername = "ldap_server.domain.com" for named subsystem ldapsecadpt
change param port=ldap_port for named subsystem ldapsecadpt
change param basedn="ou=people,o=example.com" for named subsystem ldapsecadpt
change param applicationuser="uid=appuser,ou=dirdemos,ou=people,o=example.com" for named subsystem
 ldapsecadpt
change param applicationpassword=LDAP_PASSWORD for named subsystem ldapsecadpt
change param sharedcredentialsdn="uid=mssql,ou=dbcreds,ou=people,o=example.com" for named subsystem
 ldapsecadpt
```

```
change param RolesAttributeType= physicalDeliveryOfficeName for named subsystem ldapsecadpt
```

3. Execute the following commands on the server manager console to change the security adapter for the required component (for example, `sccobjmhgr_enu` for call center). See the following example for eservice ENU application:

```
change param SecAdptMode=ldap for comp eCommWirelessMgr_enu
change evtloglvl SecMgrLog=5 for comp eServiceObjMgr_enu
change evtloglvl SecAdptLog =5 for comp eServiceObjMgr_enu
```

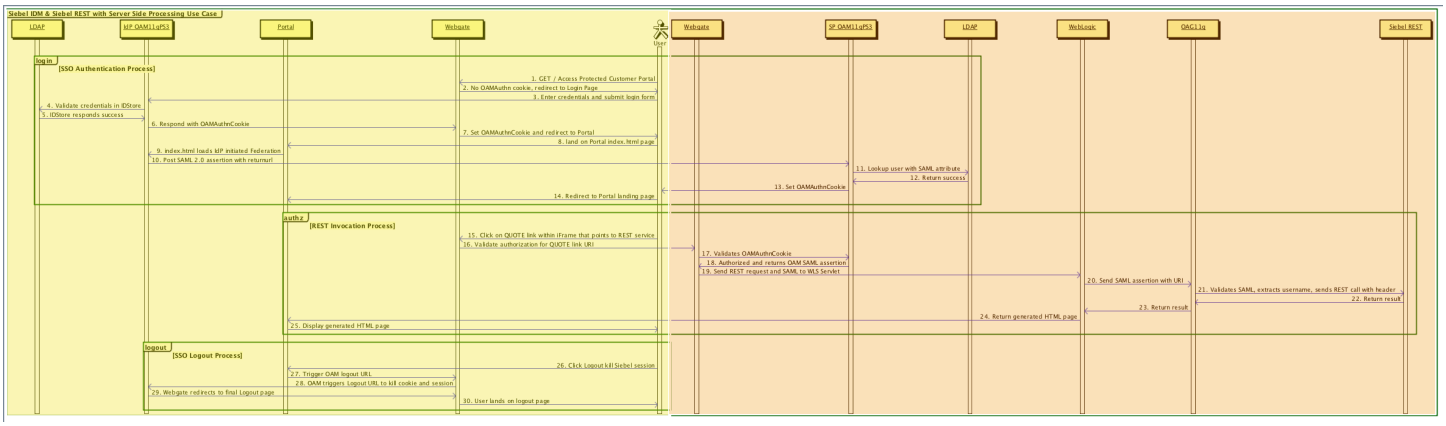
   The last two commands (optional) are to increase the logging levels for SecMgr and SecAdpt so that in case of any issues you can analyse a detailed log file.
4. Bounce Siebel services for the changes to take effect.
5. Update user name and password in the AI profile through SMC and deploy.

Identity Provider-Initiated Single Sign-On Authentication Process

The following images show the typical steps in an identity provider-initiated SSO authentication process where the portal application, which links to Siebel REST and Web services, acts as the identity provider (IdP) and initiates the federation. The process uses Oracle WebLogic server with Oracle Access Manager and Oracle API Gateway for *illustrative purposes*, but any Web application server with a SAML identity provider solution and a gateway for the service provider can be used.

> **Note:** For Siebel REST, you can use any identity provider (IdP) or gateway solution from any vendor. For more information, see *Siebel REST API Guide* .

The following image shows an identity provider-initiated SSO authentication process.



The typical steps in the IdP-initiated SSO authentication process shown in this image (using Oracle WebLogic server with Oracle Access Manager and Oracle API Gateway for illustrative purposes) are:

1. **GET/Access protected Customer Portal.** A non-authenticated user requests access to a protected Customer Web Portal.
2. **Redirect to Login page.** There is no OAMAuthn cookie, so the user is redirected to the login page.
3. **Enter credentials and submit login form.** The user enters their credentials and submits the login form.
4. **Validate credentials in IDStore.** Oracle Access Manager validates the user credentials in the IDStore (Oracle LDAP or Oracle Unified Directory installed with Identity Store).

5. **IDStore responds success.** The IDStore returns success to Oracle Access Manager.
6. **Respond with OAMAuthnCookie.** Oracle Access Manager responds with the OAMAuthnCookie to Oracle Webgate.
7. **Set OAMAuthnCookie and redirect to portal.** Oracle Webgate sets the OAMAuthnCookie and redirects the user to the portal.
8. **Land on portal index.html page.** The user lands on the portal's index.html page.
9. **index.html loads IdP initiated Federation.** The index.html page loads the IdP-initiated federation.
10. **Post SAML assertion with returnurl.** Oracle Access Manager posts SAML assertion with returnurl.
11. **Lookup user from the SAML attribute.** Oracle Access Manager checks with Oracle LDAP to look up the user from the SAML attribute.
12. **Return success.** Oracle LDAP returns success.
13. **Set OAMAuthnCookie.** Oracle Access Manager sets the OAMAuthnCookie.
14. **Redirect to portal landing page.** The user is redirected to the portal landing page.
15. **Click on QUOTE link within iFrame that points to REST service.** The user initiates the REST invocation process by clicking the QUOTE link, which points to the REST service.
16. **Validate authorization for QUOTE link URI.** Oracle Webgate validates authorization for the QUOTE link URI.
17. **Validates OAMAuthnCookie.** Oracle Webgate validates OAMAuthnCookie and sends the information on to Oracle Access Manager.
18. **Authorized and returns OAM SAML assertion.** Oracle Access Manager authorizes and returns OAMSAML assertion to Oracle Webgate.
19. **Send REST request and SAML to WLS Servlet.** Oracle Webgate sends the REST request and SAML to the Oracle WebLogic server.
20. **Send SAML assertion with URI.** Oracle WebLogic server sends the SAML assertion with URI to the Oracle API Gateway.
21. **Validate SAML, extracts username, sends REST with call header.** Oracle API Gateway validates SAML, extracts the user name, and sends a REST call with the header to Siebel REST.
22. **Return result.** Siebel REST returns the result to the Oracle API Gateway.
23. **Return result.** Oracle API Gateway returns the result to the Oracle WebLogic server.
24. **Return generated HTML page.** Oracle WebLogic server returns the generated HTML page to the portal.
25. **Display generated HTML page.** The portal displays the generated HTML page to the user.
26. **Click Logout to terminate Siebel session.** The user clicks Logout to terminate the Siebel session.
27. **Trigger OAM logout URL.** The portal invokes the Oracle Access Manager logout URL.
28. **OAM triggers Logout URL to terminate the session.** Oracle Webgate invokes the Oracle Access Manager logout URL to terminate the session.
29. **Oracle Webgate redirects to final Logout page.** Oracle Access Manager redirects Oracle Webgate to the final logout page.
30. **User lands on logout page.** The user lands on the logout page.

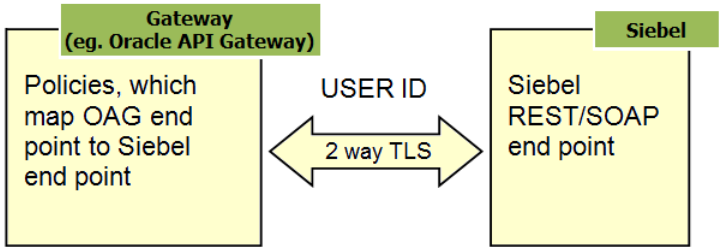
For more information about each step in this process, consult the supporting documentation for your Web application server (for example, Oracle WebLogic), identity management solution (for example, Oracle Access Manager), and gateway (for example, Oracle API Gateway).

> **Note:** For information about using OAuth with Siebel REST, see *Using OAuth with Siebel REST* and *Siebel REST API Guide* .

About Oracle API Gateway Role in Single Sign-On Authentication Process

The role of the gateway in the SSO authentication process is to act as the Assertion Consumer Service. The gateway validates the SAML token generated by the ID provider. All requests that are targeted to Siebel REST/SOAP must point to the gateway. The SOAP/REST end point is mapped to the gateway end point and vice versa. It is recommended to implement two-way TLS (Transport Layer Security) between Oracle API Gateway and Siebel REST as shown in the following image.

Note: You can use any gateway to process the assertion responses. For information about installing Oracle API Gateway, see *https://docs.oracle.com/cd/E39820_01/doc.11121/gateway_install_docs/content/install_gateway.html*.



Note: For information about using OAuth with Siebel REST, see *Using OAuth with Siebel REST* and *Siebel REST API Guide* .

Security Adapter Configuration When SSO is Enabled

Siebel offers multiple ways to communicate Siebel user identity to Siebel. Siebel understands user context only by the use of a user ID (for example: `SADMIN`). So if an Identity Provider (IdP) passes an email as an ID to Siebel (for example: `SADMIN@oracle.com`) , then it is Siebel's responsibility to map that ID to a Siebel user ID. Nothing changes for Siebel Object Manager when Single Sign-on (SSO) or federation is in place. The authentication flow remains the same in Siebel for both SSO with SAML (federated SSO with Security Assertion Markup Language) and non-SSO. A trust token is used instead of a password in SSO cases. The selection of a security adapter is guided by implementation constraints.

About Using an LDAP Security Adapter When SSO is Enabled

When using an LDAP security adapter, LDAP is implemented to map IDs using a single database user. This eliminates the need to maintain a large set of database users for Siebel. LDAP validates users by checking the mapped Siebel

database user credentials. In SSO cases, LDAP uses a trust token as the password and this password is common for all users.

- If different attributes are propagated from an IdP or used for login, then configure and use an adapter-defined user name. In the case of SSO with SAML, a *directory lookup* is required to map the adapter-defined user name to the Siebel user ID. For more information, see *Configuring Adapter-Defined User Name*.
- Optionally, LDAP can be used to store Siebel user responsibilities as roles in a directory attribute instead of in the Siebel database (for example, if you want to share the information). For more information, see *Configuring Roles Defined in the Directory*.

For production environments, it is recommended that you use an LDAP security adapter to maintain Siebel users.

About Using a Database Security Adapter When SSO is Enabled

When using a Database security adapter, the adapter is implemented to map IDs using a single database user. This approach eliminates the need to maintain a large set of database users for Siebel. Users are validated by checking the mapped Siebel database user credentials. In SSO cases, a trust token is used as the password and this password is common for all users.

> **Note:** No directory support is available when using a Database security adapter. As a result, the Identity Provider (IdP) must pass the exact Siebel user ID as an ID to Siebel (for example: SADMIN).

Configuring Single Sign-On with a Database Security Adapter

As of Siebel CRM 20.10 Update, you can use a database security adapter in Single Sign-On (SSO) mode without LDAP. Prior to Siebel CRM 20.10, you could only use an LDAP security adapter for SSO. The tasks involved in configuring a database security adapter to support SSO are as follows:

1. *Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode*
   a. *Enabling JDBC Over TLS* - this is a prerequisite to configuring SSO with a database security adapter, where an encrypted database connection (over TLS) is required for a secure production environment.
2. *Configuring Object Manager's Database Security Adapter in Advanced Mode*

Using database authentication without SSO is not recommended for production environments.

Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode

Create a Siebel Gateway security profile with Database Authentication Advanced mode when Single Sign-On (SSO) is supported. The instructions are the same for SSO and non-SSO, except for Step 5g in the following procedure:

The steps in this procedure are the same whether you're adding a new Siebel Gateway profile or updating an existing Siebel Gateway profile via safe mode to use Database Authentication Advanced mode.

> **Note:** Only one security profile can be set up for a gateway.

Create a Siebel Gateway Security Profile

Here's how to create a Siebel Gateway security profile with Database Authentication Advanced mode:

1. Make sure JDBC is enabled over TLS as shown in *Enabling JDBC Over TLS*.
2. Sign in to the Siebel Management Console and configure CGHostURI as always.
3. Select **Profiles** > **Security**.
4. Select Add (the plus (+) icon) and then enter the name of the security profile in the Create Profile field (for example: GWProfile).
5. In the Data Sources section on the Data Sources tab:
    a. Enter the name of the data source in the Name field.
    b. For Type, select the **Database Authentication Advanced** mode option.
    c. Select the **SQL Style of Database** option. The options are: Oracle Database Enterprise Edition, Microsoft SQL Server, and IBM DB2.
    d. Enter the database Connection String information. The following table shows how to enter the database Connection String information according to the selected SQL Style of Database.

> **Note:** The database Connection String can be one of the following: any SQL Style of Database, Oracle Data Guard, or Oracle RAC (Real Application Clusters).

SQL Style of Database	TCP/TCPS	Connection string
Oracle Enterprise Edition	TCP	`(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP) (HOST = slc1****.oracle.com) (PORT = 1*5*))) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = qahlp1) ) )` **Note:** Copy the connection string from tnsname.ora file.
Oracle Enterprise Edition	TCPS	`(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS) (HOST = slc1****.oracle.com) (PORT = 2*8*))) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = test) ) )` **Note:** Copy the connection string from tnsname.ora file.
Microsoft SQL Server	TCP	`[host]:[port];databaseName=[databaseName];`

SQL Style of Database	TCP/TCPS	Connection string
Microsoft SQL Server	TCPS	`[host]:[port];databaseName=[databaseName];encr trustServerCertificate=true;`
IBM DB2	TCP	`[host]:[port]/[databaseName]`
IBM DB2	TCPS	`[host]:[port]/[databaseName]:sslConnection=true;`

e. Enter the Table Owner (for example: ORAHLPP).
f. (Optional) If user password hashing is required, then select the Hash User Password checkbox.
g. Select the Configure Web Single Sign-On (Web SSO) checkbox to set the SSO related parameters described in the following table.

> **Note:** Deselect this option for non-SSO support.

Parameter	Description
Trust Token	Specify the trust token, which is used as the password when running in SSO mode. The value entered in this field must match the Trust Token value (alias DBSecAdpt_TrustToken) configured with the object manager's database security adapter. For more information, see *Configuring Object Manager's Database Security Adapter in Advanced Mode*.
Shared DB User Name	Specify the database user name to connect to the Siebel database.
Shared DB Password	Specify the password for the Shared DB Username parameter.

h. Select **Next** to go to the Security Information screen.

6. In the Basic Information section on the Security Information tab:
   - Ensure that **Database Authentication Advanced Mode** is selected.
   - Ensure that **DBsecAdpt** is specified in the Security Adapter Name field.
   - Select the Database Security Adapter Data Source (for example: GWProfile).
   - Enter Authorization Roles (in comma-separated format). The Siebel Administrator is the default role.
7. In the Testing section on the Security Information tab, enter the database User Name and Password, where password is one of the following, and then Select Submit to test and save the profile.
   - Enter the trust token as the password if the SSO option is selected.
   - Enter the database password if the SSO option is *not* selected.

Enabling JDBC Over TLS

Enabling JDBC over TLS is a prerequisite to configuring SSO with a database security adapter, where an encrypted database connection (over TLS) is required for a secure production environment.

The procedure to enable JDBC over TLS is different depending on the selected database type, which can be one of the following:

- *Oracle Database Enterprise Edition*
- *Microsoft SQL Server*
- *IBM DB2*

Oracle Database Enterprise Edition

To enable JDBC over TLS for Oracle Database Enterprise Edition:

1. Copy over the wallet directory containing the wildcard certificates from the Oracle database server location and put the directory into a new wallet folder location on the client, for example, as follows: `<path>\network\admin\wallet`.
2. Make sure all files in the wallet folder can be read by the end user running sqlplus.
3. Modify the client sqlnet.ora as follows:

```
<-- Changes required in client sqlnet.ora -->
WALLET_LOCATION =(SOURCE =(METHOD = FILE)(METHOD_DATA =(DIRECTORY = <path>\network\admin\wallet)))
SQLNET.AUTHENTICATION_SERVICES = (TCPS,NTS,NONE)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION=1.2
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
```

4. Add the following connection string to tnsnames.ora:

```
<-- Changes required in tnsnames.ora ->
ora19_tls = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST = slc1****.oracle.com)(PORT
 = 2*8*)))
(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = test)) )
```

5. Connect using sqlplus and test it:

```
sqlplus <username>/<password>@ora19_tls
```

6. Get the CA Certificate file from the Oracle Server.
7. Import the CA file into the trust store used by the Gateway:

```
keytool -import -trustcacerts -file <Oracle CA file path> -keystore <truststorepath
\siebeltruststorename.jks>
```

Microsoft SQL Server

To enable JDBC over TLS for Microsoft SQL Server:

1. Get the CA Certificate file from the SQL server.
2. Import the CA file into the trust store used by the Gateway:

```
keytool -import -trustcacerts -file <sql server CA file path> -keystore <truststorepath
\siebeltruststorename.jks>
```

IBM DB2

To enable JDBC over TLS for IBM DB2:

1. Get the CA Certificate file from the DB2 server.
2. Import the CA file into the trust store used by the Gateway:

```
keytool -import -trustcacerts -file <DB2 CA file path> -keystore <truststorepath
\siebeltruststorename.jks>
```

Configuring Object Manager's Database Security Adapter in Advanced Mode

The following procedure shows how to configure the object manager's database security adapter in Database Authentication Advanced mode when Single Sign-on (SSO) is supported. Using database authentication without SSO is not recommended for production environments.

To configure the object manager's database security adapter in Advanced mode

1. After the security profile has been created, as shown in *Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode*, create the enterprise and server profiles and deploy them if not already done so.
2. Connect to the server manager and set the following parameter values for the component of interest: `SecAdptMode=DBSSO` and `SecAdptName=DBSecAdpt`.

```
<-- Component Parameters -->
change param SecAdptMode=DBSSO for comp <component name>
change param SecAdptName=DBSecAdpt for comp <component name>
```

3. Add the database adapter advanced subsystem parameter values described in the following table for SSO support. These parameters are required in addition to other existing parameters.

```
<-- Named subsystem "dbsecadpt" advanced parameters -->
change param DBSecAdpt_SingleSignOn=TRUE for named subsystem dbsecadpt
change param DBSecAdpt_TrustToken=<value> for named subsystem dbsecadpt
change param DBSecAdpt_SharedDBUsername=<DB user name> for named subsystem dbsecadpt
change param DBSecAdpt_SharedDBPassword=<DB password>for named subsystem dbsecadpt
```

Parameter	Default Value	Description
Single Sign On (alias DBSecAdpt_SingleSignOn)	FALSE	(TRUE or FALSE) If TRUE, then the security adapter is used in Web SSO mode instead of using security adapter authentication. This parameter applies only in a Web SSO environment..
Trust Token (alias DBSecAdpt_TrustToken)	<empty>	The adapter compares the TrustToken value provided in the request with the value stored with the subsystem. If they match, then the application object manager accepts that the request has come from the Application Interface, which is trusted.

Parameter	Default Value	Description
Shared DB Username (alias DBSecAdpt_SharedDBUsername)	<empty>	User Id to connect to the Siebel database.
Shared DB Password (alias DBSecAdpt_SharedDBPassword)	<empty>	Password associated with the Shared DB Username parameter.

4. Restart the Siebel service.

Configuring the Application Interface Profile for Single Sign-On

The following procedure shows how to configure an Application Interface profile for Single Sign-On (SSO).

To configure the Application Interface profile for SSO

1. Log in to Siebel Management Console.
2. Click Profiles in the navigation menu, and then click Application Interface.

   Existing Application Interface profiles are listed, if any.
3. Select the profile that you want to modify, and then click Edit.

   Alternately, click Add (the plus (+) icon) to create a new application interface profile.
4. To set the SSO related parameters described in the following table, do one of the following for REST or UI Applications as required:
   - **For REST.** Go to the Basic Information tab, Authentication section, then the REST Inbound Authentication section, and select the Single Sign-On option under Authentication Type.
   - **For UI Applications.** Go to the Applications tab, then the Enhanced Authentication section of the application that you want, and select the Configure Web Single Sign-On (Web SSO) check box.

Parameter	Description
Trust Token	Specify the trust token, which is used as the password when running in SSO mode. The value entered in this field must match the Trust Token value (alias DBSecAdpt_TrustToken) configured with the object manager's database security adapter.
User Specification	Specify the user specification for SSO authentication, which will be used as the name of the http header which carries the Siebel USERID for header based SSO.

5. Click Submit to save your changes to the profile, and then deploy the profile.

Using OAuth with Siebel REST

For Siebel Inbound and Outbound REST OAuth, certain customizations must be made as described in the following topics:

- *Using OAuth with Siebel REST Inbound Web Services*
- *Configuring OAuth Support for Siebel REST Outbound Connections (21.8 to 22.8)*

Using OAuth with Siebel REST Inbound Web Services

This topic shows how to configure inbound REST requests using OAuth 2.0.

How to Configure Inbound REST Requests Using OAuth 2.0

You can use OAuth 2.0 protocol in the Siebel REST API to send authentication information to access Siebel resources. In general, the Siebel REST API layer contacts the OAuth server over a secure channel (for example, HTTPS) to validate the access token received or to obtain additional token information. The Siebel application supports only the introspection method of validating incoming access tokens. The following prerequisites are required on the Siebel side before configuring OAuth for authentication. You must install and set up the components, including OAuth components, to suit your own business needs.

- The Siebel Object Manager must be configured for SSO when OAuth is enabled for authentication. The related security adapter is also required in SSO mode. In 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 TrustToken parameter defined for the custom security adapter. For more information about configuring SSO, see *Siebel Security Guide*.
- The Siebel REST API layer contacts the OAuth server over a secure channel to validate or get token information. To enable HTTPS, the required certificates from the OAuth server must be installed in the environment where the Siebel REST API is hosted.

Note: Siebel supports only the introspection method when validating incoming tokens. Using the signature method to validate incoming tokens is unavailable. However, if you are using JWT tokens and the signature method is required for validation, then you must do the following:

- Configure Siebel REST API for SSO. For more information about configuring SSO, see *Siebel Security Guide*.
- Configure the OAuth token validation using an API Gateway. This must be done before the request reaches the Siebel application. For more information on Oracle API Gateway, see your supporting documentation.

The following topics discuss the procedure to configure Siebel REST API for OAuth authentication and a sample client to generate token and access Siebel REST API with generated token.

- Siebel Object Manager setup with SSO
  - Setting Siebel EAI Object Manager For LDAP/SSO
  - Setting Siebel EAI Object Manager For DB/SSO
- Configuration of OAuth Client And Introspection Client in OAuth Server
  - Configure and register OAuth Client in OAuth Server

    - Configure and register Introspection Client in OAuth Server
- Configuration of Application Interface (AI) For OAuth Configuration
    - Configuring OAuth As Authentication Type for REST Inbound
- Client application using Siebel REST with OAuth
    - Generate Token
    - Validate/Introspect the token
    - Access Siebel REST API with the generated Token

Note: Performing these actions will require two system restarts at different points.

Setting Siebel EAI Application Object Manager for LDAP/SSO

To setup Siebel REST API Inbound authentication, we need to setup a Siebel EAI Object Manager (EAIObjMgr_<lang>) that will be using LDAP/SSO using the *LDAPSecAdpt* profile. Follow the below steps for LDAP/SSO setup.

1. Login to Siebel Call Center application or any DB authentication application and navigate to Site Map >> Administration - Server Configuration >> Profile Configuration.
2. Query for the *LDAPSecAdpt* profile to view the LDAP profile parameters.
3. Provide the *LDAPSecAdpt* profile parameters depending on your LDAP directory server.

   Example: LDAPSecAdpt Profile Parameters for LDAP Authentication

Parameter	Description
Port	LDAP Port
BaseDN	dc=xx,dc=xx,dc=xx
ApplicationUser	cn=username,dc=xx,dc=xx,dc=xx
ApplicationPassword	password
ServerName	LDAP Server Name
SharedCredentialsDN	cn=SharedUser,cn=username,dc=xx,dc=xx,dc=xx
CredentialsAttributeType	mail
UsernameAttributeType	uid
SharedDBUsename	DB Username
SharedDBPassword	DB Password
PasswordAttributeType	userPassword

4. Once the LDAP parameters are entered, make sure to enable Single Sign On (SSO) by adding below parameters.

   Example: SSO Parameters For LDAPSecAdpt For SSO Authentication

Parameter	Description
SingleSignOn	TRUE
TrustToken	ABCDE (This is an example string only. Use a string that meets your business requirements.)

5. Make sure to enable the EAI component group and ensure it is online. Once the SSO parameter is setup, connect to Siebel Server Manager and enable the *LDAPSecAdpt* profile for the EAI Object Manager (EAIObjMgr_<lang>).

   Example: Server Manager Command To Make EAI Object Manager Use LDAP/SSO

```
change param SecAdptName=LDAPSecAdpt for comp EAIObjMgr_enu
change param SecAdptMode=LDAP for comp EAIObjMgr_enu
```

6. Restart the Siebel service.

Setting Siebel EAI Application Object Manager for DB/SSO

As of the Siebel CRM 20.10 update, you can use a database security adapter in Single Sign-On (SSO) mode without LDAP. Prior to Siebel CRM 20.10, you could only use an LDAP security adapter for SSO. The tasks involved in configuring a database security adapter to support SSO are as follows.

If you would like to use DB/SSO using the *DBSecAdpt*, then you can setup Siebel REST API Inbound authentication with Siebel EAI Object Manager (EAIObjMgr_<lang>) using DB/SSO starting from Siebel 20.10 and later versions. Follow the steps from *Siebel Security Guide* in the section “Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode”, and once completed, perform the below steps to enable EAI Object Manager for the *DBSecAdpt* profile in advanced mode:

1. After the security profile has been created, as shown in the “Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode” section, create the enterprise and server profiles and deploy them if not already done.
2. Connect to the server manager and set the following parameter values for the component of interest (EAIObjMgr_<lang> for example): SecAdptMode=DBSSO and SecAdptName=DBSecAdpt.

```
<-- Component Parameters -->
change param SecAdptMode=DBSSO for comp EAIObjMgr_enu
change param SecAdptName=DBSecAdpt for comp EAIObjMgr_enu
```

3. Add the database adapter advanced subsystem parameter values described in the following Server Manager commands for SSO support. These parameters are required in addition to other existing parameters.

```
<-- Named subsystem "dbsecadpt" advanced parameters -->
change param DBSecAdpt_SingleSignOn=TRUE for named subsystem dbsecadpt
change param DBSecAdpt_TrustToken=<value> for named subsystem dbsecadpt
change param DBSecAdpt_SharedDBUsername=<DB user name> for named subsystem dbsecadpt
change param DBSecAdpt_SharedDBPassword=<DB password>for named subsystem dbsecadpt
```

4. Restart the Siebel service.

For more information about configuring SSO, see *Siebel Security Guide*.

Configure and Register OAuth Client in OAuth Server

This document uses IDCS as the OAuth Server and it is for illustration purposes. This feature is independent of the OAuth Server. For this, create a confidential application with Introspect disabled using Oracle Identity Cloud Service (IDCS).

Prerequisites:

1. Make sure to have a OCI Tenancy and a Federation configured in your tenancy.
2. Login to your OCI Tenancy and go to Hamburger Menu >> Identity & Security.
3. Click **Federation**.
4. In the Federation, you should see "OracleIdentityCloudService" and Type as IDCS with status of "Active".
5. Click **OracleIdentityCloudService**.
6. On the OracleIdentityCloudService page, the console URL to access IDCS will be shown which would be the admin URL that should be clicked to access the IDCS login page.

Note: Please use your respective Federation service vendor documentation to create confidential application. For IDCS, you can use the *IDCS documentation*.

Steps to Create Confidential Application in IDCS Without Introspect Option for use as OAuth Client

1. Log in to IDCS Admin Console using the console URL picked from the Federation from OCI tenancy.
2. Open the Applications page.
3. This will open the Add Application window and select "Confidential Application" from the same.
4. Provide any name for the Confidential Application. Example: Siebel Postman OAuth Client
5. Click **Next** and select the "Configure this application as a client now" option.
6. Once this option is selected, it will expand and show the list of parameters that need to be configured. For Allowed Grant Types, select/check Client Credentials and Authorization Code. For the Redirect URL, provide the application URL where the user will be redirected after authentication and make sure to provide the absolute URL.
7. In the same page, go to the Token Issuance Policy section and narrow down on Resources and add a scope and provide the Resource name as "Siebel Postman OAuth Client" and Protected as "No" and the scope in the form of https://AIHostname:AIHTTPSPort/siebel/v1.0/data
8. Click **Next** and in the resources page, define scope to add workflow, service, and data.
9. Click **Next** and in the web tier policy page, skip the option to configure web tier policy.
10. Click **Next** and on the authorization page, click **Finish**.
11. Once you click Finish, you will see a pop-up stating that the application has been added. Along with this, you will get the Client ID and Client Secret that will be used by the OAuth client.
12. Click **Close** and then select the Activate button to activate the application.

Once this is done, your Siebel OAuth Client Application configuration is completed on the IDCS.

Inbound REST Requests and OAuth Scopes

The Siebel application will honor the OAuth scope (the types of APIs you may call and operations you may perform for incoming REST requests) that you supply and that you have defined in your OAuth server. When you get your OAuth token, it will define the scope you have defined and pass that to the Siebel application. You can define the scope of your operation from general to specific. If you are using a scope of GET, for example, you would use the same token you got from your Oauth server for any GET request. If you have refined the scope further by adding the data API for GET operations, then you use your Oauth token for all GET data operations. As shown below, you can define your scope to gradually become more restrictive. When the incoming REST request is read, the Siebel application verifies the scope

for the operations provided with your OAuth token, with the actual request to make sure that the REST request it has received is authorized to perform the operations it is requesting.

These are simple examples of scopes you may have defined in your OAuth server:

> **Note:** This example shows the data API, but this is true for all other Siebel CRM REST APIs such as service, workflow and others. These examples show a single API, but you can pass more than one API as scope by separating them with a space.

Scope: “data service workflow” sends three APIs. You can refine each one individually such as:

```
Scope: data.Account.Account workflow.<workflowname>
```

Here the scope is that we are calling the GET method for the data resource. This scope allows the REST request to get data from any resource and is wide open.

GET.data

Now the REST request is limited to getting data from the Account resource. Account is the Business Object and has many possible child Business Components. This allows getting data from any of those children.

GET.data.Account

This is the final stage where we are restricting reading data from only the Account Business Component as a child of the Account Business Object.

GET.data.Account.Account

The same can be done for the other types of HTTP methods such as POST, PUT, DELETE.

This restricts updates to only the Account BC under the Account BO.

POST.data.Account.Account

This restricts inserting records to only the Account BC under the Account BO.

PUT.data.Account.Account

This restricts deleting records to only the Account BC under the Account BO.

DELETE.data.Account.Account

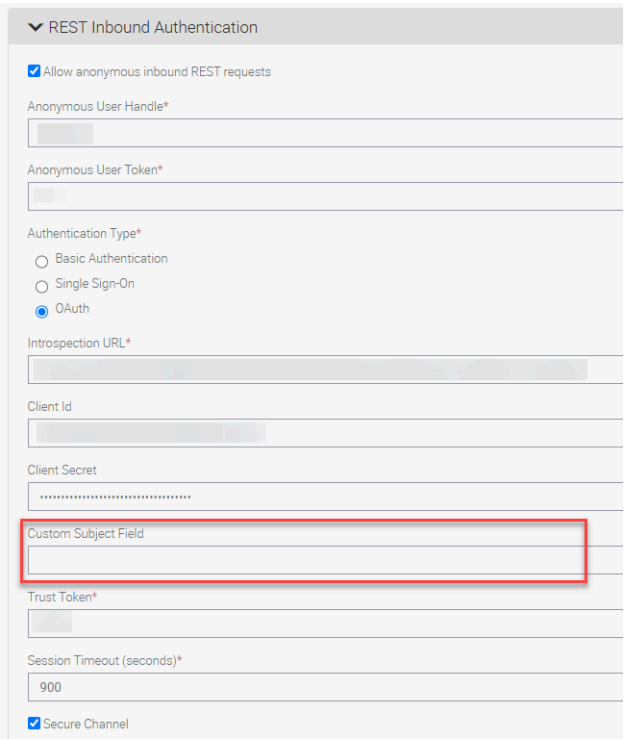
Configuring Application Interface To Use OAuth For Siebel REST Inbound Authentication

Next, the Application Interface needs to be configured with the SSO parameter for the IDCS integration to use OAuth for REST Inbound.

1. Select the correct Application Interface profile and click on the Edit (pencil) icon.
2. Go to the first tab which will show the REST Inbound parameters enabled in the Application Interface (AI).

3. Configure the REST API oAuth authentication using the following parameters:
   - **Introspection URL**: Required field. This is the OAuth introspection URL.
   - **Client ID:** Required field. This is the client ID for the IDCS Confidential Application created with Introspect enabled.
   - **Client Secret:** Required field. This is the client secret for the IDCS Confidential Application created with Introspect enabled.
   - **Custom Subject Field:** Optional field that allows you to specify a field created by an OAuth server to hold the Subject attribute to use in validation. Typically, this is the username or sub field, but some OAuth servers create their own. If you leave this field blank the sub or username or user_id field will be used. If this field has a value, subject information will be taken from this custom field from the OAuth token. Specifying which field to use allows flexibility in the OAuth server choice.
   - **Trust Token:** Required field. The Trust Token value must be the same as the security adapter *TrustToken* parameter value.
   - **Session Timeout (seconds):** Required field. This is the REST Object Manager session timeout.
   - **Secure Channel:** Set this parameter to true and import the Introspection URL's CA certificate into the Application Interface truststore. Deselect this check box when the Introspection URL's CA certificate is not available in the Application Interface truststore, however Oracle does not recommend this option.

     > **Note:** Import the Introspection URL CA certificate into the Application Interface truststore. As part of the Siebel AI/SAI profile configuration updates in 26.7, certificate validation is always enabled by default. The Secure (ValidateCertificate) property is no longer used in AI/SAI profiles, and this option is no longer configurable.If you maintain custom or copied seeded AI/SAI profile JSON files, remove "ValidateCertificate": true, entry before creating profiles from the seeded profile JSON file. This cleanup is required because profile creation can fail when stored seeded profile data still contains this deprecated property. Oracle-delivered out-of-the-box seeded profiles in the updated build have already been corrected. This does not affect creating new profiles from SMC or using existing AI/SAI profiles that were already created.



4. After checking the Secure Channel checkbox, you should import the RootCA certificate of your IDCS federation into the AI trust store in order for the communication to be secure. This is a mandatory step that must be followed.
   a. Copy the rootCA certificate of your Federation and keep it in a directory on your AI server, for example, C:/Certs/rootCA.crt.
   b. Go to $SIEBEL_ROOT/ai/jre/bin and execute the below keytool command to import the rootCA certificate into the truststore of the AI.

      ```
      keytool -import -alias rootCAFederation -file C:/Certs/rootCA.crt -keystore $SIEBEL_ROOT/ai/applicationcontainer_external/siebelcerts/siebeltruststore.jks
      ```

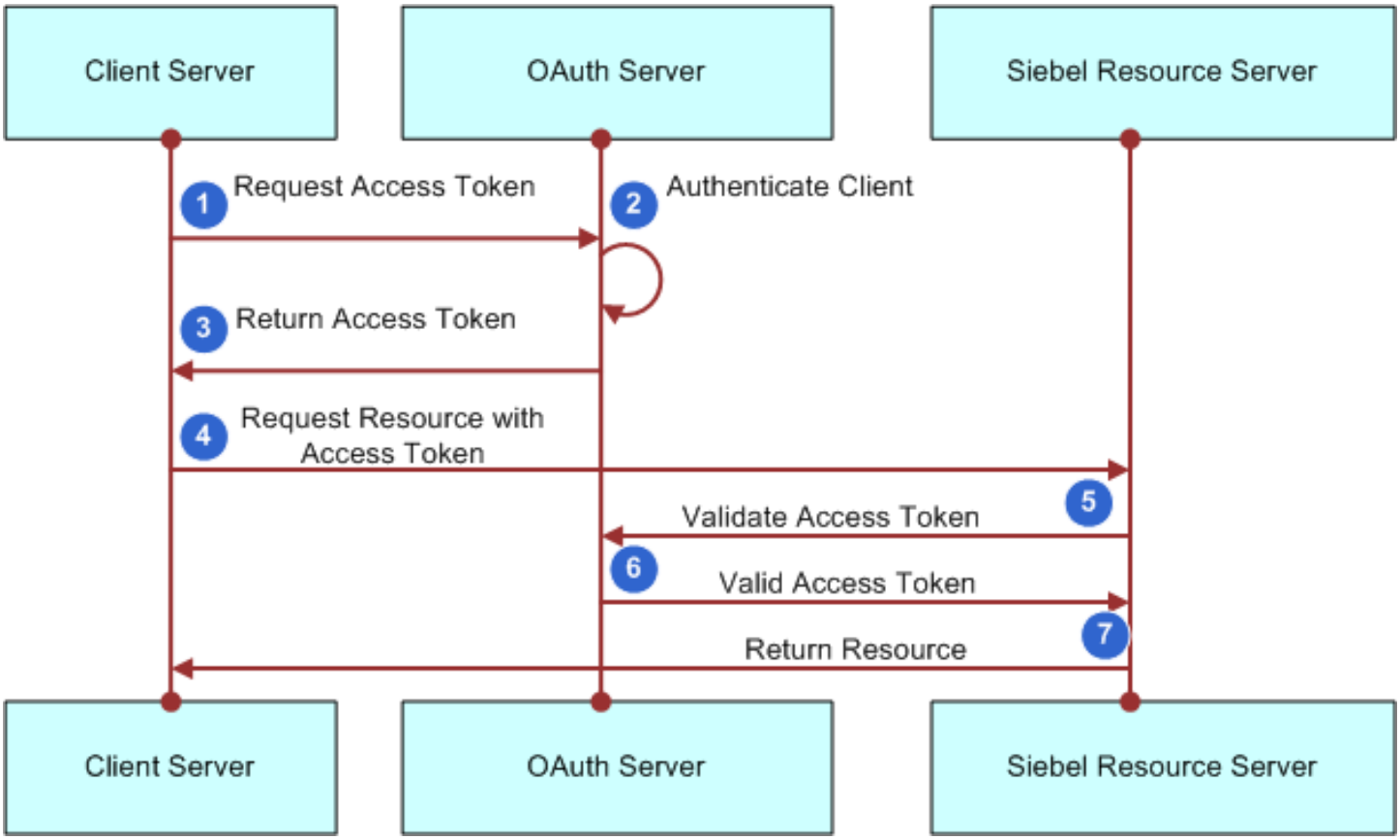
   c. When prompted for keystore password, provide the password and you will be asked to trust the certificate. Type **Yes**.
   d. The certificate will be added to the truststore.
5. Restart the Siebel AI Tomcat server for changes to take effect.

Client Application using Siebel REST with OAuth

OAuth 2.0 supports several different flows (or grants). Flow are ways of retrieving an Access Token. Deciding which one is suited for your use case depends mostly on your application type, the level of trust for the client or the experience you want your users to have. This document uses Postman as OAuth client, and it is for illustration purposes only.

Client Credentials Grant Authentication Flow

The client credentials grant flow represents an application that calls another application or service, without end user intervention. In this example, the client server application makes a call to the Siebel resource server to request business information. Since there is no end user intervention, the client is pre-authorized to have access to the resource. The following figure is an example of the Client Credentials Grant Authentication Flow.



The steps in this client credentials grant authentication flow process are as follows:

1. The business client application makes a call to the Siebel Server to request some business information by passing an access token. Since there is no end user intervention, the client is pre-authorized to have access to the resource.
2. The request is redirected to the OAuth server for authentication.
3. The OAuth server returns an access token.
4. The client server sends a request to the resource server. The request includes the access token in the HTTP header. Siebel Server looks for the USERID from the token to establish a Siebel Server session.
5. The Siebel Server validates the access token with the OAuth server.
6. If the access token is authorized by the OAuth server, then access is granted to the Siebel resource.
7. The Siebel Server returns the requested resource.

Once the confidential application has been setup on the IDCS and AI profile has been setup with the clientID/client secret and the introspection URL for REST Inbound authentication and LDAP/SSO for the EAI object manager, the next step is to generate the bearer token and make sure that the token is generated successfully for use in our OAuth flow for the client credentials flow.

For token generation, any utility like Postman or Boomerang can be used. Below are the types of grants that are available which can be used.

- Authorization Code
- Implicit
- Password Credentials
- Client Credentials

In this document, we will be covering "Client Credentials" grant type using Postman to generate token and perform introspection and validation of the REST calls.

The REST API Inbound authentication using OAuth uses Client Credentials Grant Authentication Flow.

Generate Bearer Token

1. Open Postman and create a brand-new collection named "OAuthRESTAPIKM"
2. Once the collection is created, expand it to show an empty request. Click on Add a Request to add a request and it will create a GET New Request by default.
3. In this GET request we will use a *data* call to the *Accounts* Business Component in the Siebel application. It can be in the format of:

   https://AIHostname:AIHTTPSPort/siebel/v1.0/data/Account/Account

   > **Note:** For the Bearer Token or Access Token generation, we must use POST method.

4. In the Auth section of the request, select Type as "OAuth 2.0", Add Authorization Data to "Request Headers" and provide the below values for the other parameters.
   - **Access Token**: Available Tokens (defaults)
   - **Header Prefix**: Bearer
   - **Token Name**: Any meaningful Name
   - **Grant Type**: Client Credentials
   - **Access Token URL**: https://IDCSHostName/oauth2/v1/token
   - **Client ID**: Copy clientID from the No Introspect application
   - **Client Secret**: Copy Client secret from the No Introspect application
   - **Scope**: https://AIHostname:AIHTTPSPort/siebel/v1.0/data
   - **Client Authentication**: Send client credentials in body
5. In the header section, make sure the values are set for Content-Type, Connection etc.

Parameter	Value
Accept	*/*
Accept-Encoding	gzip,deflate,br
Connection	keep-alive
Content-Type	Application/scim-json

6. Click on the Get New Access Token button. Once the button is clicked, you will get a message stating "Authentication Successful", and you will be asked to proceed further.
7. Click on "Use Token" from the pop-up window so that this token is used and replaced for the token in the Authorization for running Get Data later. Also, copy the Access Token and save it as it is required as input for the Introspection URL check.

Testing Introspection URL using Postman

Once the Bearer token has been generated, the immediate next *optional* step is to check if the introspection URL is working. This step makes sure that the connection to the IDCS application is working and if that is successful, then the

introspection URL provided in the Application Interface (AI) profile would also work and the REST API calls will also be successful.

To test the Introspection URL, do the following steps.

1. Open Postman and in the existing collection "OAuthRESTAPIKM", create another request and make it as **POST** request.
2. Name the request as Introspect OR any other name and the POST request should be in the format https://IDCSHostname/oauth2/v1/introspect
3. Under the Auth Section, make sure to select "Basic Auth" and for the username and password, enter the client ID and client secret that was generated for the IDCS confidential application with introspect enabled.
4. Now, go to the body section in the same introspect URL request and enter the token (bearer token/access token) value that was generated when the "Generate New Token" button was clicked.
5. Once these details are added, click **SEND** to execute the POST request and you should get a response with data that confirms that your Introspect URL is correct and that the introspect is working.

Below is a sample of how the payload response looks for the POST request with Introspect URL. In this payload response, you will see "sub" which is the actual User Specification (UserSpec) that we defined in the AI profile for EAI Object manager with SSO wherein the sub is the USERID or the clientID that will be used to authenticate.

Note: It is necessary to have this sub or clientID value added in the LDAP directory server for authentication to be successful.


```
{
 "active": true,
 "scope": "data",
 "client_id": "CLIENTID",
 "client_guid": "CLIENTSECRET",
 "token_type": "JWT",
 "sub_type": "client",
 "exp": 1685052145,
 "iat": 1685048545,
 "sub": "CLIENTID",
 "aud": [
 "https://AIHostname:AIHTTPSPort/siebel/v1.0/"
 ],
 "iss": "https://identity.oraclecloud.com/",
 "jti": "xxxxx",
 "tenant": "idcs-xxx",
 "user.tenant.name": "ixxx",
 "sub_mappingattr": "userName",
 "client_tenantname": "idcs-xxx",
 "client_name": "Siebel Postman OAuth Client",
 "region_name": "us-xx-xx-2",
 "gt": false
}
```


Note: In a client credentials grant flow, the client ID is sent as a subject. In this case, you must create a Siebel user or employee using the client ID as the USERID, and you must provide access to that user.

Testing REST API Calls to Siebel using Postman

Once the Introspect URL has been validated, the next step would be to test the REST API calls to Siebel using Postman.

1. Open Postman and in the existing collection "OAuthRESTAPIKM", and create a GET request with a URL value in the format of https://AIHostname:AIHTTPSPort/siebel/v1.0/data/Account/Account.
2. With the same existing values defined in the request, click **Send** to run the REST API call to Siebel to get the Account data for the clientID/userID. When it runs, it will provide the below response showing the list of ALL the accounts created by the ClientID/user.

Below is a sample of how the request output will look when GET.data.Account.Account method is run using a REST API call to capture the list of all the accounts for the clientID/user.


```
{
"items": [
{
"SBA Review": "",
"Friday End Time 2": "",
"Saturday End Time 2": "",
"Modified By Name": "clientID/UserID",
"Friday End Time 1": "",
"Saturday End Time 1": "",
"Our Position": "",
"Supply Characteristics": "",
"DeDup Key Modification Date": "",
"Prospect Flag": "N",
"Market Share": "",
"Statement Date": "",
"Reference Stage": "",
.....
"Link": [
{
"rel": "self",
"href": "https://AIHostname:AIHTTPSPort/siebel/v1.0/data/Account/Account/1-2X9B6",
"name": "Account"
},
{
"rel": "canonical",
"href": "https://AIHostname:AIHTTPSPort/siebel/v1.0/data/Account/Account/1-2X9B6",
"name": "Account"
},
{
"rel": "child",
"href": "https://AIHostname:AIHTTPSPort/siebel/v1.0/data/Account/Account/1-2X9B6/UT Account Partner",
"name": "UT Account Partner"
....
],
"Link": {
"rel": "self",
"href": "https://AIHostname:AIHTTPSPort/siebel/v1.0/data/Account/Account",
"name": "Account"
}
}
```


The above payload response would indicate that the request sent via OAuth to Siebel is able to retrieve the account details of all the accounts that were created by the clientID/user.

Configuring OAuth Support for Siebel REST Outbound Connections (21.8 to 22.8)

This topic shows how to configure OAuth support for Siebel REST outbound connections using a server script, for Siebel update 21.8 to 22.8.

OAuth is supported from Siebel CRM 21.8 onwards. You can implement it with additional scripting.

> **Note:** For instructions from Siebel Update 22.9 and above, see *Configuring OAuth Support for Siebel REST Outbound Connections (22.9+)*.

Configure OAuth Support for Outbound Any REST Proxy Business Service

This procedure shows how to configure OAuth support for any outbound REST proxy business service:

1. Create a Workspace and open it in Siebel Tools/Web Tools.
2. Import the swagger – open the API JSON file for the outbound REST service in Siebel Tools/Web Tools.
3. Verify that the proxy business service has been created:
   a. Check the method arguments for the business service where you want to configure OAuth support.
   b. If not already present, add a parameter named “Authorization:header” with the following properties:
   Name: "Authorization:header"
   Type: String
4. Add a script to the proxy business service's Service_PreInvokeMethod event handler for which you want OAuth support. For more information, see the following topics:
   - *Add Script for OAuth Support*
   - *Sample Script*
5. For the existing “Siebel XSL to XML Converter” business service, set the attributes shown in the following table. This will allow you to reference the Siebel XSL to XML Converter business service in the script.

Attribute	Value
External Use	Yes
Server Enabled	Yes
Hidden	No

6. After making these changes and adding the script in step 4, deliver the Workspace.

Adding Script for OAuth Support

You must add an OAuth support script, as shown in the following procedure, when configuring OAuth support for Siebel REST outbound connections.

To add script for OAuth support

1. Get the access token from your service provider.
   - Call the service that provides the access token using the SendReceive method of the “EAI HTTP Transport” business service by providing appropriate parameters.
   - This call will return the access token, in the response body, as a JSON string.
   - The JSON string will be in the response – in the PropertySet value of the SendReceive method.
2. Extract the access token from the response returned by the token provider:
   - Call the "jsontops" method, passing in the response PropertySet received from the SendReceive method invoked in Step 1.

- The "jsontops" method will return a PropertySet with the token and other response values as a property.
- Extract the "access_token" and "token_type" properties.

3. Set the “Authorization:header” property to contain the token_type in the Input Arguments of the proxy business service method.

Sample Script

The following is an example of a script that you add to the proxy Business Service's Service_PreInvokeMethod event handler when configuring OAuth support for Siebel REST outbound connections.

```
function Service_PreInvokeMethod(MethodName, Inputs, Outputs) {
//1. Get Access token from OAUTH server//
 var EAIHTTPTrasnport = TheApplication().GetService("EAI HTTP Transport");
 var Httpin = TheApplication().NewPropertySet();
 var Httpout = TheApplication().NewPropertySet();
 Httpin.SetProperty("HTTPRequestURLTemplate", "https://idcs-
f03fb776674c40eb80487eb12f87a170.identity.c9dev2.
oc9qadev.com/oauth2/v1/token");
 Httpin.SetProperty("HTTPContentType", "application/x-www-form-urlencoded;charset=UTF-16");
 Httpin.SetProperty("HDR.Authorization", "Basic
YjZjYTYzNWM3YjcwNGFlYmE2NzQyNTJkYWM4YTVmYzU6YmJiOWJmZjUtYjE0NS00NTg0LTgwODItNGI4ODYwYzgwMmVk");
 Httpin.SetProperty("HTTPRequestMethod", "POST");
 Httpin.SetProperty("HTTPRequestBodyTemplate", "grant_type=client_credentials&scope=urn:opc:idm:
__myscopes__");
 Httpin.SetProperty("HTTPAccept", "*/*");
 Httpin.SetProperty("CharSetConversion", "UTF-8");
 EAIHTTPTrasnport.InvokeMethod("SendReceive", Httpin, Httpout);

// Can be removed or commented after debugging complete
 TheApplication().TraceOn("", "Allocation", "All");
 TheApplication().Trace("START - TEST v1.0");
 TheApplication().Trace(Httpout.GetValue());
 TheApplication().Trace("END - TEST");
 TheApplication().TraceOff();

//2. Extract access token from json to property set//
 var Jsoconverter = TheApplication().GetService("Siebel XSL To XML Convertor");
 var tokenPS = TheApplication().NewPropertySet();
 Jsoconverter.InvokeMethod("jsontops", Httpout, tokenPS);
 var token_type = tokenPS.GetProperty("token_type");
 var access_token = tokenPS.GetProperty("access_token");
 TheApplication().TraceOn("", "Allocation", "All");
 TheApplication().Trace("START - TEST v2.0");
 TheApplication().Trace(tokenPS.GetProperty("access_token"));
 TheApplication().Trace(tokenPS.GetProperty("token_type"));
 TheApplication().Trace(tokenPS);
 TheApplication().Trace("END - TEST");
 TheApplication().TraceOff();

//3. Add access token to proxy BS input property set//
 Inputs.SetProperty("Authorization:header", token_type + " " + access_token);
 return (ContinueOperation);
}
```

Modify Script (Optional)

Depending on your particular situation, you can change the previous sample script as shown in the following table.

Change	Description
HTTPRequestURL Template	In the sample script shown here, the HTTPRequestURLTemplate is set to **`https://idcs-f03fb776674c40eb80487eb12f87a170.identity.c9dev2.oc9qadev.com/oauth2/v1/token`**. You can change this URL to match the correct end point for your external service.
HDR.Authorization	**`"Basic <Base64 encode of client_id:client_secret>"`** is the Base64 Encoded value of the Client ID and Client Secret. Siebel must be registered in the Out bound server's (Resource Server) OAuth server to get the client_id & client_secret, as follows: • Step 1: Register Siebel Application as a client in external applications OAuth Server. • Step 2: Base64 Encode the Client ID and Client Secret obtained from Step 1. • Step 3: Obtain an Access Token using Base64 Encode of the Client ID and Client Secret.

To resolve a "Cannot connect to server error"

1. Create a domain user and add it to the local Administrators group (and set the password).
2. Add the local user to the Administrator group.
3. Log in to the Siebel application with the created *local user*.
4. Go to the Security section of your browser and ensure that the following are set:
    - Check for the publisher's certificate revocation
    - Check for the server's certificate revocation
    - Check that TLS1.2 is set to true
5. Open Services, go to the Siebel Server Service and log in with the local user credentials.
6. Restart the Siebel Service with that user (local user).

Configuring OAuth Support for Siebel REST Outbound Connections (22.9+)

After Siebel Update 22.9, to add a security header, you can either follow the instructions in this section or follow the instructions at *Configuring OAuth Support for Siebel REST Outbound Connections (21.8 to 22.8)*.

For Siebel Update 21.8 to 22.8, follow the instructions in *Configuring OAuth Support for Siebel REST Outbound Connections (21.8 to 22.8)*.

> **Note:** The difference in the setup steps is that before Update 22.8 you add a Proxy Business Service Method Argument (Name: "Authorization:header") and then add a script to the proxy business service's Service_PreInvokeMethod event handler to assign a value to this parameter. As of Siebel Update 22.9, you can also achieve this using the Custom Filter service steps for injecting the "Authorization" or any other parameter as described in *Overview of the REST Outbound Filter Service* in the Siebel REST API Guide.

Configure OAuth Support for Outbound Any REST Proxy Business Service

This procedure shows how to configure OAuth support for any outbound REST proxy business service:

1. Create a Workspace and open it in Siebel Tools/Web Tools.
2. Import the swagger – open the API JSON file for the outbound REST service in Web Tools.
3. Verify that the proxy business service has been created. Check the method arguments for the business service where you want to configure OAuth support.
4. Create a new filter business service; for example 'RESTFilterTesting' with methods, for example UpdateInput and UpdateOutput methods.
5. Add a script to the newly created Filter business service's Service_PreInvokeMethod event handler for which you want OAuth support. For more information, see the following topics:
   a. *Add Script for OAuth Support*
   b. *Sample Script*
   c. Configure Administration – Web Service -> Outbound REST Services screen with the above for Request Filter under Filters for the REST Service -> Service Methods that you need to inject these above parameters with the Custom Filter Service that you created (for example 'RESTFilterTesting') at step 4. Caution needs to be taken to add the Filter Service method (for example UpdateInput) used in the script, to make sure that the appropriate parameters get added to the input (Request)/output (Response) property.
   d. You can add appropriate script if required, to intercept the response such as the script below.

```
function Service_PreInvokeMethod (MethodName, Inputs, Outputs)
{
 if(MethodName == "UpdateOutput" && Outputs!= null)
 {
 // write your script code here to update the response
 }
 return (CancelOperation);
}
```

6. For the existing "Siebel XSL to XML Converter" business service, set the attributes shown in the following table. This will allow you to reference the Siebel XSL to XML Converter business service in the script.

Attribute	Value
External Use	Yes
Server Enabled	Yes
Hidden	No

7. After making these changes and adding the script in step 4, deliver the Workspace.

   Here's a sample updated Request done by the Filter business service script:

```
> Value =
> Type =
- > Child property set #1 at level 1:
- > Value =
- > Type = url
- > httpMethod = POST
```

```
- > url = https://https://petstore3.swagger.io/api/v3/pet
- > Child property set #2 at level 1:
- > Value =
- > Type = query
- > query =
- > Child property set #3 at level 1:
- > Value =
- > Type = body
- - > Child property set #1 at level 2:
- - > Value =
- - > Type = Req2SwaggerPetstoreOpenAPI30:body
- - - > Child property set #1 at level 3:
- - - > Value =
- - - > Type = ReqBody__SKIP__WRAPPER
- - - - > Child property set #1 at level 4:
- - - - > Value =
- - - - > Type = pet
- - - - > long_id = 512312459
- - - - > string_status = pending
- - - - > string_name = kk5name123
- - - - - > Child property set #1 at level 5:
- - - - - > Value =
- - - - - > Type = category
- - - - - > long_id = 11
- - - - - > string_name = categorykk5name
- - - - - > Child property set #2 at level 5:
- - - - - > Value =
- - - - - > Type = ListOftags__Array
- - - - - - > Child property set #1 at level 6:
- - - - - - > Value =
- - - - - - > Type = tags
- - - - - - > long_id = 5
- - - - - - > string_name = tagskk15name
- - - - - - > Child property set #2 at level 6:
- - - - - - > Value =
- - - - - - > Type = tags
- - - - - - > long_id = 6
- - - - - - > string_name = tagskk25name
- - - - - > Child property set #3 at level 5:
- - - - - > Value =
- - - - - > Type = ListOfphotoUrls__Primitive
- - - - - - > Child property set #1 at level 6:
- - - - - - > Value =
- - - - - - > Type = photoUrls
- - - - - - > string_elem__value = 55
- - - - - - > Child property set #2 at level 6:
- - - - - - > Value =
- - - - - - > Type = photoUrls
- - - - - - > string_elem__value = 66
- > Child property set #4 at level 1:
- > Value =
- > Type = security
- > Child property set #5 at level 1:
- > Value =
- > Type = misc
- > serviceMethod = addPet
- > Child property set #6 at level 1:
- > Value =
- > Type = header
- > Authorization = tokentype 1234567890
- > Content-Type = application/json
```

Add Script for OAuth Support

You must add an OAuth support script, as shown in the following procedure, when configuring OAuth support for Siebel REST outbound connections.

To add script for OAuth support

1. Get the access token from your service provider.
   - Call the service that provides the access token using the SendReceive method of the "EAI HTTP Transport" business service by providing appropriate parameters.
   - This call will return the access token, in the response body, as a JSON string.
   - The JSON string will be in the response – in the PropertySet value of the SendReceive method.
2. Extract the access token from the response returned by the token provider:
   - Call the "jsontops" method, passing in the response PropertySet received from the SendReceive method invoked in Step 1.
   - The "jsontops" method will return a PropertySet with the token and other response values as a property.
   - Extract the "access_token" and "token_type" properties.
3. Set a property by name "Authorization" into the `header` PropertySet which is one of the child PropertySet of Input PropertySet of the newly created Filter business service Service_PreInvokeMethod created previously and assign the value to this property by substituting token_type + " " + access_token.

Sample Script

The following is an example of a script that you add to the Custom Filter (for example "RESTFilterTesting") business service's Service_PreInvokeMethod event handler when configuring OAuth support for Siebel REST outbound connections.

```
function Service_PreInvokeMethod(MethodName, Inputs, Outputs) {
//1. Get Access token from OAUTH server//
 var EAIHTTPTrasnport = TheApplication().GetService("EAI HTTP Transport");
 var Httpin = TheApplication().NewPropertySet();
 var Httpout = TheApplication().NewPropertySet();
 Httpin.SetProperty("HTTPRequestURLTemplate", "https://idcs-
f03fb776674c40eb80487eb12f87a170.identity.c9dev2.
oc9qadev.com/oauth2/v1/token");
 Httpin.SetProperty("HTTPContentType", "application/x-www-form-urlencoded;charset=UTF-16");
 Httpin.SetProperty("HDR.Authorization", "Basic
YjZjYTYzNWM3YjcwNGFlYmE2NzQyNTJkYWM4YTVmYzU6YmJiOWJmZjUtYjE0NS00NTg0LTgwODItNGI4ODYwYzgwMmVk");
 Httpin.SetProperty("HTTPRequestMethod", "POST");
 Httpin.SetProperty("HTTPRequestBodyTemplate", "grant_type=client_credentials&scope=urn:opc:idm:
__myscopes__");
 Httpin.SetProperty("HTTPAccept", "*/*");
 Httpin.SetProperty("CharSetConversion", "UTF-8");
 EAIHTTPTrasnport.InvokeMethod("SendReceive", Httpin, Httpout);

// Can be removed or commented after debugging complete
 TheApplication().TraceOn("", "Allocation", "All");
 TheApplication().Trace("START - TEST v1.0");
 TheApplication().Trace(Httpout.GetValue());
 TheApplication().Trace("END - TEST");
 TheApplication().TraceOff();

//2. Extract access token from json to property set//
 var Jsoconverter = TheApplication().GetService("Siebel XSL To XML Convertor");
 var tokenPS = TheApplication().NewPropertySet();
 Jsoconverter.InvokeMethod("jsontops", Httpout, tokenPS);
```

```
 var token_type = tokenPS.GetProperty("token_type");
 var access_token = tokenPS.GetProperty("access_token");
 TheApplication().TraceOn("", "Allocation", "All");
 TheApplication().Trace("START - TEST v2.0");
 TheApplication().Trace(tokenPS.GetProperty("access_token"));
 TheApplication().Trace(tokenPS.GetProperty("token_type"));
 TheApplication().Trace(tokenPS);
 TheApplication().Trace("END - TEST");
 TheApplication().TraceOff();

//3. Add access token to Custom Filter Service BS input property set//
 var j;
 if(MethodName == "UpdateInput" && Inputs != null)
 {
 for (var i = 0; i < Inputs.GetChildCount(); i++)
 {
 j = Inputs.GetChild(i);
 if(j.GetType() == "header")
 {
 j.SetProperty("Authorization", token_type + " " + access_token);
 break;
 }
 }
 }
 return (CancelOperation);
}
```

Modify Script (Optional)

Depending on your particular situation, you can change the previous sample script as shown in the following table.

Change	Description
HTTPRequestURL Template	In the sample script shown here, the HTTPRequestURLTemplate is set to **`https://idcs-f03fb776674c40eb80487eb12f87a170.identity.c9dev2.oc9qadev.com/oauth2/v1/token`**. You can change this URL to match the correct end point for your external service.
HDR.Authorization	**`"Basic <Base64 encode of client_id:client_secret>"`** is the Base64 Encoded value of the Client ID and Client Secret. Siebel must be registered in the Out bound server's (Resource Server) OAuth server to get the client_id & client_secret, as follows: • Step 1: Register Siebel Application as a client in external applications OAuth Server. • Step 2: Base64 Encode the Client ID and Client Secret obtained from Step 1. • Step 3: Obtain an Access Token using Base64 Encode of the Client ID and Client Secret.

To resolve a "Cannot connect to server error"

1. Create a domain user and add it to the local Administrators group (and set the password).
2. Add the local user to the Administrator group.
3. Log in to the Siebel application with the created *local user*.

4. Go to the Security section of your browser and ensure that the following are set:
    - Check for the publisher's certificate revocation
    - Check for the server's certificate revocation
    - Check that TLS1.2 is set to true
5. Open Services, go to the Siebel Server Service and log in with the local user credentials.
6. Restart the Siebel Service with that user (local user).

7 Siebel Application Interface Security Features

Siebel Application Interface Security Features

This chapter describes several options that relate to security issues and the Siebel Application Interface. It includes the following topics:

- *About the Siebel Web Client and Using HTTPS*
- *Implementing Secure Login*
- *Logging Out of a Siebel Application*
- *Login User Names and Passwords*
- *Account Policies and Password Expiration*
- *About Using Cookies with Siebel Business Applications*
- *About Service Discovery Initiated by Trusted and Untrusted Sources in Siebel Application Interface*

About the Siebel Web Client and Using HTTPS

Siebel Application Interface uses an HTTP port with a redirection port set to always use HTTPS. As a result, all access to HTTP will redirect to HTTPS.

It is mandatory to deploy Siebel with a reverse proxy so that the Siebel Application Interface port will not be exposed. If SSL is terminated at reverse proxy level, then you must configure Siebel Application Interface for HTTP.

SES containers require an HTTP port for Siebel Server to communicate with SES to route the JBS (64-bit Java business service) and outbound requests via SES; here, Siebel Server communicates with the SES container using localhost and HTTP port. All outbound communications in non-Windows environments happen via the SES container.

```
// Non-Windows
Sieb Server -> SES Container(HTTP) -> external(HTTPS)

// Windows
Sieb Server -> external (HTTPS)
```

Siebel Web Client is configured for HTTPS by the Siebel installer. Certificate and certificate store creation is a prerequisite for the Siebel installer to pick and use during HTTPS configuration. For more information, see the following:

- *Certificate Requirements for Communications*
- *About Generating Server Keystore, Client Keystore and Truststore Files*
- *Siebel Installation Guide*

Implementing Secure Login

Secure login is enabled when Siebel Web Client is configured and accessible over HTTPS. The Siebel installer enforces HTTPS for Web server access. For more information, see the topic about installing Siebel Business applications in *Siebel Installation Guide* .

With secure login, the Siebel Web application server transmits user credentials entered in a login form from the browser to the Web server using TLS, that is, over HTTPS.

Note: You cannot log into a Siebel application by presenting user credentials as parameters in a URL.

For information about administering Siebel Server components, see *Siebel System Administration Guide* .

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.

If you are using Siebel Business Applications, clicking Close (the X icon) 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 Active Session Timeout Value parameter set in the Siebel Application Interface profile for the application interface. For more information about this parameter, see *Siebel Application Interface Profile Parameters*.

Login User Names and Passwords

The following features are typically available on the Siebel login dialog box to assist users:

- The Remember My User ID check box

  This feature is provided by your browser (and not by Siebel).
- The Forgot Your Password? link

  For information on retrieving forgotten passwords, see *Retrieving a Forgotten Password (Users)*.

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 or applicable custom security adapter
- Database authentication where supported by the RDBMS

If you are using an LDAP security adapter, then password expiration is handled by the external LDAP 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.

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 use cookies for a variety of purposes. This topic describes the types of cookies used and provides instructions for enabling cookies for Siebel CRM.

All cookies used by Siebel CRM are encrypted using standard encryption algorithms. Siebel CRM uses the following kinds of cookies:

- **Session cookie.** Manages user sessions for Siebel Web Client users. For details, see *Session Cookie*.
- **Auto-login credential cookie.** Stores user credentials for Siebel Web Client users. For details, see *Auto-Login Credential Cookie*.

> **Note:** It is recommended that you always run Siebel applications using HTTPS mode in order to mark cookies as *secure*. This ensures that security does not mix secure and insecure content. Applications run using HTTP mode will not mark cookies as secure.

Using cookies helps to maintains user session information. Browsers with cookies disabled cannot maintain a Siebel user session. Siebel does not support or recommend cookieless mode.

Related Topic

Enabling Cookies for Siebel CRM

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.

Web browsers with cookie handling disabled cannot maintain a Siebel user session.

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 Siebel Application Interface.
2. The session ID is passed to the client in a cookie.
3. The following occurs:
    - 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 Siebel Application Interface 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.

Session cookie is used to maintain a stateful session and the SRN, which is generated after an explicit user login is used to maintain a secure session for the logged in user. SRN protects all writer operations in a user session.

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.

Session ID Encryption

Siebel session ID is encrypted with AES256.

> **Note:** If a user changes their 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.

Session Cookies with sameSiteCookies set to Strict

Session cookies default to `sameSiteCookies="Strict"`:

- `JSESSIONID`
- `_sn_<application>_<lang>`

If required, you can change this behavior as described in the following procedure. Before doing so, however, you must have a full understanding of the security impact of modifying this behavior when Siebel communicates with external sites.

To modify sameSiteCookies

1. Open the context.xml file located here:

   ```
   <Application Interface Install Location>\conf\context.xml
   ```

2. Modify `sameSiteCookies="Strict"` by setting sameSiteCookies to a new supported value available on all browsers used by end users that meet the security parameters for your organization.

   In the following example, sameSiteCookies has been changed to "None":

   ```
   <CookieProcessor
   className="org.apache.tomcat.util.http.LegacyCookieProcessor"
   sameSiteCookies="None" />
   ```

3. Restart the application interface for the changes to take effect.

> **Note:** Siebel session cookies are already marked as Secure - that is, the Secure attribute is assigned to all session cookies by default.

Auto-Login Credential Cookie

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 AES 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
```

Enabling Cookies for Siebel Business Applications

This topic describes how to enable the Microsoft Internet Explorer Web browser to handle cookies used by Siebel CRM. These instructions can vary depending on your supported browser version.

Note: If you are using a browser other than Internet Explorer to run Siebel CRM, 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.

About Siebel Session Warning Message

If multiple tab browsing is not configured for your application and you try to start a second Siebel session while another session is currently active, then a Siebel session warning message similar to the following appears. For more information about configuring multiple tab browsing, see *Configuring Siebel Open UI* .

```
You have initiated a Siebel Session while another Siebel session is currently active.
Please choose the option that applies to you:
- You already have a Sieble session with unsaved data running in another window. To save
 data from a second session go to the already open session and either save and exit
 or continue to use that data.
- You do no have unsaved data in your other session and wish to close it and launch a new
 session. Click here.
- You have closed your previous Siebel browser instance using the Close button instead of
 the Logoff feature and wish to open a new Siebel session. Click here.
```

After a successful UI login to Siebel application, two cookies are sent as follows:

- `Siebel Session Number`. This cookie is the security token passed along with the request. It is encoded and holds valuable information required to connect to the correct task. `Siebel Session Number` remains until you explicitly log out of the application or close your browser.
- `[sameuisession]`. This unique cookie is attached to the particular browser tab from where a user request is sent. It is set in javascript and expires after 3 seconds when the application unloads like it does when you close the browser.

This effectively means the following:

- If you close the (first) tab, the `[sameuisession]` will expire after 3 seconds and if you try to use the same `Siebel Session Number` from another (second) tab, then the Siebel session warning message appears.
- If you try to run the application URL from another tab, the `Siebel Session Number` will be sent correctly but since no `[sameuisession]` is set, the Siebel session warning message appears.

About Service Discovery Initiated by Trusted and Untrusted Sources in Siebel Application Interface

External untrusted connect string URLs should not be used for production loads, testing loads, or to identify if Siebel Cloud Gateway is running. Using external URLs causes a significant increase in load on the database. Performance will differ significantly between a service discovery request triggered by Siebel Application Interface and an external call coming through the UI, REST UI, or SOAP interface.

The paths taken by trusted and untrusted requests are:

- **Trusted Source.** This is where service discovery is initiated by Siebel Application Interface.

  In this scenario, there is no userID/password based authentication at the gateway.
- **Untrusted Source.** This is where service discovery is initiated by the end-user client or browser.

  In this scenario, there is userID/password based authentication at the gateway. This is required to access the application interface and Siebel application.

8 User Administration

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*
- *About Anonymous Browsing*
- *Process of Implementing Anonymous Browsing*
- *About Self-Registration*
- *User Experience for Self-Registration*
- *Process of Implementing Self-Registration*
- *Identifying Disruptive Workflows*
- *About Managing Forgotten Passwords*
- *Internal Administration of Users*
- *About Adding a User to the Siebel Database*
- *Delegated Administration of Users*
- *Maintaining a User Profile*

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 *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 *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*. For information on implementing anonymous browsing, see *Process of Implementing Anonymous Browsing*.

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*
- *Setting Configuration Parameters for Anonymous Browsing*
- *Configuring Views for Anonymous Browsing or Explicit Login*

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*.

This task is a step in *Process of Implementing Anonymous Browsing*.

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*.
- 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:

> **Note:** Responsibilities and their relationship to Views can be Workspace enabled in your development environment. If they have been Workspace enabled in your development environment and you are working in that environment, then you can only modify them in an editable Workspace. You do not need an editable Workspace to create and edit Responsibilities and their relationship to Views in your Production environment.

- 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 *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

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*.

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 Siebel Application Interface profile, set the following parameters:
   - **Anonymous User Name**

     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 the Anonymous User Name parameter. Do not specify Siebel administrator (SADMIN) as the Anonymous User Name; doing so allows anonymous users to access every part of the Siebel system.

   - **Anonymous User Password**

     This is the authenticated password that is paired with the Anonymous User Name parameter.

   For more information on setting parameter values in the Siebel Application Interface profile, see *Siebel Application Interface Profile Parameters*.

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*.

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. Update the repository and deliver the updates, then 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.
- You can configure any eligible Siebel application to either allow or disallow self-registration.
- You can implement Lightweight Directory Access Protocol (LDAP) 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 *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 and then clicks Next. For example, the fields for Siebel eService are described in the following table.

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.

Field	Guideline
	For LDAP 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 end 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, for example, payment information and address information.
5. On the Usage Terms form, the user must agree to the terms of the license agreement to be registered.

The Registration Confirmation message appears.

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*
- *Setting the Propagate Change Parameter for Self-Registration*

- Review *About Activating Workflow Processes for Self-Registration*
- *(Optional) Modifying Self-Registration Views and Workflows*
- *(Optional) Managing Duplicate Users*

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*.

This task is a step in *Process of Implementing Self-Registration*.

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. *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 *Configuring Access Control*.

Setting the Propagate Change Parameter for Self-Registration

This topic describes the Siebel Propagate Change parameter. Setting the Propagate Change parameter to `True` simplifies user administration when you implement user self-registration.

This task is a step in *Process of Implementing Self-Registration*.

The user directory can be administered through Siebel Business Applications if you implement security adapter authentication. Changes such as adding a user, or changing a password by an internal administrator, a delegated administrator, or when a user self-registers, are propagated to the user directory.

Set the Propagate Change 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 Propagate Change 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 LDAP Security Adapter.
3. In the Profile Parameters applet, set the Propagate Change parameter to True.

For additional information about setting the Propagate Change parameter, see *Server Parameters for Siebel Gateway*.

> **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*.

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

The following table shows the views specified in the workflow processes that provide interactive forms during self-registration.

View Name	Applications Using This View	Description
VBC User Registration Initial Form View VBC User Registration Password Error Msg View VBC User Registration Missing Info Msg View VBC User Registration Legal Confirmation View VBC User Registration Login Error Msg View VBC User Registration Confirmation Msg View VBC User Registration Declined View VBC User Registration Create User Error Msg View VBC User Registration Security Setup Error Msg View	All	These views, common to all applications that use the User Registration Process, comprise two groups: Personal Information form and messages resulting from flawed entries or a duplicate user ID with an existing user record. Usage Terms form and messages resulting from accepting or declining to agree.
VBC User Registration Contact Information View	Default	This view is the Contact Information form used by default.
VBC User Registration Company Information - Company View (SCW) VBC User Registration Company Information - Individual View (SCW)	Siebel Partner Portal	These views collect contact information and information about the user's company.

View Name	Applications Using This View	Description
VBC User Registration Contact Information View (SCW)		

(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*.

You can modify the default self-registration functionality in several ways. See the following topics for additional information:

- *Replacing the License Agreement Text*
- *About Revising a Workflow Process*
- *Custom Business Services*
- *Redefining Required Fields*
- *Adding or Deleting Fields in an Existing View*
- *About Changing the Physical Appearance of a View or Applet*
- *About Creating a New View for Self-Registration*

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 an asterisk (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 after 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, using 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 earlier in this procedure, such as MiddleName.

12. Update the repository and deliver the updates, then unlock the User Registration project.

    When viewed in the self-registration interface, the new required field has an asterisk (a star icon) beside it.

> **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 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. Update the repository and deliver the updates, then 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 an asterisk (a star icon) displays in the user interface. By convention, fields that you require users to complete during the self-registration process have an asterisk (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*.

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 remain 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 following fields, using 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 earlier in this procedure.

5. Update the repository and deliver the updates, then 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. Complete only the following fields, using 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. Update the repository and deliver the updates, then 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*.
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*.

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*. 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 earlier in this procedure.

   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 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*.

- 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*.

For additional information about managing forgotten passwords, see also the following topics:

- *Retrieving a Forgotten Password (Users)*
- *Architecture for Forgotten Passwords*
- *About Modifying the Workflow Process for Forgotten Passwords*

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

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* and *Retrieving a Forgotten Password (Users)*.

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 the three preceding steps, with modifications for completing the fields in the record, 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. Update the repository and deliver the updates, then unlock the User Registration project.

Architecture for Forgotten Passwords

Forgot Your Password? is implemented in the User Registration Forgot Password Process workflow process. This process is a subprocess in User Registration Initial Process.

As described in *Retrieving a Forgotten Password (Users)*, 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

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*.
- Request different identification data from the user

  For information on this task, see *Modifying Workflow Process to Request Different Identification Data*.

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.

The following table describes the arguments for the FindContact method.

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.
Input Arguments	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

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) checks any empty fields to confirm that they are 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

Modifying Workflow Process to Request Different Identification Data

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*.

   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 and complete only the following fields using 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 earlier in this procedure that you want to add, such as City
HTML Display Mode	Delete the default value, so the field is empty
HTML Row Sensitive	Check
HTML Type	Pick Text

Field	Guideline
Sort	Check
Text Alignment	Pick an alignment
Visible	Check
Visible - Language Override	Enter Y

5. Configure the appropriate applet Web template for VBC User Registration Initial Form Applet to display or hide the field.
6. Update the repository and deliver the updates, then 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.

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 the following table.

Field	Guideline
Input Argument	Enter the name of the field in the User Registration business component that you identified in *Modifying the User Interface for User Registration*, 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 identified in *Modifying the User Interface for User Registration*, 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

Modifying Workflow Process to Query Null Fields

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 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 *Configuring Access Control*. See the following topics for information on adding users to the Siebel database:

- *Adding a New Employee*
- *About Adding a New Partner User*
- *Adding a New Contact User*
- *Modifying the New Responsibility for a User Record*

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, using the indicated guidelines, and then save the record.

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

Field	Guideline
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 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*.
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*.
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 *Configuring Access Control*.

Related Topics

About Adding a User to the Siebel Database

Modifying the New Responsibility for a User Record

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

Employee record should never be deleted, but rather deactivated for two reasons:

1. If an Employee record is deleted than any reference to that employee (such as the "Created By" and "Updated By" system fields and the Audit Trail) will no longer be able to show the Employee's Login, but rather just a ROW_ID. To avoid this situation of losing referential integrity, Employees should not be deleted.
2. From a functional perspective, employees may leave an organization (or go on extended leave) and then return some time later. By keeping the Employee record, that user can be reactivated and their history of Activities, Accounts, and all other entities will be maintained and available to that user, saving administrative time and effort.

To deactivate an employee

Follow the steps to complete the task:

1. Navigate to the **Administration** > **User screen**, then the **Employees View**.
2. Select the employee that you want to deactivate.
3. Set the **User Status** value to "Inactive", this will prevent the user from being able to login.
4. Remove the employee's access to the physical database or the external authentication manager (for example, "SSO" or "ldap"). This is not required to block logins to Siebel CRM, but is a good security practice.

> **Note:** Step number 4 is optional.

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

Modifying the New Responsibility for a User Record

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, using the indicated guidelines, and then save the record.

   The new user appears in the Users list.

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.

Field	Guideline
	For LDAP 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*.
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*.
Time Zone	Choose a time zone so that times for events can be expressed in terms of this zone.
User Type	This field serves as a filter so that different applications can query for contact users only applicable to each particular application.
Work Phone # Home Phone # Fax #	The application interprets only the digits the user provides. Any separators are disregarded.

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.

Related Topics

About Adding a User to the Siebel Database

Adding a New Contact User

Modifying the New Responsibility for a User Record

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

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*
- *Access Considerations for Delegated Administration*
- *Registering Contact Users (Delegated Administration)*
- *Registering Partner Users (Delegated Administration)*

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 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 that you configure the LDAP security adapter to propagate new and modified user data from the Siebel database to the user directory.

If you implement an adapter-defined user name in your user authentication environment, then you cannot implement tools that allow Siebel user IDs stored in the directory to be managed from within Siebel Business Applications, including delegated administration of users. For information about user authentication, see *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

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 *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

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*.

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, using the indicated guidelines, and then save the record.

   The new record appears in the Users list.

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 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*.
Home Phone # Work Phone # Work Fax #	The application interprets digits only in these telephone number entries. Any separators are disregarded.

Field	Guideline

Related Topic

Delegated Administration of Users

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, using the indicated guidelines, and then save the record. The new partner user record appears in the Users list.

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 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*.
Work Phone # Home Phone # Work Fax # Pager #	The application interprets digits only in these telephone number entries. The user can enter any separators.

Related Topic

Delegated Administration of Users

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*
- *Changing a Password*
- *Changing the Active or Primary Position*

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

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*, 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

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.

Related Topic

Maintaining a User Profile

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.

9 Configuring Access Control

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*
- *Access Control Mechanisms*
- *Planning for Access Control*
- *Setting Up Divisions, Organizations, Positions,and Responsibilities*
- *About View and Data Access Control*
- *Listing the Views in an Application*
- *Responsibilities and Access Control*
- *Viewing Business Component View Modes*
- *Configuring Access to Business Components from Scripting Interfaces*
- *Viewing an Applet's Access Control Properties*
- *Listing View Access Control Properties*
- *Example of Flexible View Construction*
- *About Implementing Access-Group Access Control*
- *Implementing Access-Group Access Control*
- *Managing Tab Layouts Through Responsibilities*
- *Managing Tasks Through Responsibilities*
- *Administering Access Control for Business Services*
- *Administering Access Control for Business Processes*
- *Clearing Cached Responsibilities*
- *About Configuring Visibility of Pop-Up and Pick Applets*
- *About Configuring Drilldown Visibility*
- *Party Data Model*

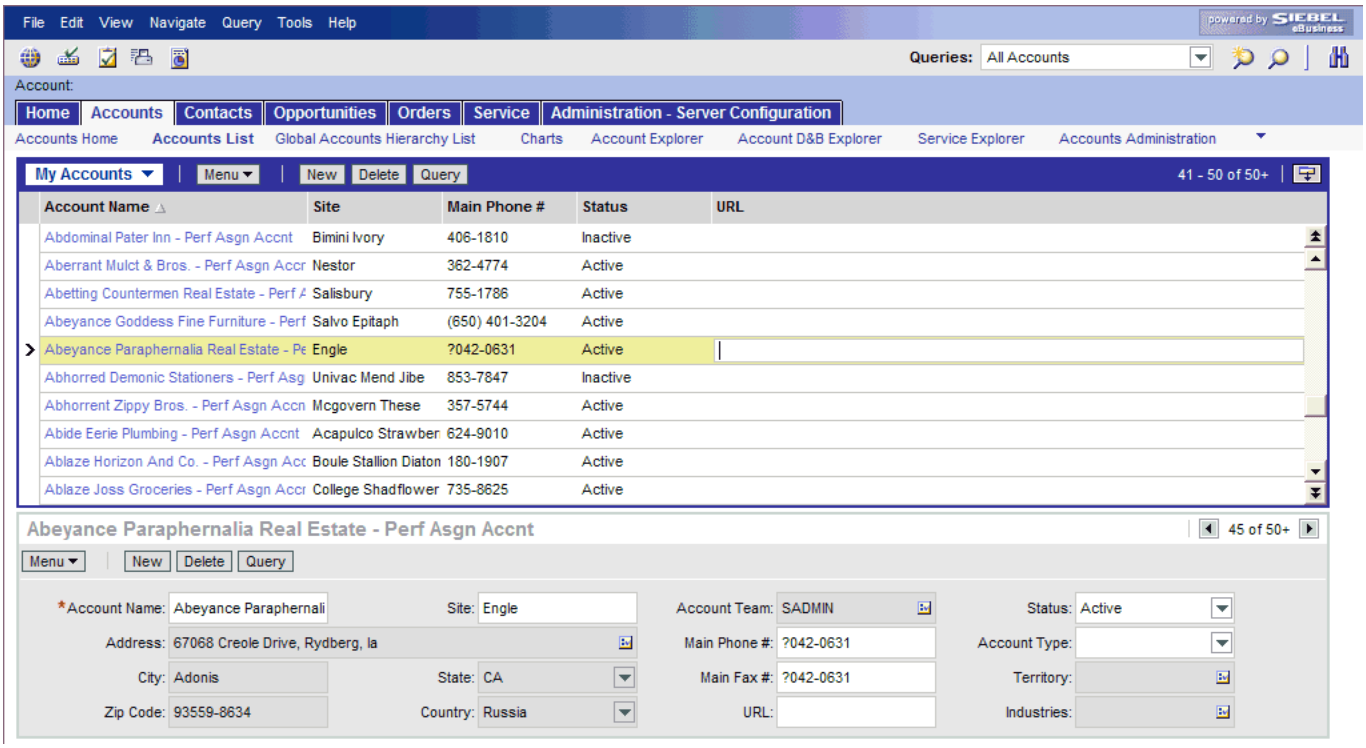
About Access Control

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 start of the window. In the following example, 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.

For example, the following image 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.



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:

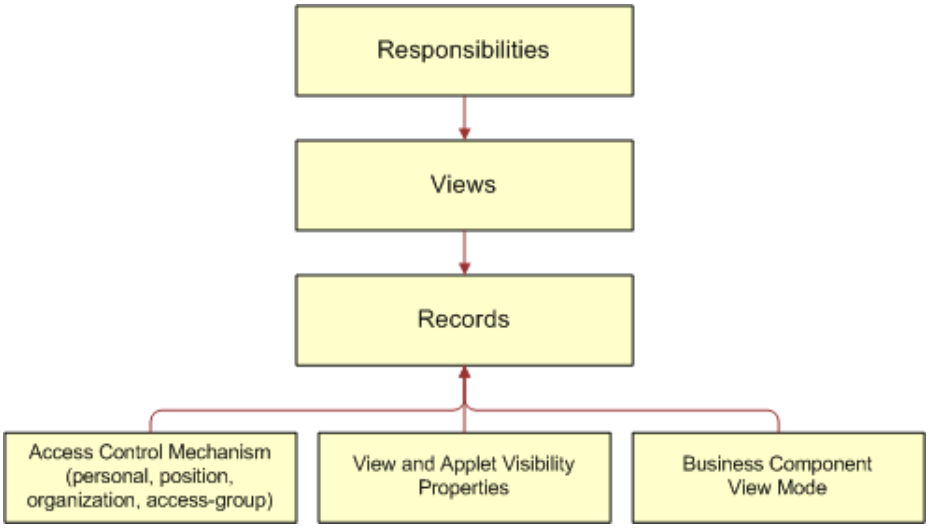
- **View-level access control.** A screen is composed of views, and the collection of views to which users have access determines the application functionality available to them. Access to views is determined by responsibilities.

  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*.

- **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*
  - *Access Control for Data*
- **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*.

The following image illustrates the Siebel access control elements. As shown in this image, responsibilities provide access to views, and the data records visible to a user on a view are determined by the type of access control (personal, position, organization, access group) that applies to the data, the business component view mode, and view and applet visibility properties.



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*.

Parties are categorized into the following party types: Person, Position, Organization, Household, User List, and Access Group. The following table describes the qualitative differences among different parties and identifies the applicable party type for each party.

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.
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.
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.
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.

Party	Party Type	Examples	Distinguishing Features
			• An account can be promoted to a partner organization.
Division	Organization	• An organizational unit within your company such as Manufacturing or Corporate. • A group of people operating within a particular country.	• A division exists for the purposes of mapping a company's physical structure into the Siebel database and for providing a container for position hierarchies. • A division can have a parent division. It can also have child divisions. • Data cannot be associated directly with a division. (Divisions that are not designated as organizations do not drive visibility.)
Organization	Organization	• An organizational unit within your company, such as your European organization. • 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.
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

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.

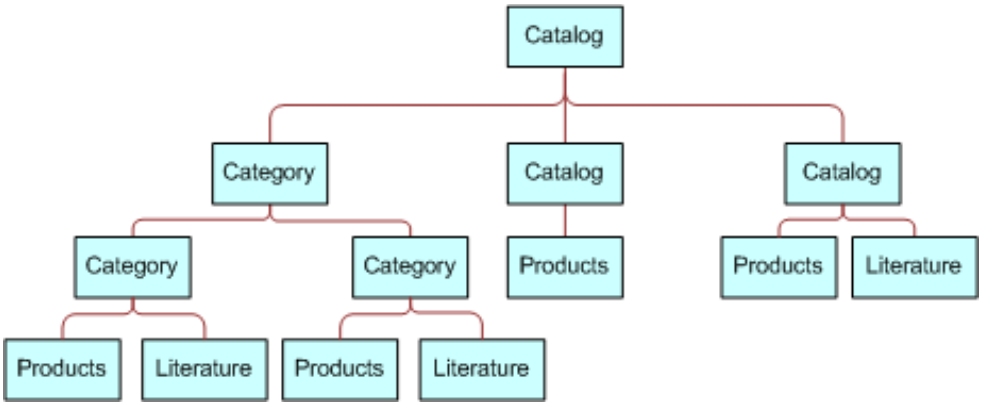
- **Other data**
  - Other data includes referential data that is not master data, such as price lists, cost lists, rate lists, and SmartScripts.
  - Access is controlled at the data item level.

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 the following figure.



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

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*.
- *Position access control.* This includes single-position, team, and manager access control. For details, see:
  - *About Position Access Control*
  - *About Single-Position Access Control*
  - *About Team (Multiple-Position) Access Control*
  - *About Manager Access Control*
- *Organization access control.* This includes single-organization, multiple-organization, and suborganization access control. For details, see:
  - *About Organization Access Control*
  - *About Single-Organization and Multiple-Organization Access Control*

    - *About Suborganization Access Control*

- *All access control.* For details, see *About All Access Control*.
- *Access-group access control.* For details, see *About Access-Group Access Control*.

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

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*.
- **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*.
- **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*.

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

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*. For information about implementing access control in a view, see *Listing View Access Control Properties*.

Related Topic

Access Control Mechanisms

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*. For information about implementing access control in a view, see *Listing View Access Control Properties*.

Related Topic

Access Control Mechanisms

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

Access Control Mechanisms

Listing View Access Control Properties

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*.
- **Multiple-organization access control.** You can associate multiple organizations with individual data. For details, see *About Single-Organization and Multiple-Organization Access Control*.

- **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*.

> **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*.

A contact user is indirectly associated with an organization through the proxy employee specified for a Siebel customer application. For information about proxy employees and access control, see the following topics:

- *Security Adapter Authentication*
- *Seed Data*
- *Access Control Mechanisms*

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.

The information in the following table 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.

Object Type	Object	Relationship
Customer data	Account	Multiple
Customer data	Competitor	Multiple
Customer data	Contact	Multiple
Customer data	Forecast Series	Multiple
Customer data	Household	Multiple
Customer data	Marketing Event/Activity	Multiple

Object Type	Object	Relationship
Customer data	Opportunity	Multiple
Customer data	Order	Multiple
Customer data	Partner	Multiple
Customer data	Product Defect	Multiple
Customer data	Project	Multiple
Customer data	Quote	Multiple
Customer data	Service Request	Multiple
Customer data	User List	Multiple
Referential data (includes master data)	SmartScript	Multiple
Referential data (includes master data)	Literature	Multiple
Referential data (includes master data)	Price List	Multiple
Referential data (includes master data)	Cost List/Rate List	Multiple
Referential data (includes master data)	Period	Single
Referential data (includes master data)	Product	Multiple
Referential data (includes master data)	Catalog	Not Applicable (catalogs use access-group access control)
Administrative data	Employee	Multiple
Administrative data	Division	Single
Administrative data	List of Values Type	Multiple
Administrative data	List of Values	Single

Object Type	Object	Relationship
Administrative data	Position	Single
Administrative data	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*. For information about business component view modes, see *Viewing Business Component View Modes*.

Related Topic

Access Control Mechanisms

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

Viewing Business Component View Modes

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

Viewing Business Component View Modes

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 earlier 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 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*.

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

Access Control Mechanisms

About Implementing Access-Group Access Control

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*.
- **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*.

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*
- *About Planning for Divisions*
- *About Planning for Organizations*
- *About Planning for Positions*
- *About Planning for Responsibilities*

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 the following table.

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*.
Positions	Y	Control the data set (records) to which a user has access. See *About Position Access Control*.
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

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

About Planning for Organizations

About Planning for Positions

About Planning for Responsibilities

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

About Planning for Divisions

About Planning for Positions

About Planning for Responsibilities

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.)

You cannot make a position obsolete by setting the End Date. This field records only the end date for the current employee associated with the position. It does not make the position obsolete after that date has passed.

CAUTION: Do not delete or merge positions because doing so renders the primary position invalid.

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

About Planning for Divisions

About Planning for Organizations

About Planning for Responsibilities

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* and *Managing Tasks Through Responsibilities*.

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

About Planning for Divisions

About Planning for Organizations

About Planning for Positions

Setting Up Divisions, Organizations, Positions, and Responsibilities

This topic outlines procedures for setting up divisions, organizations, positions, and responsibilities. For more information, see the following topics:

- *Setting Up Divisions*
- *Setting Up Organizations*
- *Setting Up Positions*
- *Setting Up Responsibilities and Adding Views and Users*

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.

Field	Guideline
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

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. After updating the Siebel repository, you must publish and deliver those updates to the Siebel runtime repository for them to take effect. 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*.
- **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*.

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*.
- **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*.
- **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*.

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*.

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

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*.

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*.

For additional information on using responsibilities to provide access control, see the following topics:

- *About Associating a Responsibility with Organizations*
- *Local Access for Views and Responsibilities*
- *Read Only View for Responsibilities*
- *Assigning a Responsibility to a Person*
- *Using Responsibilities to Allow Limited Access to Server Administration Views*

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 Topics

Responsibilities and Access Control

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*.

Related Topic

Responsibilities and Access Control

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.

Note: Responsibilities and their relationship to Views can be Workspace enabled in your development environment. If they have been Workspace enabled in your development environment and you are working in that environment, then you can only modify them in an editable Workspace. You do not need an editable Workspace to create and edit Responsibilities and their relationship to Views in your Production environment.

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

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

Assigning a Primary Responsibility

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*.
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 Security Profile using the Siebel Management Console.

Section Under Security Profiles	Parameter	Value
Basic Information	Authorization Roles (comma-separated) For more information about setting this parameter, see *Parameters for Configuring Security Adapter Authentication*.	Siebel Administrator,SubAdminRole

   For information on the Security Profile, see *About Authentication for Siebel Gateway Access*.
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

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.

The following table shows the fields in the BusComp View Modes list that determine the allowable visibility for a business component.

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.

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.
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.
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 interface.

Value	Description
None	Do not allow any direct operations on the business component from scripting interfaces.

Value	Description
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.
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 the next step in this procedure). 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.

Value	Description
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.

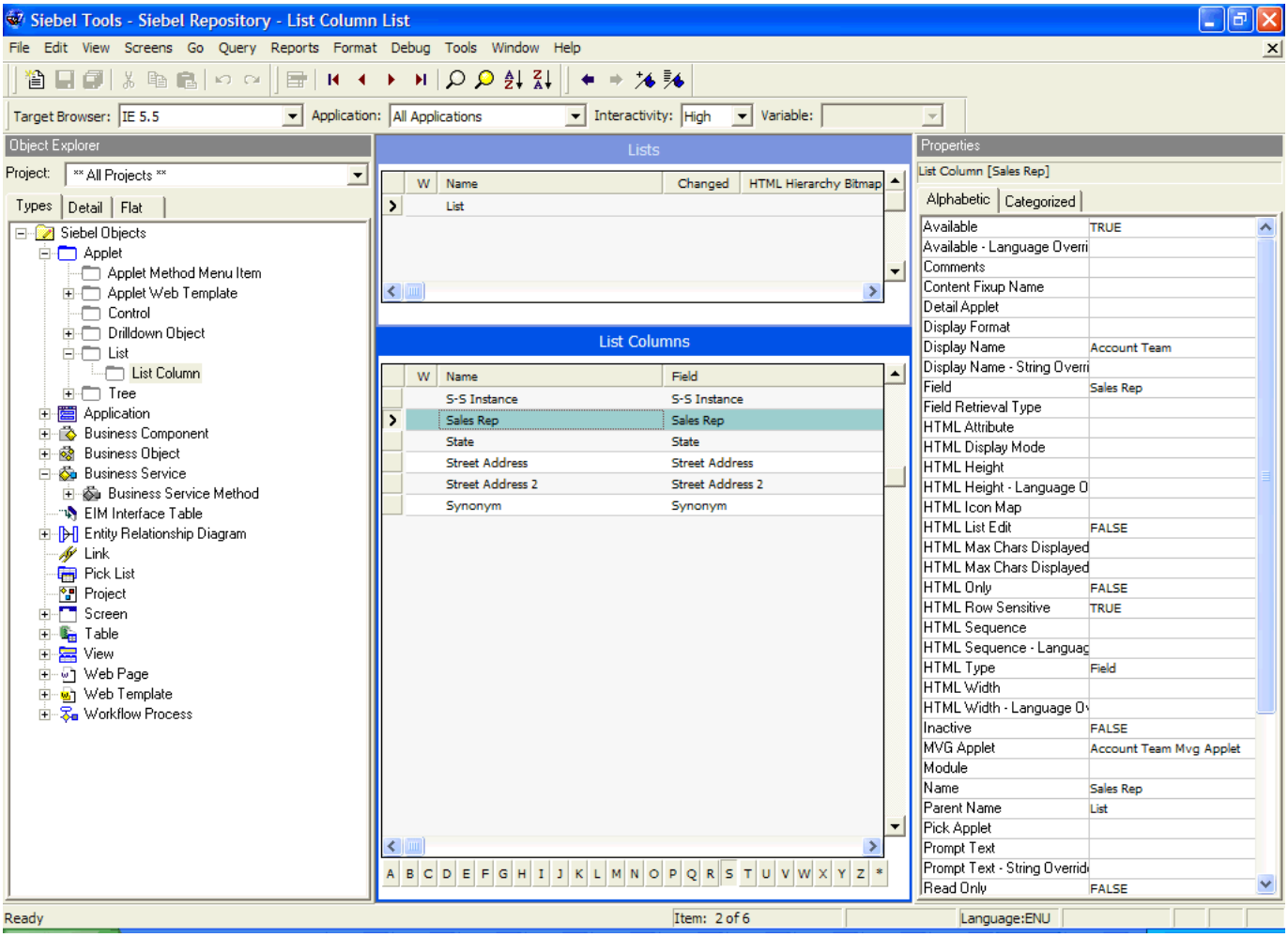
To view an applet's access control properties

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 + (plus) to expand the subtree for a subcomponent, and then click its subcomponent.

   A detail list for the subcomponent appears after the Applets list. Two applet properties in particular contribute to data visibility: Business Component and Display Name.

4. In the Object Explorer, choose Applet, List, and then List Columns.
   As shown in the following figure, 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.



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*.

    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.

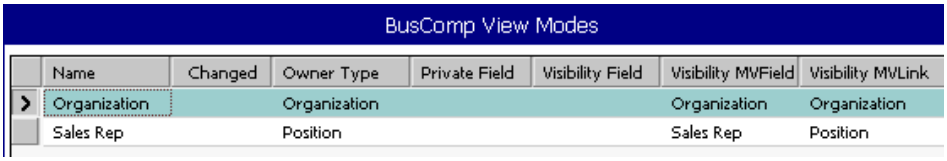
  In Admin mode, every record in a view that uses team access control is visible, even those with no primary position designated. (This mode is distinct from *All* visibility, which shows all records that have a primary team member designated.)

  > **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. After updating the Siebel repository, you must publish and deliver those updates to the Siebel runtime repository for them to take effect. For more information about required practices when using Siebel Tools, see *Configuring Siebel Business Applications* .

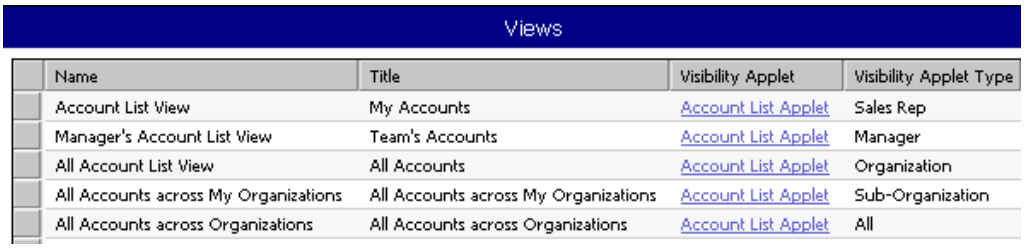
The following image shows the BusComp View Modes list in Siebel Tools for the Account business component. As indicated by the Owner Type field, organization and position view modes are allowed. As indicated in Visibility MVField, accounts can be associated with multiple organizations and multiple positions (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

The following image 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

These five example views provide different lists of account data because they have different visibility applet types specified, as shown in the following table.

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.

View	Visibility Applet Type	Data Access
		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

Viewing Categorized Data (Users)

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.

The following image illustrates one access control structure that solves this business problem. 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.

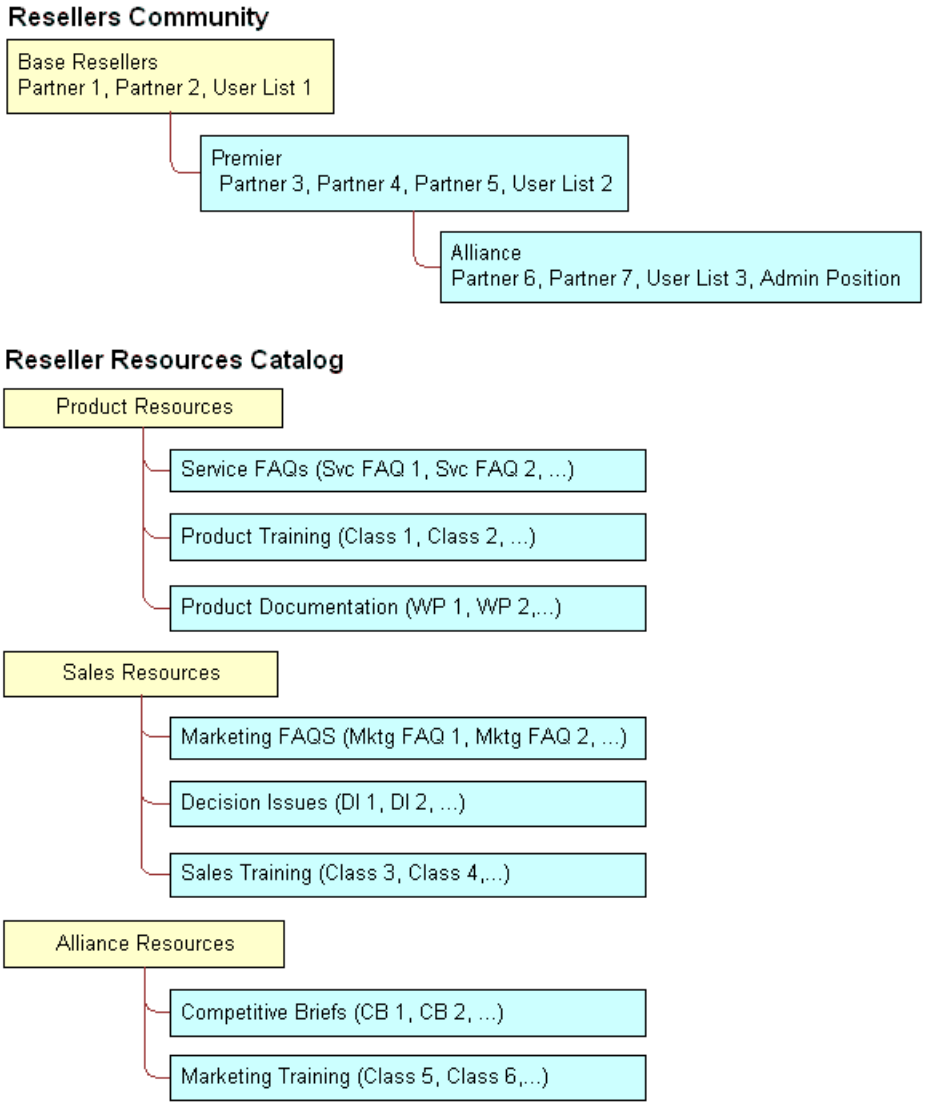
Apply the following principles to construct this structure:

- **Resellers Community.** Construct the Resellers Community so 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.

- **Reseller Resources Catalog.** Construct the Reseller Resources Catalog so 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

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

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*.

- 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*.

- *Administering Access Groups*.

  Administer access groups; build the access groups and modify their structures as needed.

- *Associating Access Groups with Data*.

  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

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*.
- Associate positions with employees and partner users.

  For information on this task, see *Adding a New Employee* and *About Adding a New Partner User*.
- Maintain position hierarchies.

  For information on this task, see *About Position Access Control* and *About Planning for Positions*.

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*. 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*. For information on planning for organizations, see *About Organization Access Control* and *About Planning for Organizations*.

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*.

The following procedure describes how to create a user list and add users to it. You can delete users from a user list similarly.

To create a user list

1. Navigate to the Administration - Group screen, then the User Lists view.
2. In the User Lists list, add a new record.

   A new user list record appears.
3. Enter a name for the user list. Optionally, change the default entry for Group Type.
4. Save the record.
5. To add users to the user list you created, select the list.
6. In the Users list at the end 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.

Related Topic

Implementing Access-Group Access Control

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 highest node of an access group hierarchy. For information about access groups, see *Access Control for Parties* and *About Access-Group Access Control*.

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, using the indicated guidelines, and then save the record.

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 highest (first) 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

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, using the indicated guidelines, and then 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 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, using the indicated guidelines, and then save the record.

Field	Guideline
Admin	Set this flag to allow users in this access group to administer this category.

Field	Guideline
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

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*
- *Assigning a Primary Responsibility*
- *Exporting and Importing Tab Layouts*

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

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

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

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*
- *Creating Task Links for a Responsibility*

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 that you selected earlier in this procedure.
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.
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 empty, then tasks are displayed in the order that you list them here.
Image	Select the graphic image that is displayed as a hyperlink next to this task in the task list.
Group	This field is used if search specifications are applied to filter the tasks that are displayed in the task applet, if multiple task applets are associated with the responsibility.

Administering Access Control for Business Services

Business services can be accessed by all users by default. However, the administrator can restrict access to specified business services and business service methods. The administrator can then associate responsibilities with the restricted business services or associate the business services with responsibilities. This allows the administrator to restrict access to business services based on the end user's responsibility. To access a restricted business service, an end user must be associated with the responsibility that allows access to the restricted business service. An end user who is assigned more than one responsibility can access any restricted business service that is associated with one of his or her responsibilities.

For business services that allow you to specify a view mode to access data, you can specify which view mode can be used by different responsibilities. The following figure shows two examples of view modes that can be associated with a responsibility to restrict the set of data records a user with the responsibility accesses.

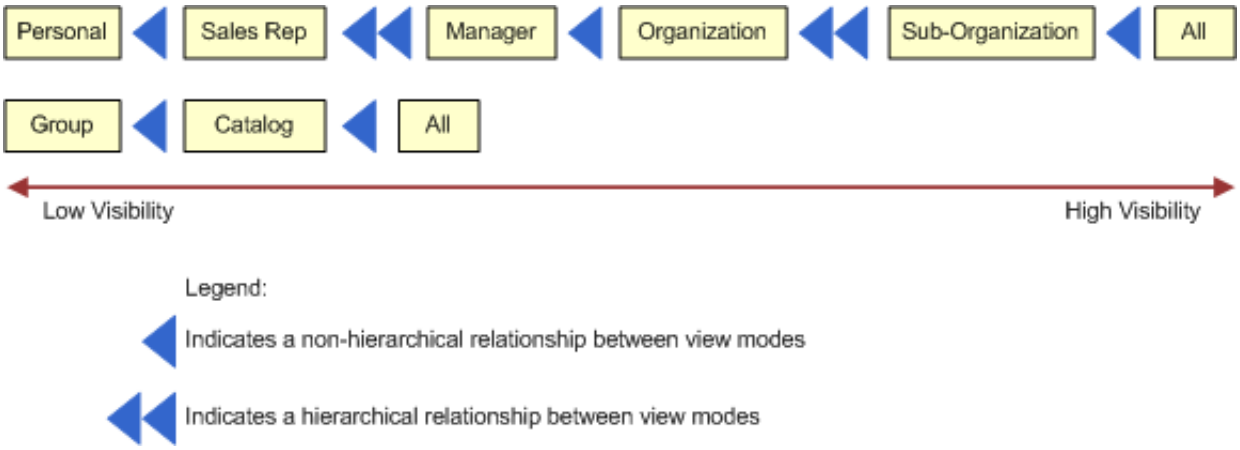
- The view modes in the first example are as follows:

1 Personal, 2 Sales Rep, 3 Manager, 4 Organization, 5 Sub-Organization, 6 All.

- The view modes in the second example are as follows:

1 Group, 2 Catalog, 3 All.

The level of visibility broadens as you move from 1 to 6 in the first example and from 1 to 3 in the second example; for example, the Manager (3) view mode grants access to more data than the Sales Rep (2) view mode.



The image 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*
- *Associating a Responsibility with a Business Service*
- *Example of Associating a Responsibility with Business Service Methods*
- *Clearing Cached Business Services*
- *Disabling Access Control for Business Services*

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 that you selected in the preceding step.

The Business Service dialog box displays the list of business services that are currently associated with the responsibility that you selected.

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 that you selected earlier in this procedure, 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 that you selected earlier in this procedure 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 then go to Step 13 of this procedure. If not, continue to the next step in this procedure.

   > **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 that you selected earlier in this procedure, 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 that you selected earlier in the procedure 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

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.

Note: Responsibilities can be Workspace enabled in your development environment. If they have been Workspace enabled in your development environment and you are working in that environment, then you can only add a Business Service Method to them in an editable Workspace.

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 earlier in this procedure, 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 that you selected in the preceding step 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 in this procedure. If not, continue to the next step in this procedure.

   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 that you selected earlier in this procedure, 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 that you selected earlier in this procedure must support view modes to allow you to select a value from the Broadest Visibility list.

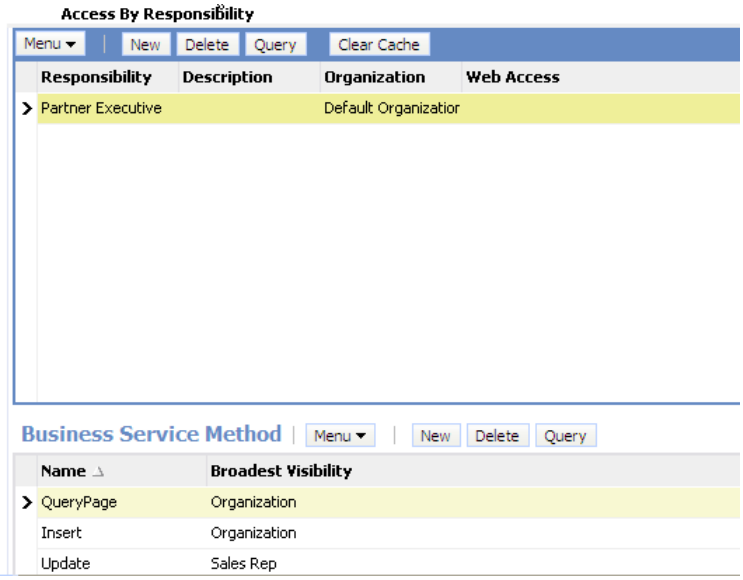
13. Step off the record to save changes.

Related Topic

Administering Access Control for Business Services

Example of Associating a Responsibility with Business Service Methods

The following image 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.



A user with Partner Executive responsibility in the example illustrated in this image 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

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

Disabling Access Control for Business Services

You can use the OM - Enable Resource Access Control parameter to control access to business services in a component as follows:

- Set OM - Enable Resource Access Control to True to enable access control for business services in a component.

  This allows only users with responsibilities to access the business services in the component. Siebel checks access control each time a user accesses a business service.

  Enabling access control for business services can have an effect on response times for your Siebel Business Applications.

  > **Note:** The default value for OM - Enable Resource Access Control is True.

- Set OM - Enable Resource Access Control to False to disable access control for business services in a component.

  This allows everyone to access the business services.

The following procedure demonstrates how to set the value for OM - Enable Resource Access Control for a selected component.

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

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*
- *Associating a Responsibility with a Business Service*

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, remove, delete, or modify a responsibility in the Responsibilities view (Responsibilities List View) or even modify or rearrange the views for a responsibility or the responsibilities for a user, then you must clear the cache as

shown in the following procedure 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 the Clear Cache button.

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

This 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, previously described, 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.

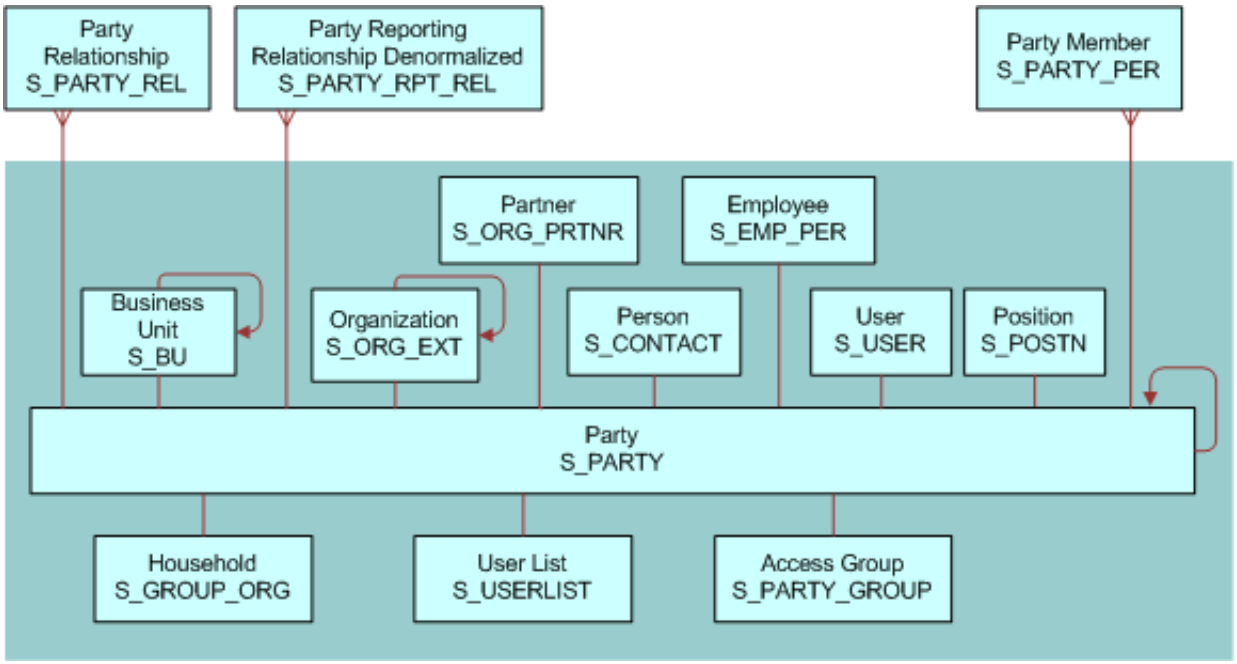
Party Data Model

The S_PARTY table is the base table for all of the parties listed in *Access Control for Parties*: Person (or Contact), User, Employee, Position, Partner User, 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 the following image, the base table (S_PARTY) 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 box (Party Relationship, Party Reporting Relationship Denormalized, and Party Member) are used to define relationships among parties.



The following subtopics illustrate how the party data model applies to various particular parties:

- *How Parties Relate to Each Other*
- *Person (Contact) Data Model*
- *User Data Model*
- *Employee Data Model*
- *Position Data Model*
- *Account Data Model*

- *Division Data Model*
- *Organization Data Model*
- *Partner Organization Data Model*
- *Household Data Model*
- *User List Data Model*
- *Access Group Data Model*

How Parties Relate to Each Other

Parties have some required relationships as follows:

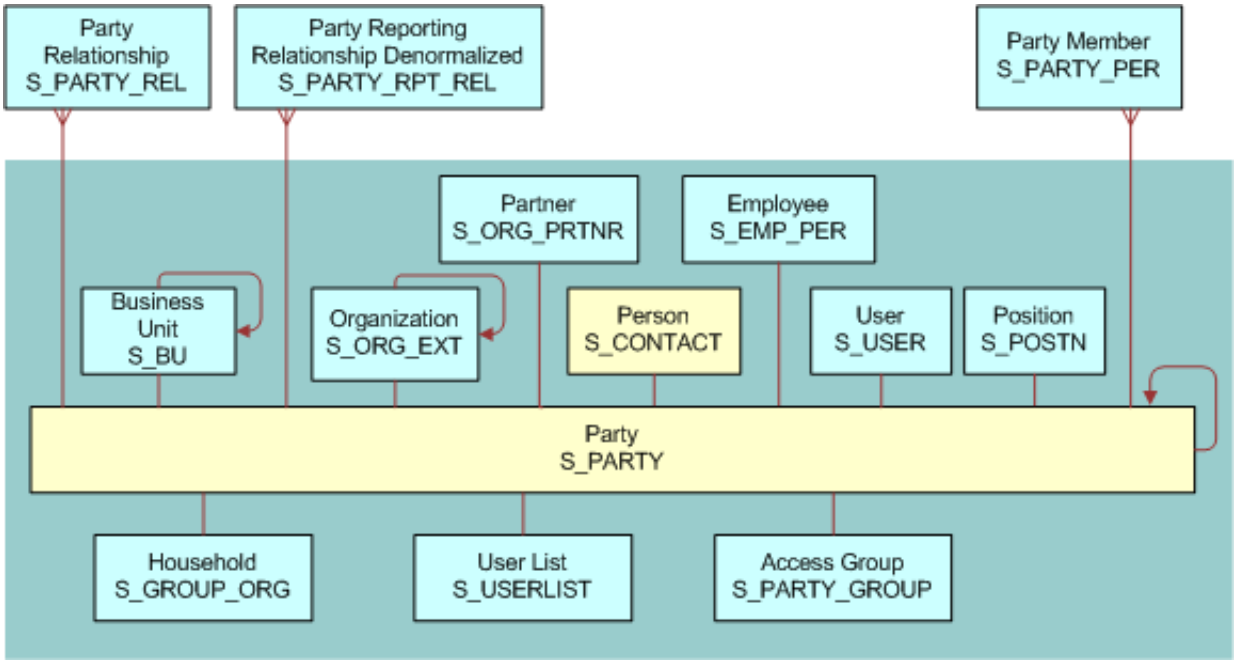
- Divisions, organizations, and accounts are instances of the Organization party type.
- A division, internal or partner, is also an organization if its internal organization flag is TRUE (INT_ORG_FLG = "Y") and it has an associated S_BU record.
- Every division is associated with one organization: either 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 the following image, the base table (S_PARTY) 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.

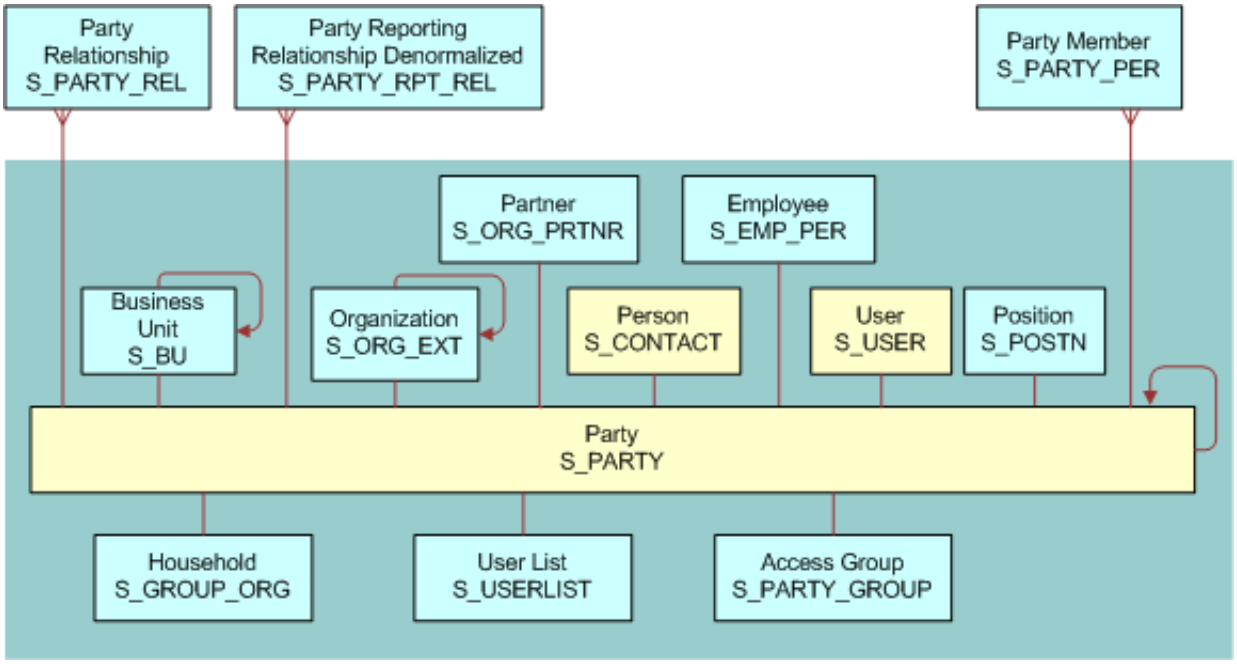


User Data Model

In the following image, the base table (S_PARTY) 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.

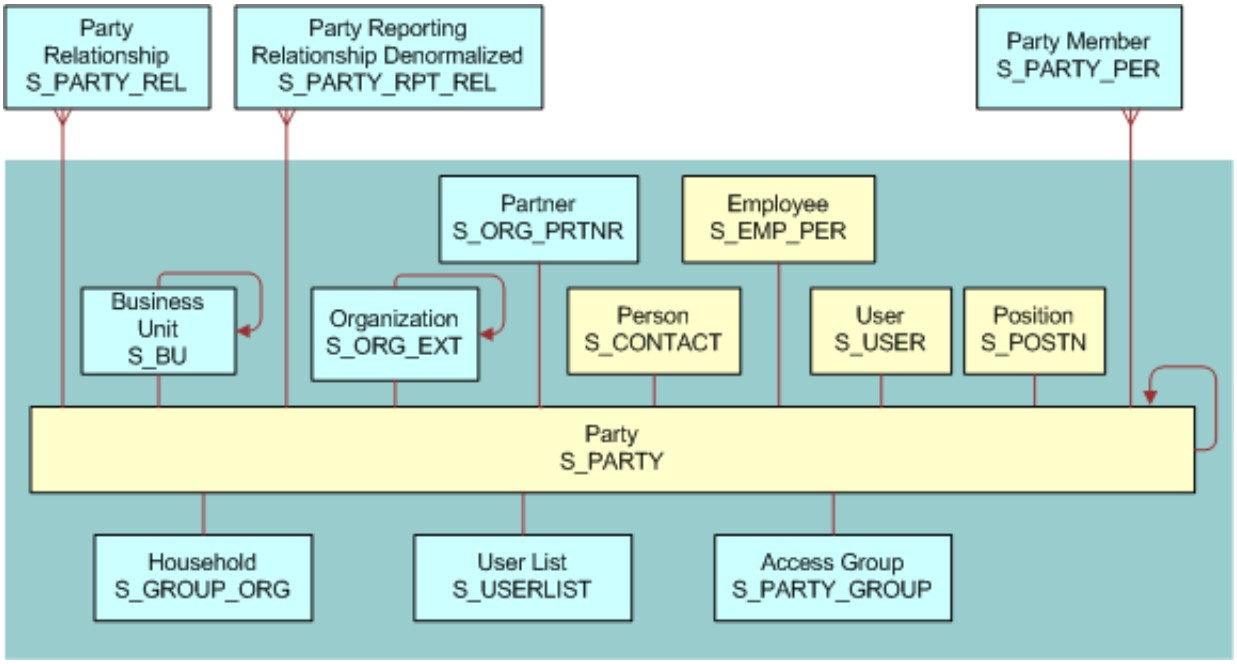


Employee Data Model

In the following image, the base table (S_PARTY) 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:

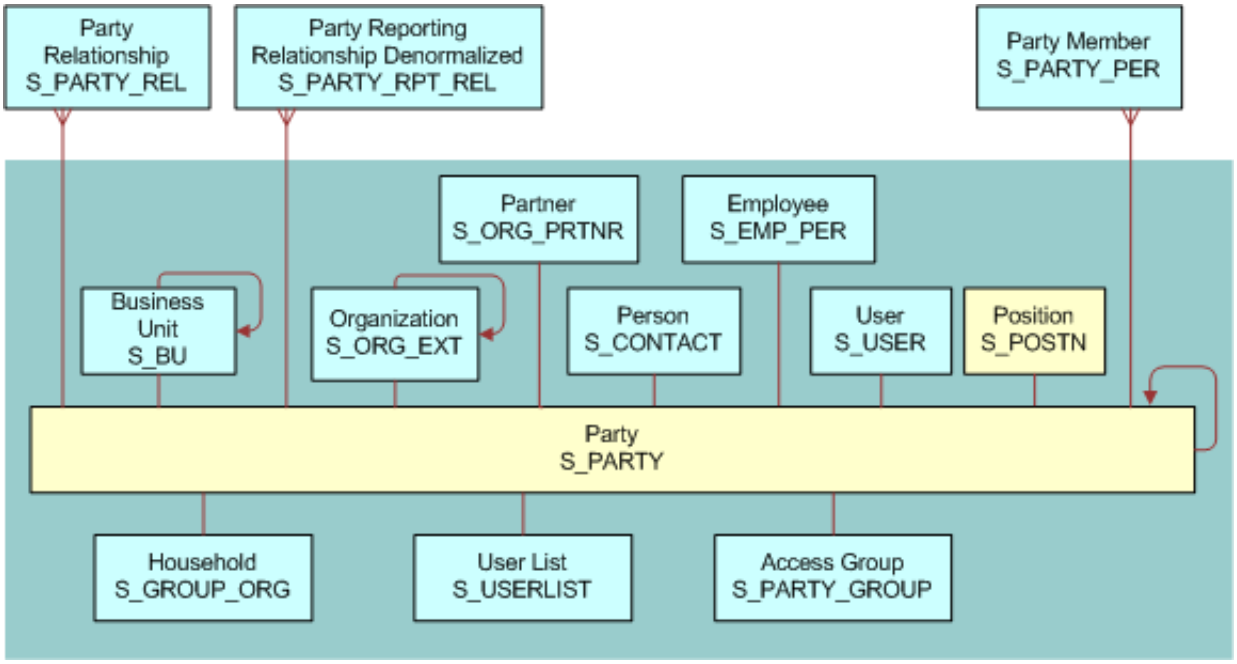
- S_EMP_PER provides employee data for this user.
- A position defined using the S_POSTN table is typically (but not necessarily) associated with an employee.
    - If the organization to which the position belongs is not a partner organization, then the employee is an internal employee.
    - If the organization is a partner organization, then the employee is a partner user.



Position Data Model

In the following image, the base table (S_PARTY) and extension table (S_POSTN) that define a Position are highlighted.

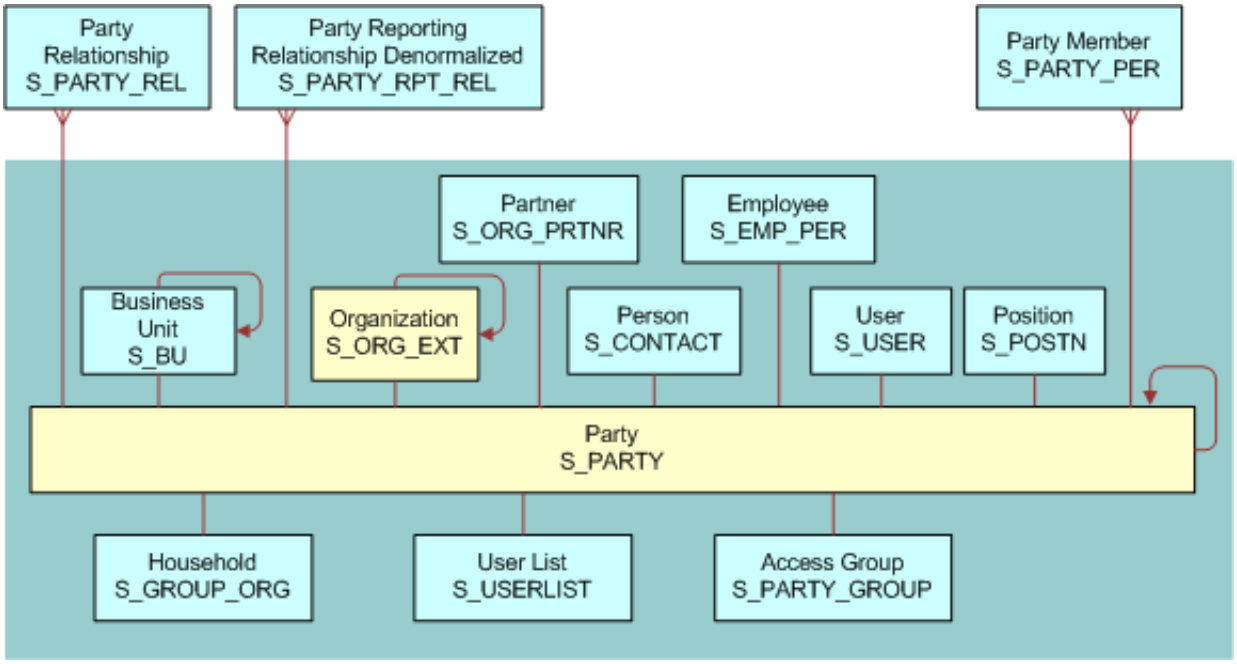
Note: In positions, as in other areas of your Siebel application, foreign key references are implemented with the ROW_ID column in the base tables. The ROW_ID column is not visible in the user interface and cannot be changed manually. This is because the integrity between the various base tables would 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).



Account Data Model

In the following image, the base table (S_PARTY) and extension table (S_ORG_EXT) that define an Account are highlighted.

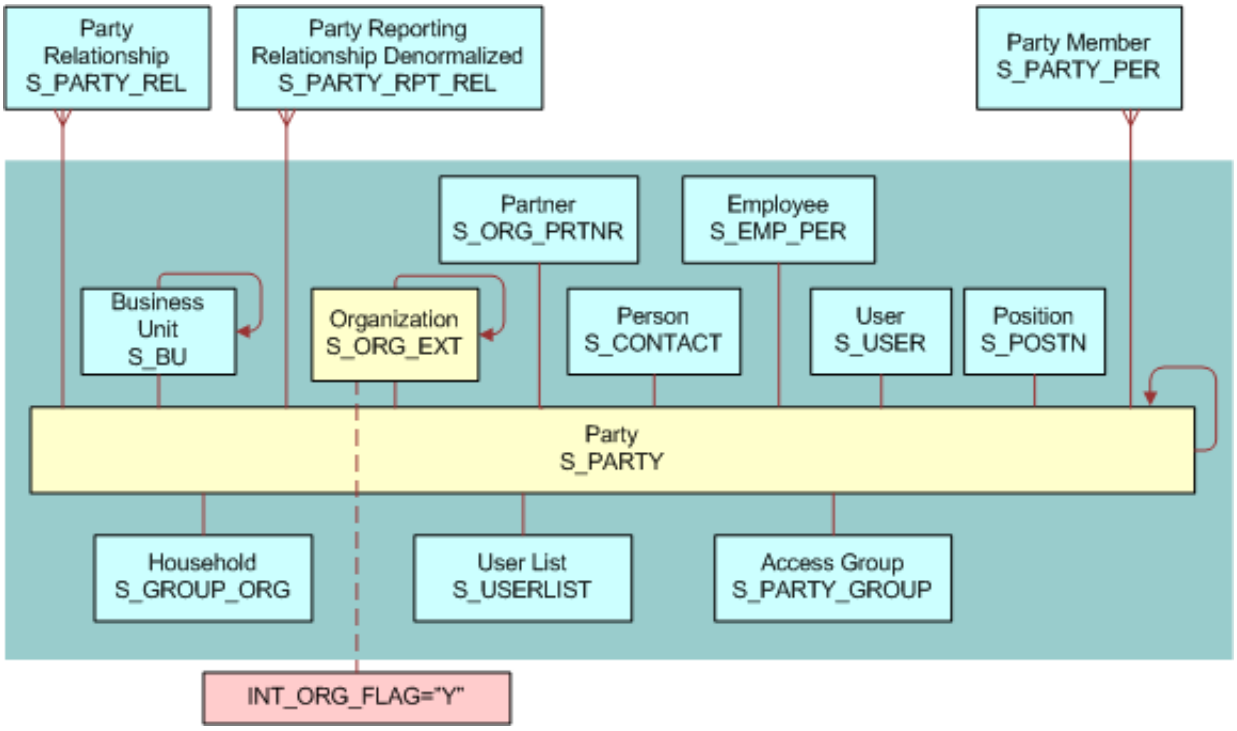
Note: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.



Division Data Model

In the following image, the base table (S_PARTY) 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.

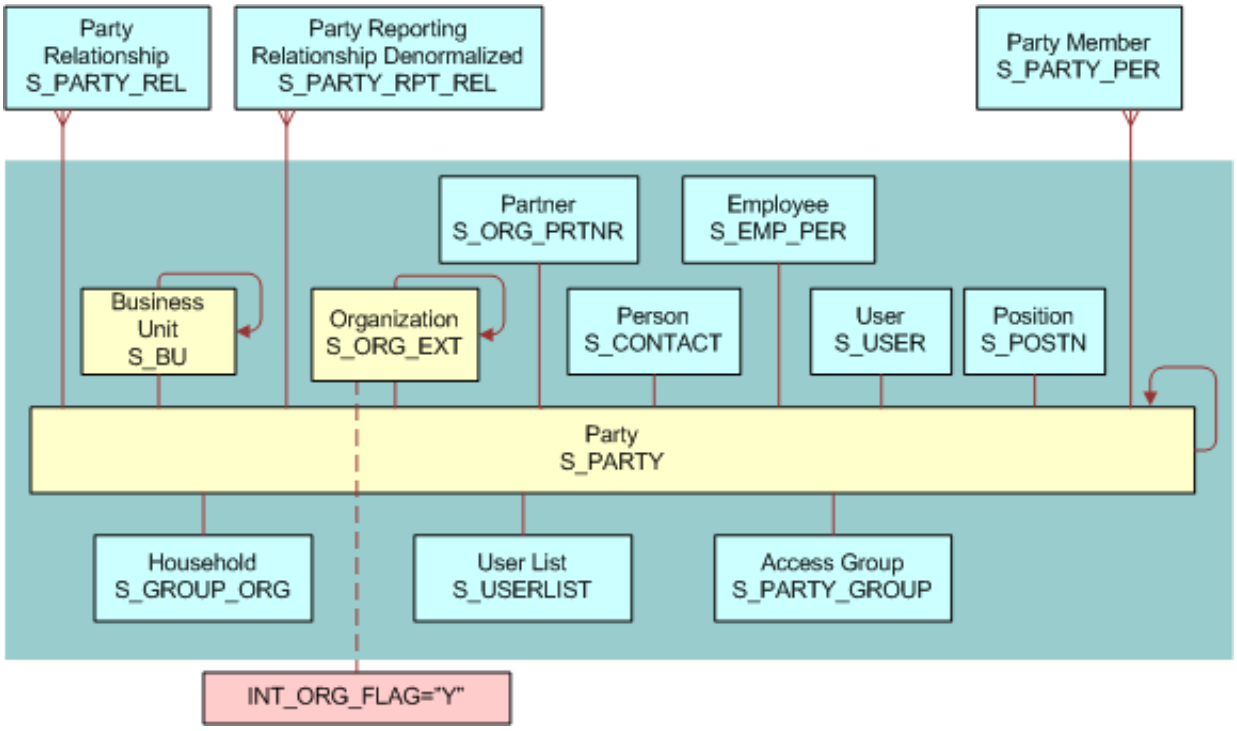
Note: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.



Organization Data Model

In the following image, the base table (S_PARTY) 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.

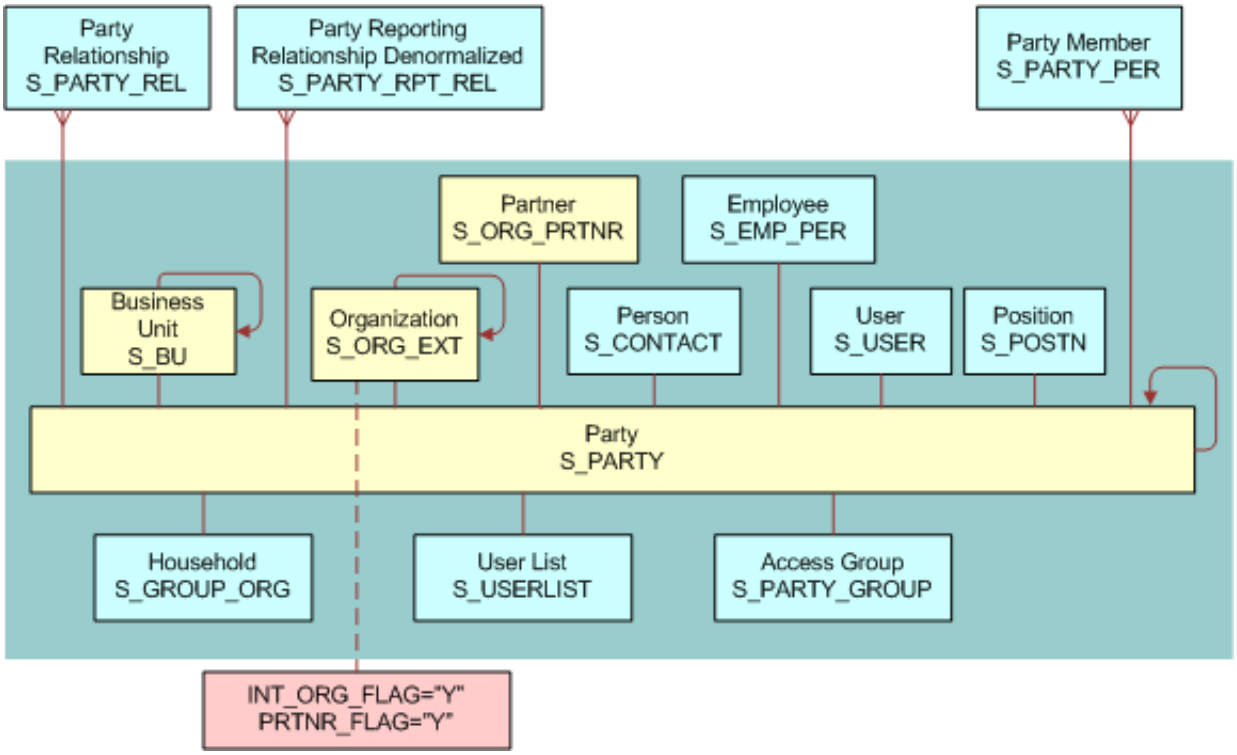
Note: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.



Partner Organization Data Model

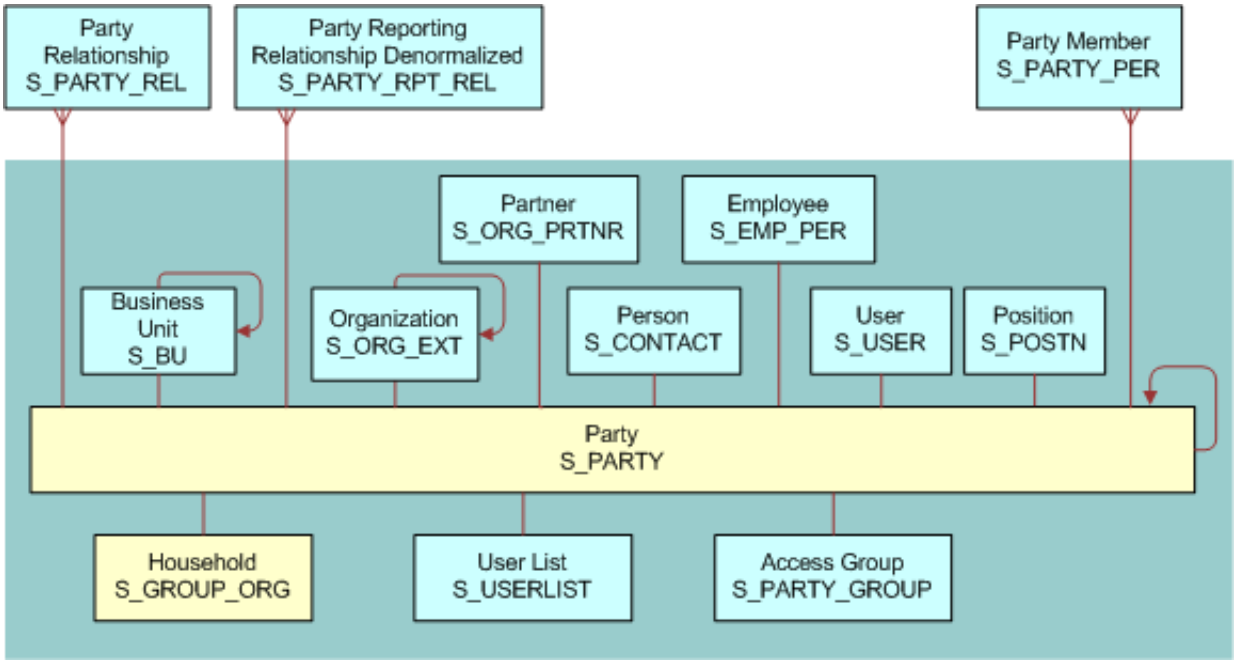
In the following image, the base table (S_PARTY) and extension tables (S_ORG_EXT, S_BU, and S_ORG_PRTNR) that define a Partner Organization are highlighted. A Partner Organization is the same as an Organization but the flag PRTNR_FLG in S_ORG_EXT qualifies it as a Partner Organization.

Note: Accounts, Divisions, Organizations, and Partner Organizations share many of the same data model elements.



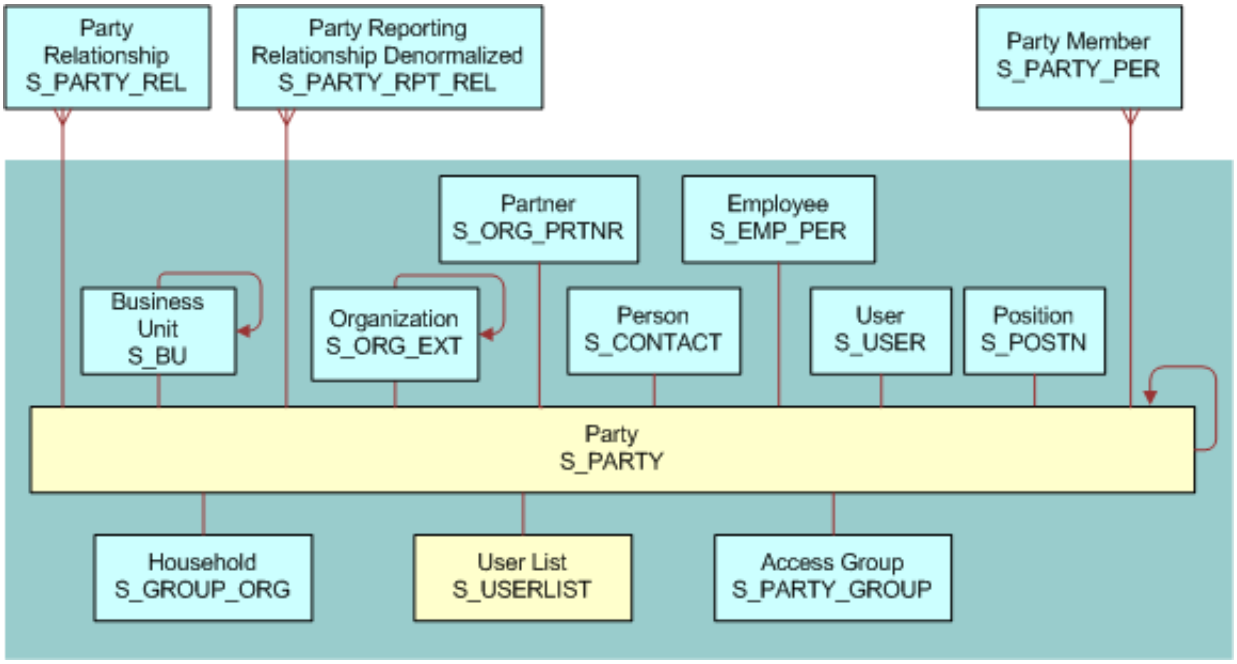
Household Data Model

In the following image, the base table (S_PARTY) and extension table (S_ORG_GROUP) that define a Household are highlighted.



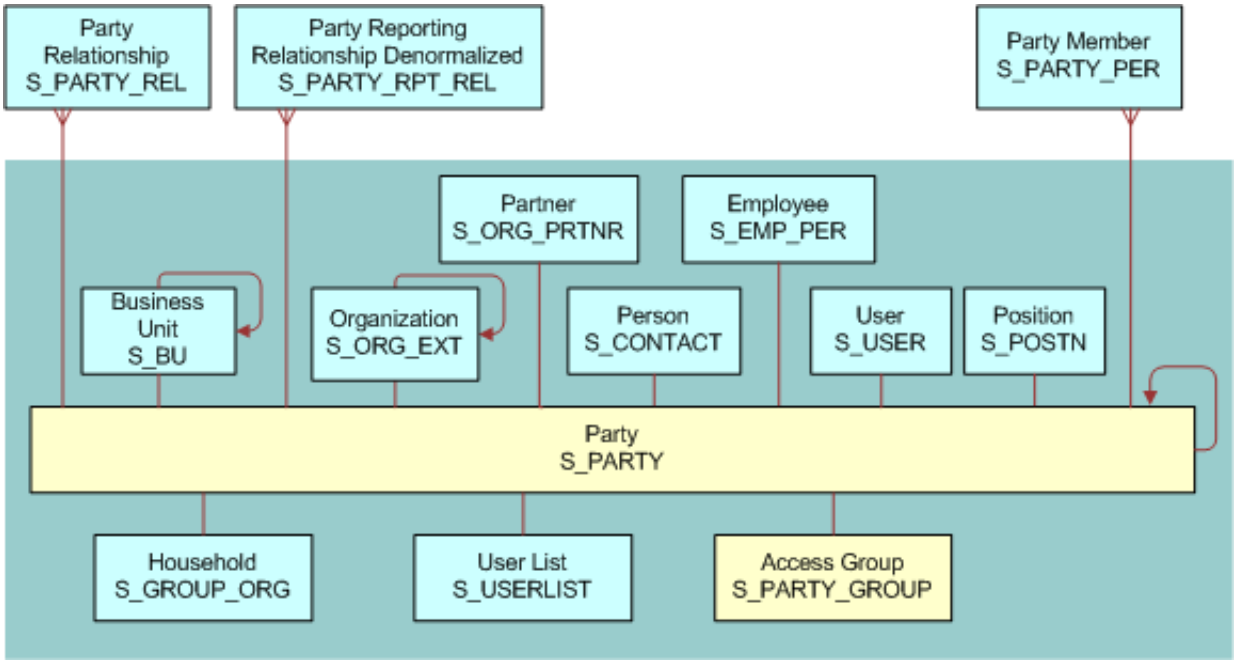
User List Data Model

In the following image, the base table (S_PARTY) and extension table (S_USERLIST) that define a User List are highlighted.



Access Group Data Model

In the following image, the base table (S_PARTY) and extension table (S_PARTY_GROUP) that define an Access Group are highlighted.


Party Relationship S_PARTY_REL
Party Reporting Relationship Denormalized S_PARTY_RPT_REL
Party Member S_PARTY_PER
Partner S_ORG_PRTNR
Employee S_EMP_PER
Business Unit S_BU
Organization S_ORG_EXT
Person S_CONTACT
User S_USER
Position S_POSTN
Party S_PARTY
Household S_GROUP_ORG
User List S_USERLIST
Access Group S_PARTY_GROUP

10 Troubleshooting Security Issues

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*
- *Troubleshooting User Registration Issues*
- *Troubleshooting Access Control Issues*

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 the following table.

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) directory.	Use database authentication instead of external authentication for administration users. Administrator users must log into the application using 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* and related sections. Alternatively, authentication for a secondary data source such as the Siebel Gateway can be configured.
Adding users or changing passwords is not reflected in the directory.	The Propagate Change parameter is set to FALSE for the security adapter.	Set the Propagate Change parameter to TRUE for the security adapter. For more information, see *Server Parameters for Siebel Gateway*.
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*.
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*.

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 the following table.

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*.
		• 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 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.

Symptom or Error Message	Diagnostic Steps or Cause	Solution
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* • *Identifying Disruptive Workflows*
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*. • 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 the following table.

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.
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*.

Symptom or Error Message	Diagnostic Steps or Cause	Solution
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 RestrictedFieldActivation user property 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: **`NoRestrictedFieldActivationModenumber valueOfVisibilityMode`** For example, the following entry overrides the default behavior in the Personal view mode: **`NoRestrictedFieldActivationMode1 Personal`**
Multiple sessions of an eCustomer application are opening in the same browser, without throwing any session warning message.	An eCustomer can open multiple sessions of eCustomerObjMgr_enu in the same browser (all HTML5-compliant browsers) without receiving a session warning message.	The multiple sessions warning message only works on regular (login) sessions and does not work on anonymous browsing sessions that circumvent the login page (for example: SWECmd=GotoView). There is no request for login if an anonymous user has access to the home page and the object manager session is directed to the home screen (via SWECmd=GotoView). For the multiple sessions warning message to appear in an anonymous browsing session, you must request the login page using a regular session instead of anonymous browsing. Instead of using the SMECmd=GotoView mechanism in the application interface, define the start page at the application level (for example, in Siebel Tools).

11 Authentication-Related Configuration Parameters

Authentication Related Configuration Parameters

This chapter describes the configuration parameters that are applicable to implementing a security adapter and other important authentication and security-related parameters that must be configured in the Siebel Management Console. It includes the following topics:

- *Server Parameters for Siebel Gateway*
- *Security Profile Configuration for Siebel Gateway*
- *Parameters for Configuring Security Adapter Authentication*
- *Authentication and Security-Related Parameters in the Enterprise Profile*
- *Security-Related Parameters in the Server Profile*
- *Siebel Application Interface Profile Parameters*
- *Siebel Application Configuration Parameters*

Note: In general, parameter values related to security adapter configuration must be verified by your Lightweight Directory Access Protocol (LDAP) administrator or database administrator. Many values shown are examples only and might not be suitable for your deployment.

Server Parameters for Siebel Gateway

The server parameters for Siebel Gateway can be set at one or more of the Enterprise, Siebel Server, or component (Siebel Application Interface) levels in the Siebel Management Console. 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 (Siebel Application Interface) 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 Custom at the component level for the eService Object Manager component, then the Custom 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 *Security Adapter Authentication*.

> **Note:** You can set Enterprise (profile) parameters and Object Manager (application interface profile) parameters on the Siebel Gateway using Siebel Server Manager or the Siebel Management Console. However, you cannot set security profile parameters using Siebel Server Manager, you must use the Siebel Management Console to set security profile parameters. For information about using Siebel Server Manager to edit parameters on Siebel Gateway, see *Siebel System Administration Guide* . For information about editing parameters on Siebel Gateway using the Siebel Management Console, see *Configuring Security Adapters Using the Siebel Management Console*.

The following topics provide more information about the parameters you can configure for Siebel Gateway:

- *Configuring Security Adapters Using the Siebel Management Console*
- *Security Profile Configuration for Siebel Gateway*
- *Parameters for Configuring Security Adapter Authentication*
- *Authentication and Security-Related Parameters in the Enterprise Profile*
- *Security-Related Parameters in the Server Profile*

Security Profile Configuration for Siebel Gateway

The security profile, which is centrally stored in the registry, contains the configuration parameters that determine how access to Siebel Gateway is authenticated. The security profile that you define when you configure Siebel Gateway is automatically used to prepopulate the security-related parameters for various different configurations including the Siebel Gateway and Enterprise (enterprise profile).

Siebel Gateway authorization is required whether you use the Siebel Management Console, Siebel Server Manager, or other utilities to access the gateway. When a user attempts to log in to the gateway, the user's credentials are passed by the server to the authentication provider specified in the security profile, which checks that the user has the required administrator privileges to access the gateway. If it has, the gateway starts to process service requests.

> **Note:** Authentication is not required for starting the gateway, only for connecting to it.

You configure the security profile using Siebel Management Console. Any changes made to the security profile are not active until you restart the Siebel Gateway. For more information on configuring a security profile for Siebel Gateway, see *Configuring Security Adapters Using the Siebel Management Console* and *Parameters for Configuring Security Adapter Authentication*.

> **Note:** When creating a new profile, make sure that the name you choose for the profile is unique and does not already exist, otherwise profile creation will fail.

Parameters for Configuring Security Adapter Authentication

The following table describes the parameters in the Security Profile that relate to database, LDAP, or custom authentication. You set these parameters when configuring a security profile to use a database, LDAP, or custom security adapter. You define these parameters in the Data Sources section and Basic Information section under Security Profiles in the Siebel Management Console.

- You can define database authentication parameters for the following named subsystems:

  InfraSecAdpt_DB. That is, for the DBSecAdpt named subsystem or a similar security adapter with a nondefault name.

  InfraDataSource. That is, for the ServerDataSrc named subsystem or another data source.

  > **Note:** Database authentication is supported for development environments only, it is not supported for production environments.

- You can define LDAP authentication parameters for the following named subsystem:

  InfraSecAdpt_LDAP. That is, for the LDAPSecAdpt named subsystem or a similar security adapter with a nondefault name.

- You can define custom authentication parameters for the following named subsystem:

  InfraSecAdpt_Custom. That is, for the CustSecAdpt named subsystem or a similar security adapter with a nondefault name.

The named subsystem is specified as the value for the data source Security Adapter Name parameter for the database, LDAP, or custom security adapter.

Parameter	Section Under Security Profiles	Comment or Description
Name	Data Sources	Specify the name of the data source.
Type	Data Sources	Specify the type or mode of authentication you are using. The options are: • Database Authentication (Basic mode for development only) • Database Authentication (Advanced mode) • Lightweight Directory Access Protocol (LDAP) Authentication • Custom Security Authentication (using Security SDK) 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.
Host Name	Data Sources	Specify the host name for the data source, such as the host name of the database server for database authentication.

Parameter	Section Under Security Profiles	Comment or Description
		Note that you may have to include the IP address if the server is configured to listen only with the IP address: • For Oracle and DB2: Actual Host FQDN. • For MSSQL: **`server\<instance>`**. • For LDAP: LDAP Host. You must specify the FQDN (fully qualified domain name) of the LDAP server, not just the domain name. For example, specify ldapserver.example.com, not example.com.
Port	Data Sources	Specify the port number for the source, such as the port number of the database server for database authentication. For example, specify: • 51510 for DB2 • 389 for LDAP, 636 for LDAPS • 151 for Oracle • 32100 for MSSQL
Application User Distinguished Name (DN)	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify 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 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. You must implement an application user.
Application Password	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify the password for the user defined by the Application User Distinguished Name parameter. In an LDAP directory, the password is stored in an attribute. The application password must be encrypted. Clear text passwords are not supported for the LDAPSecAdpt named subsystem. For more information, see *Changing Encrypted Passwords Using the Siebel Management Console*.
Base Distinguished Name (DN)	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify 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 after this directory. For example, 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.
Custom Library	Data Sources	Name of the custom security adapter implementation. For example, custsecadpt in the case of custsecadpt.so, custsecadpt.dll and so on. Do not give the file extension.

Parameter	Section Under Security Profiles	Comment or Description
	This option appears if you select Custom Authentication.	
SQL Style of Database	Data Sources This option appears if you select Database Authentication or Custom Authentication.	Specify the SQL style for your Siebel database. Specify one of the following: • Oracle Database Enterprise Edition • Microsoft SQL Server • IBM DB2
Database Service Name	Data Sources This option appears if you select Database Authentication.	The database name: • For the DB2390 version of DB2, you must deploy the db2jcc_license_cisuz.jar file into the **webapp/siebel/lib** directory of the Siebel Application Interface and Siebel Gateway. • For MSSQL, specify the database name. • For Oracle, the database service name can hold the SID or Service Name as dictated by the Oracle database installation (listener.ora file).
Table Owner	Data Sources This option appears if you select Database Authentication Basic or Advanced mode.	The table owner for the database.
CRC Checksum	Data Sources This option appears if you select Custom Authentication and only if the Custom Library parameter is Not Null.	Provide the value of the checksum performed on the applicable security adapter library (DLL). This value, applicable for the Siebel Server only, ensures that each user accesses the Siebel database through the correct security adapter. If this field is empty or contains the value 0 (zero), then no checksum validation is performed. If you upgrade your version of Siebel Business Applications, then you must recalculate the checksum value and replace the value in this field. For more information, see *Configuring Checksum Validation*.
Credentials Attribute	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify the attribute type that stores a database account. For example, if Credentials Attribute 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 space between the two key-value pairs but no space within each pair. The keywords **username** and **password** must be lowercase. If you implement LDAP 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 Algorithm	Data Sources	Specify the hash algorithm to be used for password hashing.

Parameter	Section Under Security Profiles	Comment or Description
	This option appears if you select Hash DB Password or Hash User Password.	• SHA1, which is the default value, is read-only for the Siebel Gateway security profile; for other profiles, it is editable. • SHA2 is not supported.
Hash DB Password	Data Sources This option appears if you select LDAP or Custom Authentication.	Select this check box to specify password hashing for database credentials passwords.
Hash User Password	Data Sources This option appears if you select Database Authentication Basic or Advanced mode, LDAP, or Custom Authentication.	Select this check box to specify password hashing (using the hashing algorithm specified using the Hash Algorithm parameter) for user passwords. For more information, see *About Password Hashing*.
Password Attribute Type	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify the attribute type under which the user's login password is stored in the directory. The LDAP entry must be userPassword.
Propagate Change	Data Sources This option appears if you select LDAP or Custom Authentication.	Select this check box to allow administration of the directory through Siebel Business Applications UI. When an administrator then adds a user or changes a password from within the 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 (optional)	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify the attribute type for roles stored in the directory. For example, if Roles Attribute 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*.
Shared Databases Account Distinguished Name (fully qualified domain name)	Data Sources This option appears if you select LDAP or Custom Authentication.	Specify the absolute path (not relative to the Base Distinguished Name) of an object in the directory that has the shared database account for the application. If not set, then the database account is looked up in the user's DN as usual. If set, then the database account for all users is looked up in the shared credentials DN instead. The attribute type is determined by the value of the Credentials Attribute parameter. For example, if the Shared Database Account Distinguished Name parameter is set to `"uid=HKIM, ou=people, o=example.com"` when a user is authenticated, the security

Parameter	Section Under Security Profiles	Comment or Description
		adapter retrieves the database account from the appropriate attribute in the HKIM record. This parameter's default value is an empty string.
Shared DB User Name	Data Sources This option appears if you select Configure Web Single Sign-On for Database Authentication Advanced mode, LDAP, or Custom Authentication.	Specify the user name to connect to the Siebel database. You must specify a valid Siebel user name and password for the Shared DB User Name and Shared DB Password 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 an LDAP directory. For more information, see *Storing Shared Database Account Credentials as Profile Parameters*.
Shared DB Password	Data Sources This option appears if you select Configure Web Single Sign-On for Database Authentication Advanced mode, LDAP, or Custom Authentication.	Specify the password associated with the Shared DB User Name parameter.
Security Adapter Mapped User Name	Data Sources This option appears if you select LDAP or Custom Authentication.	If this check box is selected, then when the user key name passed to the security adapter is not the Siebel User ID, then the security adapter retrieves the Siebel User ID for authenticated users from an attribute defined by the Siebel Username Attribute parameter.
Siebel Username Attribute	Data Sources This option appears if you select LDAP or Custom Authentication, and if the Security Adapter Mapped User Name check box is selected.	If set, then this parameter is the attribute from which the security adapter retrieves an authenticated user's Siebel User ID. If not set, then the user name passed in is assumed to be the Siebel User ID.
SSL	Data Sources This option appears if you select LDAP or Custom Authentication.	Specifies whether or not to enable Secure Sockets Layer for socket connections to the host.
Enable SSL	Data Sources This option appears if you select LDAP or Custom Authentication.	Specifies whether or not TLS is used for communication between the LDAP security adapter and the directory. If this check box is not selected, then TLS is not used. To use TLS, 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.
Configure Web Single Sign-On	Data Sources	Specifies that the security adapter uses Web Single Sign-On (Web SSO) authentication rather than security adapter authentication.

Parameter	Section Under Security Profiles	Comment or Description
	This option appears if you select Database Authentication Advanced mode, LDAP, or Custom Authentication.	Note that you must disable Web SSO when you configure Siebel Gateway initially (first time running Siebel Management Console). Then after you complete Siebel Gateway initial configuration and enterprise deployment, you must add the SSO parameters retrospectively using Siebel Server Manager. For more information, see *Siebel System Administration Guide* .
Trust Token	Data Sources This option appears if you select Configure Web Single Sign-On for Database Authentication Advanced mode, LDAP, or Custom Authentication.	Specifies a password to be used with Web Single Sign-On (Web SSO) authentication.
Wallet Password	Data Sources This option appears if you select SSL for LDAP or Custom Authentication.	Specifies the password to open the wallet that contains a certificate for the certificate authority used by the directory server. Note that you do not have to specify the wallet location when configuring an LDAP security adapter because the wallet file (ewallet.p12) is placed in the trust store location.
Salt Attribute Type	Data Sources This option appears if you select LDAP or Custom Authentication.	Specifies the attribute that stores the salt value if you have chosen to add salt values to user passwords. The default attribute is title.
Salt User Password	Data Sources This option appears if you select LDAP or Custom Authentication.	Select this check box to specify that salt values are to be added to user passwords before they are hashed. This parameter is ignored if the Hash User Password parameter is set to FALSE. Adding salt values to user passwords is not supported if you are using Web Single Sign-On. For more information on salt values, see *About Password Hashing*.
User Name Attribute Type	Data Sources This option appears if you select LDAP or Custom Authentication.	Specifies the attribute type under which the user's login name is stored in the directory. For example, if User Name Attribute Type 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 Security Adapter Mapped User Name check box is selected. If you implement an adapter-defined user name (the Security Adapter Mapped User Name check box is selected), then you must set the OM - Username BC Field parameter appropriately to allow the directory attribute defined by User Name Attribute Type to be updated from the Siebel client. For more information about implementing an adapter-defined user name, see *Configuring Adapter-Defined User Name*.
Connection String	Data Sources This option appears if you select Database Authentication Advanced mode.	Specify the Connection String for the Database. For more information on connection string information, *Creating Siebel Gateway Security Profile with Database Authentication Advanced Mode*.

Parameter	Section Under Security Profiles	Comment or Description
Enterprise Security Authentication Profile (Security Adapter Mode)	Basic Information	Specify the type of authentication you are using. • Database Authentication (Basic mode for development only) • Database Authentication (Advanced mode) • Lightweight Directory Access Protocol (LDAP) Authentication • Custom Security Authentication (using Security SDK) 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.
Security Adapter Name (named subsystem)	Basic Information	The chosen security adapter. • For Database Authentication Basic and Advanced modes, it is DBSecAdpt. • For LDAP Authentication, it is LDAPSecAdpt. • For Custom Authentication, it is CustSecAdpt.
Database Security Adapter Data Source	Basic Information This option appears if you select Database Authentication.	Select the security adapter data source.
Database Security Adapter Propagate Changes	Basic Information This option appears if you select Database Authentication.	Specify whether to propagate changes for the security adapter. Select this option 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 SecThickClientExtAutent system preference must also be set to True. For details, see *Setting a System Preference for Developer Web Clients*.
Authorization Roles (comma-separated)	Basic Information	Specify one or more authorization roles (which will be checked against the users logging in to the application). The default value is Siebel Administrator. This setting applies whether you are implementing security adapter authentication or Web SSO authentication.
User Name	Testing	Specify the user name for testing authentication under the specified authentication system.
Password	Testing	Specify the password for the user account used for testing.

Authentication and Security-Related Parameters in the Enterprise Profile

The following table describes the parameters in the Enterprise Profile that relate to authentication and security. You define these parameters in the Authentication section and Security Information section under Enterprise Profiles in the Siebel Management Console.

Parameter	Section Under Enterprise Profiles	Description
User Name	Authentication	The user name.
Password	Authentication	The user password.
Authentication Profile	Authentication	The authentication profile for the Enterprise.
Primary Language	Authentication	The primary language for the Enterprise deployment.
Security Encryption Level or Type	Security Information	The level or type of security encryption. The options are: • Without Encryption • TLS 1.2 (default)
Certificate Authority (CA) Certificate File Name	Security Information This option appears if the Security Encryption Level or Type parameter is set to TLS 1.2.	The name of the CA Certificate file.
Private Key File Name	Security Information This option appears if the Security Encryption Level or Type parameter is set to TLS 1.2.	The name of the private key file.
Private Key File Password	Security Information This option appears if the Security Encryption Level or Type parameter is set to TLS 1.2.	The password for the private key file.
Enable Peer Authentication	Security Information This option appears if the Security Encryption Level or Type parameter is set to TLS 1.2.	Select this option to enable peer authentication.
Validate Peer Certificate	Security Information This option appears if the Security Encryption Level or Type parameter is set to TLS 1.2.	Select this check box to validate the peer certificate.

Security-Related Parameters in the Server Profile

The following table describes the parameters in the Server Profile that relate to security. You define these parameters in the Enhanced Settings - Security section under Siebel Server Profiles in the Siebel Management Console.

Parameter	Section Under Siebel Server Profiles	Description
Server-Specific Security Encryption Settings	Enhanced Settings - Security	Select this option to configure security and encryption for communications between the Siebel Server and other servers. If you do not select this option, then the settings are inherited from the Enterprise.
Server-Specific Security Authentication Profile Assignment	Enhanced Settings - Security	Select this option to assign an existing security adapter to this Siebel Server or to specific components.
Security Encryption Level or Type	Enhanced Settings - Security This option appears if you select the Server-Specific Security Encryption Settings parameter option.	Specify the security encryption level or type. The options are: • Without Encryption • TLS 1.2 (default)
Certificate File Name	Enhanced Settings - Security This option appears if you select the Server-Specific Security Encryption Settings parameter option and the Security Encryption Type or Level parameter is set to TLS 1.2.	The password for the private key file.
Certificate Authority (CA) Certificate File Name	Enhanced Settings - Security This option appears if you select the Server-Specific Security Encryption Settings parameter option and the Security Encryption Level or Type parameter is set to TLS 1.2.	Select this check box to enable peer authentication.

Siebel Application Interface Profile Parameters

The Siebel Application Interface profile contains parameters that control interactions between the Siebel Web Engine and the Siebel Application Interface for all Siebel Business Applications deploying the Siebel Web Client.

The Siebel Application Interface profile includes a Basic Information section for defining Authentication, Logging, and REST Inbound Defaults, an Other Information section for defining SWE, and an Applications section for defining Basic Information, Mobile, and Enhanced Authentication for individual Siebel Business Applications. Each parameter value in the Basic Information section is used by all individual applications, unless you override the parameter's value (for a specific application) with an entry in the Applications section.

You can edit the parameters in the Siebel Application Interface profile using the Siebel Management Console. For information on using the Siebel Management Console to configure application interface profile parameters, see *Siebel Installation Guide* .

In a given Siebel Application Interface profile, some parameters might not appear by default. For more detailed information on application interface profile parameters, see:

- *Authentication Parameters in Siebel Application Interface Profile*
- *About the Active Session Timeout Value Parameter*
- *Application Object Manager Parameters in Siebel Application Interface Profile*
- *SWE Parameters in Siebel Application Interface Profile*
- *REST Inbound Authentication Parameters in Siebel Application Interface Profile*

Note: Before you create and configure a Siebel Application Interface profile, make sure that you have already deployed the Siebel Server. After you have done this, the Object Manager and Application settings in Siebel Application Interface profile configuration are populated with values you can choose from that reflect available components on the Siebel Server. After you deploy a Siebel Application Interface profile, the profile is in a read-write state. You can update the configuration settings and save the profile to propagate the updates to the deployed Siebel Application Interface.

Siebel CRM supports the following security profiles:

- Application Interface profiles, which require a 1:1 mapping to security profiles (Database, LDAP, or Custom).
- For object manager-based UI applications, either Basic or SSO authentication is supported on the defined security profile.
- For object manager-based REST channels, Basic, SSO, or OAuth authentication is supported.
- For non-object manager REST calls, authentication types are not controlled by the Application Interface profile so the Basic authentication type is used with the defined security profile. For example: srvrmgr, Gateway and Siebel Manager Console-specific (non-object manager) REST calls.
- Components that are not part of the Application Interface can override the basic security profile and use a different security profile.

Authentication Parameters in Siebel Application Interface Profile

The following table describes the parameters in the Application Interface profile that relate to authentication. You define these parameters in either the Basic Information section or the Applications section under Application Interface Profiles in the Siebel Management Console.

Note: Passwords (such as, Anonymous User Password and Trust Token) are encrypted by default for the Siebel Application Interface profile. For more information, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*.

Parameter	Section Under Application Interface Profiles	Description
Active Session Timeout Value (seconds)	Basic Information - Authentication	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).

Parameter	Section Under Application Interface Profiles	Description
		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 Active Session Timeout Value parameter, see *About the Active Session Timeout Value Parameter*.
Active Session Timeout Warning Value (seconds)	Basic Information - Authentication	Before a session times out, a session timeout warning message appears prompting users to choose whether or not to extend the session. The time at which the message appears is determined by the value specified by this parameter. The default value for this parameter is 60 seconds. The time at which the session timeout warning message appears is calculated by subtracting the Active Session Timeout Warning Value from the Active Session Timeout Value. For example, if Active Session Timeout Value is set to 900 seconds and Active Session Timeout Warning Value is set to 300 seconds, then the session timeout warning message appears after 600 seconds of inactivity (900 minus 300 equals 600). • If the user selects OK in response to the session timeout warning message, then the session timer is reset to zero and is only activated again after another 600 seconds of inactivity has elapsed. • If the user selects Cancel in response to the session timeout warning message, then the session is terminated once the session timeout period is reached. • If you do not want users to receive a session timeout warning message, then set the Active Session Timeout Warning Value to zero (0).
Login Session (guest session) Timeout Value (seconds)	Basic Information - Authentication	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 Anonymous User Name and Anonymous User Password parameters to log in.
Method to Check Server Availability	Basic Information - Authentication	Provide the swe method name which will be used with the swe command name provided in the [Command to Check Server Availability] field to check the server availability. This must not be empty if the [Command to Check Server Availability] field is not empty.
Command to Check Server Availability	Basic Information - Authentication	Provide the swe command name, which will be sent to check the server availability.

Parameter	Section Under Application Interface Profiles	Description
Session Token Usage Duration (minutes)	Basic Information - Authentication	Provide the session token usage duration, which will make the application interface reject the token if it has been used for more than this value.
Session Token Timeout Value (seconds)	Basic Information - Authentication	Provide the session token time out, which will make the application interface reject the session token if the token is inactive for more than this value.
Configure Web Single Sign-On (Web SSO)	Basic Information - Authentication	The application interface operates in Web SSO mode when this parameter is `TRUE`. For more information, see *Single Sign-On Authentication*
Trust Token	Basic Information - Authentication This option appears when Web SSO is true.	Provide the trust token string, which will be used as the password when Web SSO is enabled. 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. This value must not be empty when Web SSO is enabled. In a Web SSO environment, this token string is a shared secret between the application interface and the security adapter. It is a measure to protect against spoofing attacks. This setting must be the same on both the application interface and the security adapter. For more information, see *Single Sign-On Authentication*
User Specification	Basic Information - Authentication	In a Web SSO implementation, this variable name specifies the name of the HTTP header variable to read the user's user name. Do not prefix with HTTP_.
Anonymous User Name	Basic Information - Authentication	Provide the user name required for anonymous browsing and initial access to the login pages. For example: GUESTCST. The user name selected as the anonymous user must be assigned access to views intended for anonymous browsing, but to no other views.
Anonymous User Password	Basic Information - Authentication	Provide the password for the anonymous user. For more information on setting passwords for the anonymous user, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*.

About the Active Session Timeout Value Parameter

The Active Session Timeout Value parameter is the time, in seconds, from the user's last browser request until the user's connection times out. The following table offers guidelines for setting this parameter.

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.

The types of session timeouts mentioned in the table 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 Active Session Timeout Value set in the Siebel Application Interface profile, 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 Active Session Timeout Value. 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* .

Application Object Manager Parameters in Siebel Application Interface Profile

The following table describes the Application Object Manager parameters in the Application Interface profile that relate to authentication. You define these parameters in the Applications - Basic Information section under Application Interface Profiles in the Siebel Management Console.

Parameter	Section Under Application Interface Profiles	Description
Application Name	Applications - Basic Information	Specify the application name.
Object Manager	Applications - Basic Information	Specify the object manager for the application.
Language	Applications - Basic Information	Specify the language for the application.

Parameter	Section Under Application Interface Profiles	Description
Request Start Command	Applications - Basic Information	Specify the start command for the application.
Configure HTTP Inbound Transport	Applications - Basic Information	Select this option to enable HTTP in-bound transport.
Configure Anonymous Pool	Applications - Basic Information This option appears if you select the Configure HTTP Inbound Transport option.	Select this option to use the anonymous user connection pool.
Anonymous Pool Size	Applications - Basic Information This option appears if you select the Configure HTTP Inbound Transport option and the Configure Anonymous Pool option.	Specify the pool size for anonymous user connections.
Maximum Retry for processing EAI-SOAP request	Applications - Basic Information	Specify the maximum number of retries when processing EAI-SOAP requests.
No Session Preference in EAI-SOAP	Applications - Basic Information	Select this option if no session preference is required in EAI-SOAP.

SWE Parameters in Siebel Application Interface Profile

The following table describes the SWE parameters in the Siebel Application Interface profile that relate to security and authentication. You define these parameters in the Other Information section under Application Interface Profiles in the Siebel Management Console.

Parameter	Section Under Application Interface Profiles	Description
Language	Other Information - SWE	Specify the language of the Siebel application.
HTTP-POST Request Size (byte)	Other Information - SWE	Specify the byte size to control the size of HTTP POST requests from the application interface. This field must not be empty.
Seed File Location	Other Information - SWE	Specify the location of the seed file.
Monitor Sessions	Other Information - SWE	Select this option to gather statistics on all current sessions. Results are reported in the application interface Stats page.
Collect Application-Specific Statistics	Other Information - SWE	Select this option to enable the collection of application-specific statistics.

REST Inbound Authentication Parameters in Siebel Application Interface Profile

The following table describes the REST inbound authentication parameters in the Application Interface profile. You define these parameters in the Authentication - REST Inbound Authentication section under Application Interface Profiles in the Siebel Management Console. For information about other REST parameters that you define in the Application Interface Profile, see *Siebel REST API Guide* .

Parameter	Section Under Application Interface Profiles	Description
Anonymous User Name	Basic Information - Authentication - REST Inbound Authentication	Specify the anonymous user to use for anonymous REST inbound requests. For example: GUESTCST.
Anonymous User Password	Basic Information - Authentication - REST Inbound Authentication	Specify the password for the anonymous user for REST inbound requests.
Authentication Type	Basic Information - Authentication - REST Inbound Authentication	Specify the authentication type that the Siebel Application Interface nodes accept for REST inbound authentication. The options are: • Basic Authentication • Single Sign-On • OAuth
Trust Token	Basic Information - Authentication - REST Inbound Authentication This option appears if you select the Single Sign-On or OAuth (Authentication Type) option.	Specify the trust token, which will be used as the password when Single Sign-On or OAuth is enabled. 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.
Authentication URL	Basic Information - Authentication - REST Inbound Authentication This option appears if you select the OAuth (Authentication Type) option.	Specify the URL to use for REST inbound authentication (OAuth). It is recommended that you specify the URL using the HTTPS format.
User Specification	Basic Information - Authentication - REST Inbound Authentication This option appears if you select the Single Sign-On (Authentication Type) option.	Specify the user specification to user for authentication.
Session Timeout (seconds)	Basic Information - Authentication - REST Inbound Authentication	Specify the time (in seconds) that a connection task will wait for a message from the client, before timing out.
Secure Channel	Basic Information - Authentication - REST Inbound Authentication	This option applies only for the OAuth authentication type as follows:

Parameter	Section Under Application Interface Profiles	Description
		• Select this check box only when you have already imported the Authentication URL's CA certificate into the Application Interface truststore. • Deselect this check box when the Authentication URL's CA certificate is not available in the Application Interface truststore. In this case, the Application Interface trusts all certificates while calling the Authentication URL over HTTPS.

Disabling REST Anonymous Authentication

REST anonymous authentication is used for use cases where Siebel is considered as the back-end engine and it can co-exist along with other API microservices within the same firewall. Use the following procedure to disable anonymous user for inbound REST calls.

To disable anonymous authentication for inbound REST calls

1. Log in to Siebel Management Console.
2. Click Profiles in the navigation menu, click Application Interface, and then navigate to Authentication, then the REST Inbound Authentication section of your selected application interface profile.
3. Enter user credentials, for example, as follows:

Parameter	Example Value
Anonymous User Name	`"authenticated"`
Anonymous User Password	`"authenticated"`

Note: As a result, REST requests without user credentials are unsuccessful (and fail with an HTTP 401 error).

Siebel Application Configuration Parameters

A separate configuration exists for each Siebel application for each language. The parameters for each Siebel application determine how the user interacts with the Application Object Manager and with the security adapter. The application configuration that controls a particular user session depends on the client with which a user connects as follows:

- **Configuration parameters for Siebel Server (Siebel Web Client).** For users connecting with the standard Siebel Web Client, application configuration is 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, not in the application configuration file.

See *Server Parameters for Siebel Gateway* for a description of the parameters applicable to Siebel Web Clients.

- **Configuration parameters for Siebel Tools, Mobile Web Client, or Developer Web Client.** Application configuration is located in the `SIEBEL_CLIENT_ROOT\bin\LANGUAGE` subdirectory on the client. For example, eservice.cfg is provided for Siebel eService and tools.cfg for Siebel Tools, for implementation in U.S. English, in the `SIEBEL_CLIENT_ROOT\bin\ENU` directory.

  Siebel Mobile Web Client connects directly to the local database and bypasses the Siebel Server.

  Siebel Developer Web Client connects directly to the server database and bypasses the Siebel Server.

  The parameters in the following table apply to Siebel Tools, Mobile Web Clients, and Developer Web Clients.

  > **CAUTION:** The parameter values that reference directory attributes that you provide for the Siebel LDAP security adapter are case-sensitive. The values must match the attribute names in the directory.

Parameter	Description
SecAdptMode For more information about setting this parameter, see the Enterprise Security Authentication Profile (Security Adapter Mode) parameter in the table in *Parameters for Configuring Security Adapter Authentication*.	Specifies the security adapter mode. The options are: • For database authentication, specify DB (which is the default value). • For LDAP authentication, specify LDAP. • 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.
SecAdptName For more information about setting this parameter, see the Security Adapter Name (named subsystem) parameter in the table in *Parameters for Configuring Security Adapter Authentication*.	Specifies the name of the security adapter. • For database authentication, specify DBSecAdpt (which is the default value). For Mobile or Developer Web Client configuration, the DBSecAdpt is created in the configuration. • For LDAP authentication, specify LDAPSecAdpt (or a name of your choice). For Developer Web Client configuration, the LDAPSecAdpt is created by default in the configuration if you configure LDAP using the Siebel Management Console. • 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, and is not available in the Siebel Management Console.	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, *Security Adapters and the Siebel Developer Web Client*.

Parameter	Description

Changes to an application configuration are not active until you restart the Siebel Server or Siebel client. For more information about working with configuration information, see *Siebel System Administration Guide* .

Parameters for Database Security Adapter (DBSecAdpt)

You define database authentication parameters for the following named subsystems:

- **InfraSecAdpt_DB.** That is, for the DBSecAdpt named subsystem or a similar security adapter with a nondefault name.
- **InfraDataSource.** That is, for the ServerDataSrc named subsystem or another data source.

The named subsystem is specified as the value for the data source Security Adapter Name parameter for the database security adapter.

The following parameters apply when defining a database security adapter:

- Name
- Type
- Host Name
- Port
- SQL Style of Database
- Database Service Name
- Table Owner
- Enterprise Security Authentication Profile (Security Adapter Mode)
- Security Adapter Name (named subsystem)
- Database Security Adapter Data Source
- Database Security Adapter Propagate Changes

For more information about these parameters, see *Parameters for Configuring Security Adapter Authentication*.

Note: Starting from Java 8, the odbc-jdbc driver is not supported. Because of this limitation, you must specify raw database connection details (like server host, port, database service name, and so on) instead of ODBC details when defining a database security profile.

Parameters for LDAP Security Adapter (LDAPSecAdpt)

You define LDAP authentication parameters for the following named subsystems:

- **InfraSecAdpt_LDAP.** That is, for the LDAPSecAdpt named subsystem or a similar security adapter with a nondefault name.

The named subsystem is specified as the value for the data source Security Adapter Name parameter for the LDAP security adapter.

The following parameters apply when defining an LDAP security adapter:

- Name
- Type
- Host Name
- Port
- Enterprise Security Authentication Profile (Security Adapter Mode)
- Security Adapter Name (named subsystem)
- Application User Distinguished Name (DN)
- Application Password
- Base Distinguished Name (DN)
- ConfigLdapAuthTimeout
- Hash Algorithm
- Hash DB Password
- Hash User Password
- Password Attribute Type
- Propagate Change
- Roles Attribute (optional)
- Shared Databases Account Distinguished Name (fully qualified domain name)
- Shared DB User Name
- Shared DB Password
- Security Adapter Mapped User Name
- Siebel Username Attribute
- SSL
- Enable SSL
- Configure Web Single Sign-On
- Trust Token
- Wallet Password
- Salt Attribute Type
- Salt User Password
- User Name Attribute Type

For more information about these parameters, see *Parameters for Configuring Security Adapter Authentication*.

Parameters for Custom Security Adapter (CustSecAdpt)

You define custom authentication parameters for the following named subsystems:

- **InfraSecAdpt_Custom.** That is, for the CustSecAdpt named subsystem or a similar security adapter with a nondefault name.

The named subsystem is specified as the value for the data source Security Adapter Name parameter for the custom security adapter.

The following parameters apply when defining an Custom security adapter:

- Enterprise Security Authentication Profile (Security Adapter Mode)
- Security Adapter Name (named subsystem)
- Application User Distinguished Name (DN)
- Application Password
- Base Distinguished Name (DN)
- Custom Library
- SQL Style of Database
- CRC Checksum
- Credentials Attribute
- Hash Algorithm
- Hash DB Password
- Hash User Password
- Password Attribute Type
- Propagate Change
- Roles Attribute
- Shared Databases Account Distinguished Name
- Shared DB User Name
- Shared DB Password
- Security Adapter Mapped User Name
- Siebel Username Attribute
- SSL
- Enable SSL
- Configure Web Single Sign-On
- Trust Token
- Wallet Password
- Salt Attribute Type
- Salt User Password
- User Name Attribute Type

For more information about these parameters, see *Parameters for Configuring Security Adapter Authentication*.

12 Predefined Data

Seed Data

This chapter 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*
- *Seed Users*
- *Seed Responsibilities*

In the tables in this chapter, the term *customer applications* represents the group of Siebel Sales, Siebel eService, Siebel Customer, Siebel Events, and Siebel Marketing applications.

Seed Employee

One Employee record, which is described in the following table, is provided as seed data at installation. 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 parameter on the Siebel Gateway. For information about organization access control, see *Access Control Mechanisms*.

Last Name	First Name	User ID	Responsibility	Position	Organization
Employee	Proxy	PROXYE	None	Proxy Employee	Default Organization

Seed Users

This topic includes information about the following:

- *Special Users and Privileges*: Provides information on the defined special users and privileges within Siebel Business Applications.

- *Seed Users Provided as Seed Data*: Provides information on the seed data provided with Siebel Business Applications in general.
- *Seed User Modifications for Siebel Financial Services Applications*: Provides information on the seed data provided with Siebel Financial Services applications.
- *About Seed Position and Organization Division Records*

Special Users and Privileges

Within Siebel Business Applications, special users are defined with specific roles within the application. Data to support these special user accounts is included in the seed data installed with Siebel Business Applications. You can change special user account names after installation, or delete the relevant seed data for a special user account if you do not need the functionality it provides. Do not, however, disable the Siebel administrator (SADMIN) or guest user accounts.

The following special users and privileges are defined:

- **Anonymous users.** You can define an anonymous user (or guest) account to allow access to your Siebel application by unregistered, unauthenticated users. You must also define an anonymous user if your Siebel application implements LDAP authentication.

  Three Siebel application user accounts, GUESTCST, GUESTCP, and GUESTERM are provided as seed data for use as anonymous user accounts; however, you can create a different user account for this purpose. Review the user responsibilities assigned to the anonymous user record and limit them to those necessary for sign-on and guest access.

  Anonymous browsing is enabled by default. If your Siebel application does not use functionality that requires anonymous browsing, then set the AllowAnonUsers parameter to False. For further information, see *Parameters for Application Object Manager Components*.
- **Administrator users.** A Siebel administrator database account (default user ID is SADMIN) and a Siebel application user account, SADMIN, are created during the Siebel Business Applications installation process for the administrative user. Follow these guidelines in relation to the administrator user:
  - Limit usage of the administrator role.

    Review users with administrative responsibilities. In Siebel Business Applications, the SADMIN responsibility has broad administrative privileges. For this reason, regularly review the list of users with this responsibility. Define and assign appropriate responsibilities for users that clearly reflect their line of duty.
  - Delete or disable unused administrator user IDs.
- **Directory application user.** The Directory Application User is a special user defined to handle access to the LDAP directory if this authentication mechanism is used. By setting up an application user as the only user with search, read, and update privileges to the directory, you minimize the level of access of all other users to the directory.

  The directory application user must not have a corresponding database account and must not be defined as a Siebel application user or have a Siebel application user record.
- **Shared database account user.** If you are using LDAP or Web SSO authentication, then you can configure a shared database account in the directory; this is a directory entry that contains a database account that is shared by many users. A database login is created for all Siebel users who are authenticated externally during the installation process; the default database login is LDAPUSER. You must also specify a valid Siebel user ID and password for the shared database account in the directory.

- An employee record, Proxy Employee, is provided as seed data during installation. This record provides customers (contact users) who log in to a Siebel customer application with a user ID (PROXYE), a position (Proxy Employee), and an organization (Default Organization).

  Because the PROXYE user ID gives view access to data that is associated with the related organization, review the visibility to data provided by the proxy employee user ID and, if necessary, change the organization with which the Proxy Employee user record is associated. You cannot change seed data, therefore, to modify the Proxy Employee record you must make a copy of the record, rename it, and amend the copy. For additional information, see *Siebel User Accounts*.

Seed Users Provided as Seed Data

The following table 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 Anonymous User Name parameter to the seed user ID (for example GUESTCST) when configuring the Application Interface, or set it manually in the Application Interface profile. For information on configuring the Application Interface, see *Siebel Installation Guide* . For information on manually setting passwords for the anonymous user, see *Encrypted Passwords in Siebel Application Interface Profile Configuration*.

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 User Modifications for Siebel Financial Services Applications

The following table shows modifications to the seed nonemployee User records that are provided with Siebel Financial Services applications.

The GUESTCP seed User record, which is documented in *Seed Users Provided as 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.

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

About Seed Position and Organization Division Records

The Proxy Employee Position and the Default Organization Division records are provided as seed data. The position exists within the division, and the division is its own organization. The position and division are both assigned to the seed data Employee record.

Seed Responsibilities

Different responsibility records, as described in the following table, are provided as seed data. 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.

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
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

Name	Organization	Description	Used by These Applications
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
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

Seed Responsibilities for Siebel Financial Services Applications

The following table describes 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 *Configuring Access Control*.

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.

Name	Organization	Description and Comments	Used by These Applications
			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.

Listing Views Associated with Responsibilities

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.

13 Siebel Security Hardening

Siebel Security Hardening

This chapter covers Siebel Security Hardening implementation and administration. It includes the following topics:

- *About This Chapter*
- *Overview of Security Threats, Recommendations, and Standards*
- *Securing the Network and Infrastructure*
- *Securing the Operating Systems*
- *Securing the Siebel Database*
- *Securing Siebel CRM*
- *Implementing Auditing*
- *Performing Security Testing*
- *Supported Security Standards*
- *Default Port Allocations*

About This Chapter

This chapter provides the information you need to protect your Siebel CRM deployment:

- It describes the Siebel security architecture and security concepts.
- It outlines the security controls provided by Siebel CRM.
- It provides detailed procedural information on how to implement security controls to secure your application.

This chapter provides recommendations for safeguarding your Siebel CRM 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 data, you must secure both your Siebel Business Applications and the computing environment in which they run.

This chapter describes how to harden your Siebel CRM deployment. *Hardening* is the process of protecting your computer network and applications from internal and external security threats by minimizing the areas of security vulnerability. Examples of hardening tasks include removing unnecessary software, services and utilities, disabling unused user accounts or login IDs, and setting up intrusion-detection systems. This chapter provides detailed procedural information on implementing Siebel security controls only where such information is not provided elsewhere on the *Siebel Bookshelf* .

This chapter applies to Siebel CRM version 8.1 and 8.2 and is intended for Siebel administrators, security groups, and IT staff involved in securing environments for Siebel CRM. It is assumed that users are familiar with Siebel Business Applications, their architecture, and with the general security principles within an IT environment.

Note: This chapter contains recommendations for securing the infrastructure in which Siebel CRM operates. You are responsible for ensuring all the security procedures recommended by your operating system and database vendors have been completed to provide a secure environment for Siebel CRM.

Overview of Security Threats, Recommendations, and Standards

This topic provides introductory information about securing Siebel CRM and the infrastructure and environment in which Siebel CRM operates. It includes the following topics:

- *Security Threats and Vulnerabilities*
- *General Security Recommendations*
- *Security Standards and Programs*
- *About the Oracle Software Security Assurance Program*
- *About Using Transport Layer Security with Siebel CRM*

Security Threats and Vulnerabilities

To secure your Siebel CRM environment, you must understand the security threats that exist and the typical approaches used by attackers. This understanding helps you to identify the correct countermeasures that you must adopt. The common security threats include:

- Computer viruses (malware)
- Code injection
- SQL injection
- Cross-site scripting (XSS)
- Denial of service attacks (DoS)

The following practices can make your applications vulnerable to malicious attacks:

- Using weak passwords
- Moving data between applications, computers, and sites
- Allowing information leaks
- Allowing nonsecure coding practices when configuring Siebel CRM

Monitor security sites for information on newly discovered vulnerabilities affecting third-party components or applications that are integrated with Siebel CRM software. Some of the well-known Web sites that contain information on security incidents with vulnerabilities and patches are as follows:

- *www.cert.org*
- *www.sans.org*
- *www.insecure.org*
- *www.cisecurity.org*
- *https://seclists.org/bugtraq/* (hosts the Bugtraq mailing list)

Perform security risk assessments regularly to identify possible security vulnerabilities in your environment, then address any issues. For information on this task, see *Performing Security Testing*. For general information on preventing security attacks and vulnerabilities in your environment, see *General Security Recommendations*.

General Security Recommendations

Align the policies you create to secure your Siebel CRM environment with the overall security policies and principles adopted by your organization. Some of the general policies recommended to help protect your Siebel CRM deployment and infrastructure include the following:

- Restricting network access
- Following the principle of least privilege when setting up access controls
- Monitoring activity by enabling a minimum level of logging (auditing and reviewing)
- Keeping up-to-date with the latest security information
- Configuring accounts securely, including securing session management
- Setting security parameters
- Running security-maintenance reports regularly
- Enforcing secure coding practices, for example, data validation, when creating custom code and scripts
- Encrypting Web and network communications and sensitive data in the Siebel database, for example, credit card numbers and passwords
- Installing approved enterprise-wide antivirus software to protect servers and workstations, and updating virus pattern files on a periodic and emergency basis as recommended by the vendor

Patch Management

Implement a patch management process to make sure that all the software in your environment is updated with the latest software versions and security patches. You must make sure all updates and patches for Siebel CRM are applied. Also make sure that all updates are applied for the other software that is required to run Siebel CRM, but that is not shipped by Oracle. Some examples include your operating system software and browser software.

Critical Patch Updates for Siebel Business Applications

Oracle uses critical patch updates to release security patches for all its applications, including Siebel Business Applications. Critical patch updates are issued each quarter and consist of multiple security fixes in one patch.

For a list of the latest critical patch updates and security alerts for Siebel CRM available from Oracle, and for information on security vulnerabilities fixed in a critical patch update, go to the Oracle Critical Patch Updates and Security Alerts Web site at

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Oracle provides information about product security vulnerabilities only as part of the critical patch update or Security Alert notification process.

CSV Export Functionality

If you consider macro injection a risk (see *https://www.owasp.org/index.php/CSV_Injection*), then disable CSV export in all list applets and where CSV export is available.

MIME Sniffing

Multipurpose Internet Mail Extension (MIME) sniffing, the process of inspecting byte stream content to try to determine the file format of the data within it, is disabled by default in Siebel.

Since it is essential for the browser to render customer files according to the Content-Type, customers are typically requested to convert their customer file content to match the Content-Type. You can enable MIME sniffing by commenting out the `HttpHeaderSecurityFilter` filter and its filter mapping from the web.xml file stored here:

```
$<Tomcat Container Location>\conf\web.xml
```

It is recommended that you do not enable MIME sniffing in production environments.

Security Standards and Programs

Siebel CRM adheres to a range of common industry standards relating to security so that customers can choose a security infrastructure that best suits their specific business needs. For a list of the technical standards supported with Siebel CRM, see *Industry Standards for Security*.

Siebel CRM also supports the following standards:

- Payment Card Industry Data Security Standard (PCI DSS)
- Common Criteria for Information Technology Security Evaluation (Common Criteria) standard
- Federal Information Processing Standard (FIPS) 140

For information about Siebel CRM support for the PCI DSS, Common Criteria, and FIPS standards, see *Supported Security Standards*.

Note: Siebel CRM does not provide a client that supports the Security Assertion Markup Language (SAML) standard.

About the Oracle Software Security Assurance Program

Siebel CRM is developed and maintained in accordance with the Oracle Software Security Assurance program, which incorporates security best practices in the following areas:

- Secure development process
- Critical patch updates
- External security validations
- Security information and best practices

For further information on the Oracle Software Security Assurance program, go to *http://www.oracle.com/us/support/assurance/index.html* .

About Using Transport Layer Security with Siebel CRM

It is strongly recommended that you implement Transport Layer Security (TLS) encryption for all of the following services and communication paths in a Siebel CRM implementation:

Note: The use of Secure Sockets Layer (SSL) v3.0 encryption for environments with security requirements is not supported by Oracle for Siebel CRM as a result of security vulnerabilities discovered in the design of SSL v3.0.

- For communications between Siebel Web server and Siebel Web Client.
- For communications between Siebel Server and the Web server.
- For encryption of communications between Siebel Enterprise components, for example, communications between the Siebel Server to Siebel Web server (Application Interface), or between Siebel Servers.
- For communications between an LDAP security adapter and a directory server.
- For communications using the Siebel CRM external interfaces (EAI), which use Web services to send and receive messages over HTTP.
- For communications between Siebel Server and an email server, including encryption for SMTP, IMAP, and POP3 sessions between Siebel Server and an email server.

For more information, see *Securing the Network and Infrastructure* which includes information about the following:

- *Enabling Encryption Between the Web Client Browser and Web Server*
- *Enabling Encryption Between the Web Server and Siebel Server*
- *Enabling Encryption for Security Adapters*
- *About Using TLS with Siebel Enterprise Application Integration (EAI)*
- *Securing the Siebel Web Server*
- *Securing the Siebel Server*
- *Securing the Siebel Client*
- *Securing Email Communications*

For additional information, see the following chapters:

- *Communications and Data Encryption*
- *Security Adapter Authentication*
- *Siebel Application Interface Security Features*

Note: To ensure that you are using the highest level of security, download and install the current Siebel CRM Update release to enable the highest level of security and obtain the latest security-related patches. For more information about installing the current Siebel CRM Update release and about Siebel release types, see Siebel Installation Guide for the operating system you are using. For more information about installing Siebel Patchset releases, including new features, see *Siebel CRM Update Guide and Release Notes* on My Oracle Support, 23824315.1 (Article ID), for each applicable release.

Securing the Network and Infrastructure

This topic describes how to secure your network infrastructure and outlines the minimum network configurations. It includes the following topics:

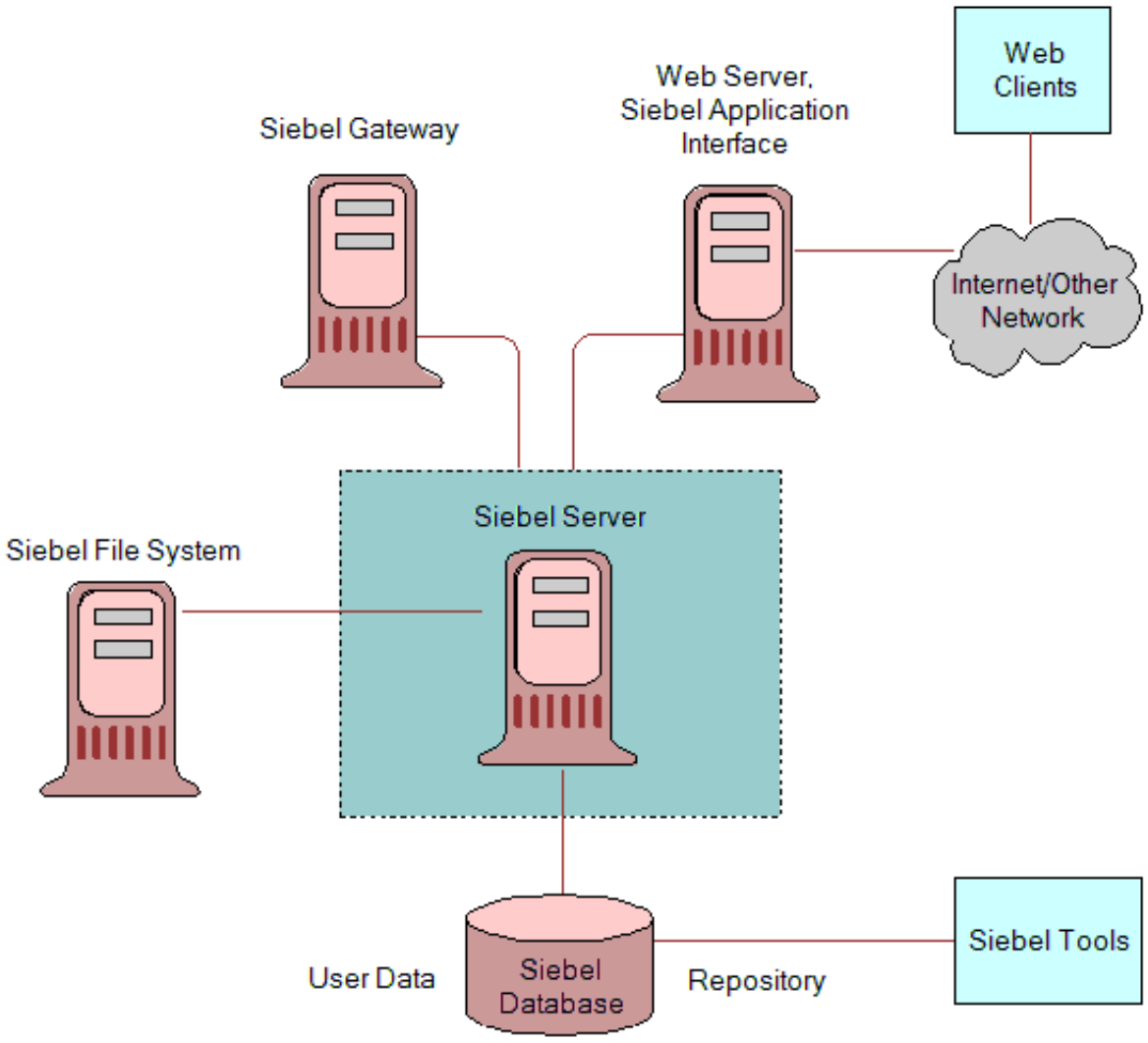
- *About Securing the Network Infrastructure*
- *Recommended Network Topology*
- *Removal of Siebel Application Interface Dependency on Oracle Database Client*
- *Network Authentication and Monitoring*
- *Enabling Encryption of Network Traffic*
- *Securing the Siebel Web Server*
- *Securing the Siebel Server*
- *Securing the Siebel Client*
- *Securing Mobile Clients*
- *Securing Siebel Remote*
- *Securing Mobile Devices Running Siebel CRM*
- *Securing the Siebel Document Server*
- *Securing Email Communications*
- *Securing the Siebel Reports Environment*

About Securing the Network Infrastructure

Where and how network computing resources reside, as well as how they work in connection with the Internet and other computers on the local network, can have a significant impact on network security. This topic describes the network components to consider in securing your Siebel CRM deployment. You must consider the physical layout of the network components and the network authentication measures required.

The following figure shows the basic components included in Oracle's Siebel CRM network:

- The components include: Siebel Server, Siebel File System, Siebel Database (storing user data and repository information), Siebel Gateway, Siebel Application Interface, Web server, Internet, Web Clients
- Access to the devices that host Siebel CRM 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, for example, by enforcing computer passwords, can be used and are transparent to Siebel CRM.
- Siebel CRM supports and encourages the deployment of firewalls throughout the enterprise as well as reverse proxy servers, Network Address Translation devices, and load balancers to secure the application from attack.
- The architecture of Siebel CRM also takes advantage of high-availability technologies, such as Microsoft Cluster Services, which spread the workload across multiple computers allowing them to function as one. High-availability technologies address the need for failover and disaster-recovery management.



The following topics provide recommendations for deploying network components in securing your Siebel CRM infrastructure:

- *Network Zones and Firewalls*
- *Guidelines for Assigning Ports on Firewalls*
- *Guidelines for Deploying Siebel CRM Across a Firewall*
- *Routers*
- *Network Address Translation*
- *Load Balancers*
- *Proxy Servers*
- *Forward Proxy Servers*
- *Reverse Proxy Servers*
- *Procedure to Configure Reverse Proxy*

- *Virtual Private Networks*
- *About Using Internet Protocol Security*
- *Preventing Denial of Service Attacks*

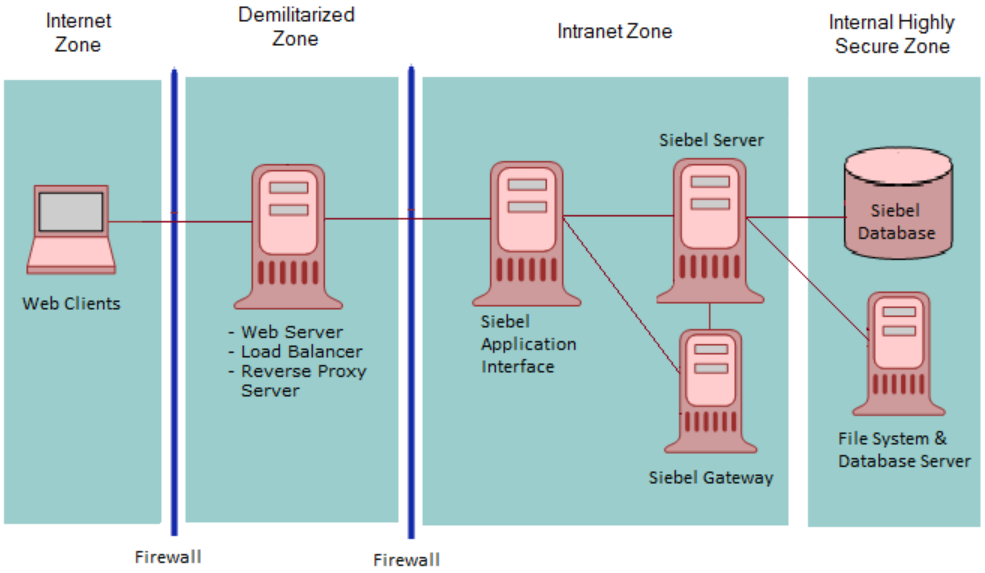
Note: Siebel CRM does not use Simple Network Management Protocol (SNMP) for managing network devices. You can disable Simple Network Management Protocol services on Siebel Servers, if required.

Network Zones and Firewalls

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

To secure a network, divide the network into zones of control by considering factors, such as the type of information contained in the zone and who needs access to that zone. Then place firewalls between the zones and implement access controls between the zones.

The following figure shows the recommended placement of firewalls in a Siebel CRM environment, which is between the Internet and demilitarized zones, and between the demilitarized and intranet zones. For optimum performance, do not install a firewall between the intranet zone and the internal highly secure zone.



As illustrated in this figure, an enterprise network for Siebel CRM typically comprises the following zones of control:

- **Internet zone.** This zone is insecure and not trusted. External Siebel Web Clients reside in this zone.
- **Demilitarized zone.** Publicly accessible servers are placed in this zone. Servers placed in this zone are called *bastion hosts*. Web server load balancers and Reverse Proxy Server reside in this zone. Clients outside the firewall access the Reverse Proxy Web server through a secure connection. This zone is where the external network first interacts with the Siebel environment.
- **Intranet zone.** This zone consists of internal networks. Components that reside inside this zone include the Application Interface, Siebel Servers, Siebel Gateway, and authentication server (Lightweight Directory Access Protocol directory server). In a deployment of Siebel employee applications, Web clients reside beyond the DMZ, somewhere between the DMZ and the unsecured Internet depending on customer security requirements.

Depending on the requirements and configured security adapter, the authentication mode can be one of the following: SSO/SAML, Database, LDAP, or Custom.

> **Note:** The Application Interface accesses the migration database when it is deployed for migration.

- **Internal highly secure zone.** Business critical information and services are placed in this zone. The Siebel Database and File System reside in this zone. Restrict access to this zone to system administrators and database administrators.

For additional information on the recommended placement of firewalls, see *Recommended Network Topology*. For information on assigning ports when setting up firewalls, see *Guidelines for Assigning Ports on Firewalls*.

Guidelines for Assigning Ports on Firewalls

This topic provides guidelines for assigning ports when setting up firewalls for your Siebel CRM implementation.

Configure communication ports as follows:

1. Set up the external firewall to enable HTTPS (default port 443) communications between external Siebel Web Clients in the Internet zone and the IP address of the Load Balancer/Reverse Proxy in the demilitarized zone according to the security parameters set on the Application Interface.

   Open the reverse proxy port configured on the reverse.
2. Set up the choke firewall (the firewall between the demilitarized zone and the intranet) as follows:
   - For communications from the Load Balancer/Reverse Proxy to the Application Interface, enable the Application Interface HTTP/HTTPS port (the default ports are 80/443)
   - For communications from the Application Interface to the Siebel Server, use the SCBroker port (Siebel load balancing) for Transmission Control Protocol (TCP) traffic. The default port used by SCBroker is 2321.
   - For communications from the Application Interface to the gateway, use the gateway port (the default port 2320).
   - For communications from the Application Interface to the database, use the database port.

   > **Note:** For inbound connections into the Siebel environment (such as, Siebel Web Client to Application Object Manager connections, inbound Web Services requests, inbound HTTP rRequests, inbound RESTFul API requests), use the Siebel Application Interface HTTPS port 8011. For outbound connections (such as, Siebel application server to application container connections, Siebel outbound REST requests, outbound EAI HTTP/HTTPS requests, outbound Web Services requests, outbound Java/JMS integrations) , use Siebel Server HTTP port 8002.
3. Oracle recommends placing an internal firewall between the intranet zone and the internal highly secure zone, then setting up the internal firewall as follows:
   - Enable port 636 for the secure transmission of authentication information between the security adapter and the Siebel Servers. (The default port is 389.)
   - For communications between the Siebel Server and the Siebel database, enable the following default ports:
     - Microsoft SQL: TCP ports 1433, 139 and UDP ports 137, 138 (ports 137–139 are for communications between the Siebel Server and the Siebel File System).
     - 1521 (Oracle)
     - 50000 (DB2)

Note: Even though Siebel Server and the Cloud Gateway are usually in the same network security zone, the gateway port must be open (the default port is 2320).

For more information on port allocations used by Siebel CRM, see *Default Port Allocations*.

Guidelines for Deploying Siebel Business Applications Across a Firewall

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

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

- Web server compression for the Application Interface must be disabled. So in the Application Interface profile, disable the HTTP 1.1-Compliant Firewall/Enable Web Compression parameter. (Use other settings where compression is known to be supported, or might be supported.) For more information, see *Siebel Installation Guide* .
- Make sure that the firewall can handle cookie-wrapping or other proxy-specific features that enable forwarding of a cookie. Or, reduce or remove the use of cookies in your Siebel Business Applications. For more information, see *About Using Cookies with Siebel Business Applications*.
- Make sure that your proxy server does not pass to the Application Interface any header content that uses HTTP 1.1 protocol. The proxy must remove any header content that is not compliant with HTTP 1.0.

Routers

Set up a screening router that selectively blocks or allows packets destined for internal resources. The screening router is typically a gateway to the external world, which is located at the perimeter, and is set up with the appropriate access list.

Network Address Translation

Network Address Translation rewrites the IP addresses of Internet connections as they cross the firewall boundary, thereby preventing direct access between the internal network and external networks, such as the Internet and partner networks.

Implement Network Address Translation on zone border security devices between the Web client and the Web server, and between the Web server and the Siebel Server.

Load Balancers

Siebel Servers are dynamically load balanced using native Siebel load balancing. In addition, third-party HTTP load balancers supporting jsession-based load balancing can be applied in front of the Siebel reverse proxy Web server to balance Web server load. Using HTTP load balancing distributes incoming network traffic over several servers.

A third-party load balancer typically can provide additional security features, such as limiting TCP port exposure to a single port for multiple Siebel Servers. Single-port exposure allows you to consolidate network access for better port monitoring and security. It also provides simplified firewall configuration. You have to configure only one virtual port.

Additional security features provided by most third-party load balancers include:

- **Denial of service (DoS) attack prevention.** In a DoS attack, a third-party HTTP load balancer helps handle the TCP connections. Incoming attacks can be caught at the load balancer before they reach the Siebel Server. A third-party HTTP load balancer typically has a built-in mechanism to stop DoS attacks at the point of entry.

- **Virtual Internet Protocol (VIP) addressing.** A third-party HTTP load balancer uses VIP addressing. Unlike an IP address, a VIP address is not associated with a specific device in a network, so VIP addressing helps prevent hackers from accessing Siebel Servers directly. Web servers in the demilitarized zone communicate with the VIP only.
- **TCP handshake protection.** The TCP handshake is replayed from the third-party HTTP load balancer to the Siebel Server rather than directly from the Web server in the demilitarized zone to the Siebel Server. This helps prevent attacks in which the TCP handshake is intercepted and redirected, for example, a SYN flood DoS attack.

When installing Siebel CRM, if you are using Siebel Server or third-party HTTP load balancers, then plan the use of TCP ports for firewall access:

- If Siebel load balancing is used, then make sure the Web server can access the SCBroker port on each Siebel server.
- If a third-party load balancer is used, then make sure the Web server can communicate with the VIP addresses and ports specified in the load balancer.
- Load balancer `JSESSIONID` persistence is required for UI applications when the load balancer in front of the application interface. The same can be used for Siebel Migration Application and test automation. Load balancer persistence is not required for REST.

For information on the default port allocations used by Siebel CRM, see *Default Port Allocations*.

Proxy Servers

Siebel CRM supports the use of both forward and reverse proxy servers within a deployment. Using proxy servers enhances security by preventing direct access to servers from the Internet.

Forward Proxy Servers

Forward proxy servers are generally used to provide Web access to the Internet for client computers when direct routing is not possible, either because it is forbidden by policy or by the network implementation. Forward proxy servers are therefore part of the client security infrastructure. They are also sometimes used by Internet service providers for caching.

Reverse Proxy Servers

A reverse proxy server acts as an intermediary to prevent direct connections from clients to Web servers. A reverse proxy server shields internal IP addresses from users by rewriting the IP addresses of the Web servers so that the Web server IP addresses are not revealed to the user. Additionally, the reverse proxy server can cache data closer to end users, thereby improving performance. Reverse proxy servers provide an additional layer of security by helping protect the Web server from direct external attacks, but do not directly help secure the Web application.

A reverse proxy server is always required in the DMZ for all implementations with and without SSO. To handle traffic between the external Siebel Web clients and the Web server/authentication plug-in, always install a reverse proxy server in the demilitarized zone (see the image in *Network Zones and Firewalls*). All application interfaces and other Siebel enterprise components are secured in the secure intranet zone.

If you deploy applications that use Siebel Open UI with a reverse proxy server or a Web server load balancer, then note the following considerations:

- Siebel CRM supports rewriting the host name and IP addresses of the Web servers.

  For example, you can rewrite the following URL: `http://ServerInternal/siebel/app/callcenter/enu`

  To the following: `http://ServerExternal/siebel/app/callcenter/enu`

- The reverse proxy server and the application interface may not run on the same port. Port and protocol switching is supported between reverse proxy and the application interface, and requires that you configure URL rewrite. URL rewrite is at the reverse proxy level and is vendor specific.
- As of Siebel CRM 20.5 Update, configuring reverse proxy is a mandatory post installation task - see *Procedure to Configure Reverse Proxy*.
- Protocol switching from HTTPS to HTTP is supported if you have enabled the TLS acceleration feature for communications between Siebel Web clients and the Siebel Application Interface.

  Note: If the TLS acceleration feature is enabled, then you can deploy TLS between Siebel Web Clients and the reverse proxy server. However, you do not have to deploy TLS between the reverse proxy server and the application interface. You can use the HTTP protocol for communications between the reverse proxy server and the application interface.

Note: For Siebel, a reverse proxy server is required in the DMZ to expose the Siebel app on the Internet or intranet. Setting up reverse proxy is usually documented as part of the Web server choice a customer makes for the platform and Web server product being used. Reverse proxies are typically lightweight and have minimal impact on the overall performance of a deployment. To determine the exact impact of using a reverse proxy, it is recommended that you contact the vendor of your chosen reverse proxy solution.

About Load Balancer Persistence if Using Reverse Proxy

The following are recommendations about (enabling) load balancer persistence when using a reverse proxy:

- **Load balancer in front of Siebel Application Interface.** Load balancer persistence is required for UI applications when the load balancer in front of the application interface. You can use the same configuration for the Siebel Migration Application and test automation. Load balancer persistence is not required for REST.
- **Load balancer in front of the reverse proxy (with or without SSO).** Load balancer persistence is optional when the load balancer is in front of the reverse proxy. There is no functional requirement mandating load balancer persistence at this level. Siebel functionality is independent of load balancer persistence.

Procedure to Configure Reverse Proxy

The following procedure shows how to configure reverse proxy, required for all implementations with and without SSO, to avoid exposing internal IP addresses for sensitive servers. As of Siebel CRM 20.5 Update, this is a mandatory post installation task.

To configure reverse proxy

1. Add proxy settings in the HTTP/HTTPS `<Connector>` element of the application interface's server.xml file. Add the proxy settings to the HTTP connector if the SSL acceleration feature is enabled, otherwise add the proxy settings to the HTTPS connector as follows:
   - When SSL acceleration is enabled:

     ```
     <Connector port="9001" ...
      proxyName="<reverseproxyhost>"
      proxyPort="<port used in loadbalancer/reverse proxy>"
     />
     ```

   - When application interface is in HTTPS, edit the server.xml file to include separate connectors for internal and external users (who are on the same application interface) as follows:

     ```
     // Port 9999 is for external users via reverse proxy:
     ```

```
<Connector port="9999"
 proxyName="<reverseproxyhostname.com>"
 proxyPort="<port used in loadbalancer/reverse proxy(eg. 443)>"
 protocol="org.apache.coyote.http11.Http11NioProtocol"
 maxThreads="600"
 SSLEnabled="true"
 scheme="https"
 secure="true"
 SSLVerifyClient="require"
 SSLEngine="on"
 SSLVerifyDepth="2"
 keystoreFile="..\Siebel\ai\applicationcontainer_external\siebelcerts\siebelkeystore.jks"
 keystorePass="******1"
 keystoreType="JKS"
 truststoreFile="..\Siebel\ai\applicationcontainer_external\siebelcerts\siebeltruststore.jks"
 truststorePass="*******1"
 truststoreType="JKS"
 ciphers="..."
 clientAuth="false"
 sslProtocol="TLSv1.2"
 relaxedQueryChars="..."
 relaxedPathChars=";"
/>

// Port 8443 is for internal users:

<Connector port="8443"
 protocol="org.apache.coyote.http11.Http11NioProtocol"
 maxThreads="600"
 SSLEnabled="true"
 scheme="https"
 secure="true"
 SSLVerifyClient="require"
 SSLEngine="on"
 SSLVerifyDepth="2"
 keystoreFile="..\Siebel\ai\applicationcontainer_external\siebelcerts\siebelkeystore.jks"
 keystorePass="******1"
 keystoreType="JKS"
 truststoreFile="..\Siebel\ai\applicationcontainer_external\siebelcerts\siebeltruststore.jks"
 truststorePass="*******1"
 truststoreType="JKS"
 ciphers="..."
 clientAuth="false"
 sslProtocol="TLSv1.2"
 relaxedQueryChars="..."
 relaxedPathChars=";"
/>
```

2. Restart the application interface for the changes to take effect.

Configuring CORS Support When Interacting with Other Applications

CORS requirements are enforced by most modern browsers. CORS typically requires that the following conditions are met:

- Same host (or alternatives provided below)
- Same port
- Same protocol (end to end)

Supporting CORS can be largely handled at a reverse proxy level for Siebel. Assuming the reverse proxy in front of Siebel is Apache HTTPd server, the proxied application can hide part of the host/domain to make domains of interacting application look the same. Relaxing the CORS requirement is configured in the HTTPd.conf file for the reverse proxy.

This setting in the reverse proxy can also adjust port differences in a similar way. The setting below is a generic way to resolve this however there are more specific ways of solving it as required.

```
Header set Access-Control-Allow-Origin
```

You can find more information in specific reverse proxy documentation implemented (Siebel CRM requires a reverse proxy in front of Siebel).

HTTPS traffic is expected to match for Siebel and any other application it works with as mixed content is not supportable. This is by default, set to secure HTTP (HTTTPS)

This configuration allows Siebel UI to be embedded in any other Origin and is the recommended approach to address CORS requirements. This setting is very useful for action links in Siebel.

For releases before Siebel CRM 20.10, follow the procedure mentioned in *Planning Cross-Domain Integrations*

From Siebel CRM release 20.10 onwards, details available in *Planning Cross-Domain Integrations* are overridden by OOB Tomcat configuration. You need to apply the related configurations in applicationcontainer_external\conf\web.xml.

Attribute	Default Value	Description
`antiClickJackingEnable`	True	Should the anti-click-jacking header (`X-Frame-Options`) be set on the response. Any anti click-jacking header already present will be replaced.
`antiClickJackingOption`	SAMEORIGI	You can set it to one of the following values. • **SAMEORIGIN**. Display the page only in a frame that resides in the same location as the page.This is the default value. • **ALLOW-FROM**. Specify the url for antiClickJackingUri when ALLOW-FROM is set. • **DENY**. Do not display the page in a frame or in an iFrame.
`antiClickJackingUri`	This attribute doesn't exist OOB	This is required if ALLOW-FROM is used for antiClickJackingOption.Display the page only in a frame that resides in the specified location. If an external application accesses a Siebel URI, then you specify the URI that this external application uses. For example, if the external application uses https://my_url.com, then you use the following value: https://my_url.com/ If a browser (such as Chrome or Safari) does not support ALLOW-FROM, then the browser ignores it.

Hardening Procedures Through Reverse Proxy

Reverse proxies can handle Referrer-Policy and Permissions-Policy related header values. Any headers can be configured in the reverse proxy. Content Security Policy (CSP) and Cross-Origin Resource Sharing (CORS) related obstacles are also generally handled as part of reverse proxy configuration.

Adding Custom HTTP Headers to Responses from Siebel

This topic explains how to configure Siebel (v26.5 and later) to add or modify custom HTTP response headers by updating the `GenericHeadersFilter` in the Siebel `web.xml`.

Steps to Add Custom HTTP Headers in the Siebel HTTP Responses

With Siebel version 26.5 and above, the Siebel application allows you to add additional custom headers to the http responses that the Siebel application returns. Below are the steps to make the configuration to add your custom headers in the response.

1. Take a backup of and then open the siebel web.xml file from the location: `applicaton_container_external/webapps/siebel/WEB-INF/web.xml`
2. With version 26.5 and above, you will see a new filter named `GenericHeadersFilter` in web.xml as shown below.

   > **Note:** We have commented out the Content-Security-Policy out of the box but you can uncomment and edit this as you need.

```
<filter>
 <filter-name>GenericHeadersFilter</filter-name>
 <filter-class>com.siebel.swsm.siebelendpoints.GenericHeadersFilter</filter-class>

 <init-param>
 <param-name>Referrer-Policy</param-name>
 <param-value>strict-origin-when-cross-origin</param-value>
 </init-param>

 <init-param>
 <param-name>X-Permitted-Cross-Domain-Policies</param-name>
 <param-value>none</param-value>
 </init-param>

 <!--init-param>
 <param-name>Content-Security-Policy</param-name>
 <param-value>script-src 'self' https://elocation.oracle.com 'unsafe-eval' 'unsafe-inline'; style-src
 'self' 'unsafe-inline'; connect-src 'self';</param-value>
 </init-param-->
</filter>
```

3. To add any new custom header please add the below xml snippet with appropriate header name and value to the `GenericHeadersFilter` section described above.

```
<init-param>
 <param-name>RESPONSE_HEADER_NAME</param-name>
 <param-value>RESPONSE_HEADER_VALUE</param-value>
</init-param>
```

   Example:

```
<init-param>
 <param-name>Cross-Origin-Resource-Policy</param-name>
 <param-value>same-origin</param-value>
 </init-param>
```

   > **Note:** Before changing or adding any header parameter (especially security headers), you must remember that doing so can modify the behavior of your existing application in different ways, such as blocking any script or resource that is accessed with cross domain or application behavior in a cluster setup. Please ensure thorough testing of your application before making the changes live.

Virtual Private Networks

Siebel CRM supports the use of Virtual Private Networks (VPNs). A VPN is a technique that allows computers outside the firewall to tunnel traffic through a firewall and to appear as if they are connected inside the firewall.

VPN technology allows employees working remotely to access many corporate intranet resources (for example, email servers, file shares, and so on) which are otherwise not sufficiently secure to be placed outside the firewall.

About Using Internet Protocol Security

Internet Protocol Security (IPsec) is a mechanism for securing communications at the Internet Protocol (IP) layer. If IPsec is implemented, then IP packets (including the TCP information) are encrypted. You do not have to configure Siebel CRM to enable IPsec in your deployment.

IPsec encrypts TCP data; that is, data at layers 4 to 7 of the OSI model. If you want to implement load balancing, then be aware that Web server load balancers cannot balance loads for encrypted information from layers 4 to 7. Before implementing IPsec, therefore, check with the server load-balancing vendor for support details.

If you implement IPsec, then follow these recommendations:

- Enable port 500 (User Datagram Protocol) and the IP protocols 50 and 51 on the perimeter firewall for IPsec communications.
- It is recommended that you enable pass-through authentication on the VPN Gateway to support Network Address Translation on the client side. (The VPN Gateway can be the firewall with VPN functionality or a separate VPN server behind the firewall).

Preventing Denial of Service Attacks

Denial of service (DoS) attacks can take different forms. However, the most common method involves one or more computers (often hijacked personal computers) bombarding a Web site or Web-accessible service with a large number of simultaneous requests. The affected servers are overwhelmed and the connections and processes are prevented from running. These types of attacks are almost always targeted against public-facing Web sites and applications.

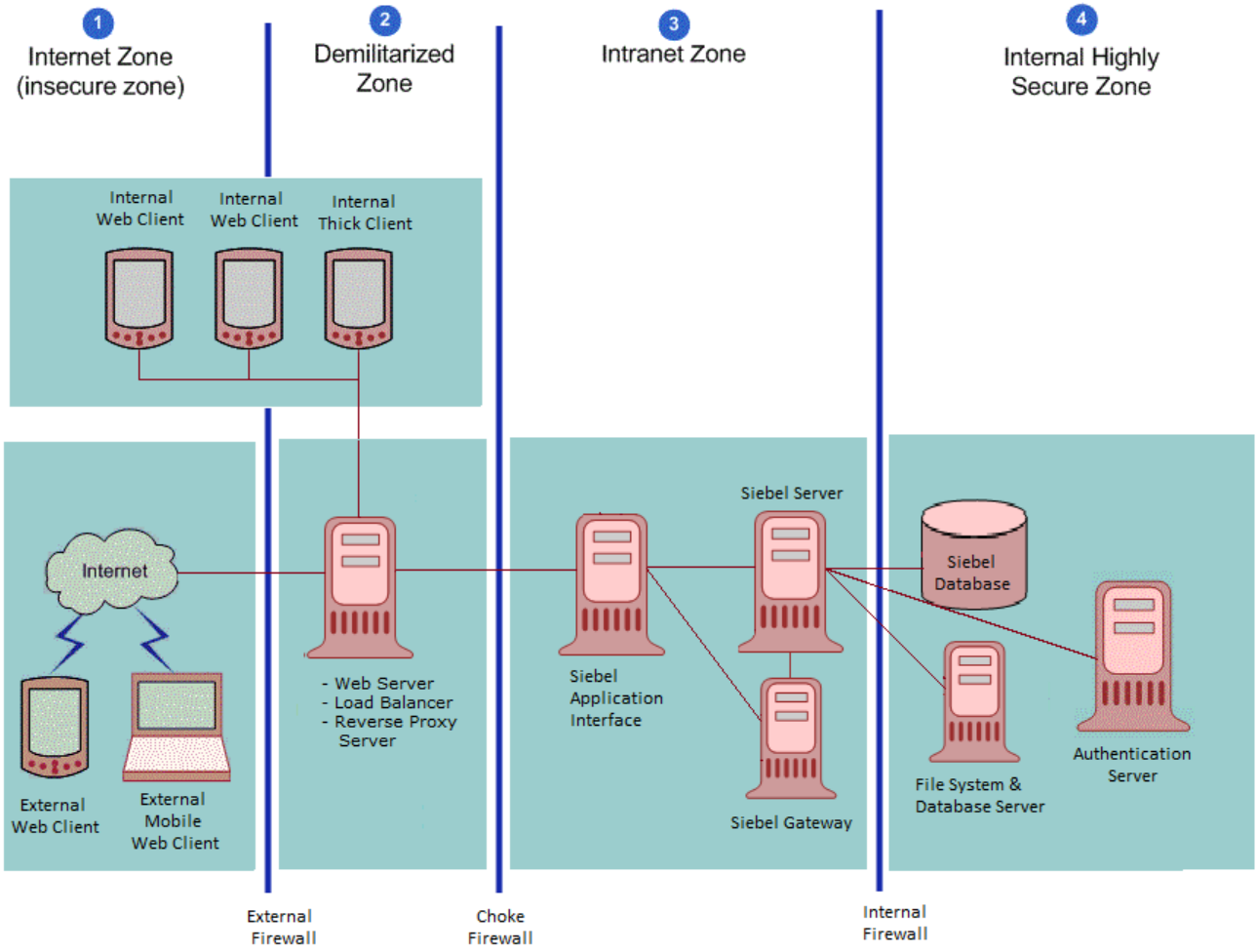
The following steps can help prevent DoS attacks from affecting your employee-facing Siebel Business Applications:

- Use different Web servers for public-facing applications and for employee-facing applications so that even if the public Web servers are overwhelmed, Web servers are still available to service employee applications. For additional information, see *Proxy Servers*.
- Run the employee-facing Application Object Managers and key components on different Siebel servers from those used to run public-facing Application Object Managers. This step helps to make sure that even if the Siebel Servers that process external applications are overwhelmed with requests, hardware resources are available to continue processing internal applications. For additional information, see *Load Balancers*.

Other methods available when configuring firewalls to assist in preventing DoS attacks include designing them to reject rapid requests from the same IP address, or to block specific IP addresses or domains. These methods are not foolproof and it might not be possible to use blocklisting on large public sites. For example, many DoS attacks use hijacked computers that are on large, well-known, Internet service providers. Blocklisting all of the users in these domains or IP ranges helps prevent the DoS attacks, but possibly prevents many valid users from using your Web site as well.

Recommended Network Topology

This topic describes the recommended topology for Siebel CRM deployments. The following figure shows the recommended placement of firewalls and related Siebel Enterprise Server components in a Siebel CRM deployment with internal and external users.



The Siebel network configuration for a secure deployment, as shown in this figure, is as follows:

1. **Internet zone.** External Siebel Web clients residing in the Internet zone access the Web server placed in the demilitarized zone through the external firewall.
2. **Demilitarized zone.** The Web server in this zone hosts a proxy server. The firewall keeps unauthorized users out of the protected network and the proxy server provides protection from various kinds of IP spoofing and routing attacks.
3. **Intranet zone.** The Application Interface is installed in the intranet zone. The Siebel Gateway and Siebel Servers are also placed in the intranet zone. Depending on the requirements and configured security adapter, the authentication mode can be one of the following: SSO/SAML, Database, LDAP, or Custom.

   > **Note:** The Application Interface accesses the migration database when it is deployed for migration.

4. **Internal highly secure zone.** This zone contains the Siebel Database and File System, and the authentication server (a Lightweight Directory Access Protocol (LDAP) server). Limit access to this zone to authorized system administrators and database administrators.

The network configuration approach illustrated in this figure follows a defense-in-depth strategy by placing firewalls between the zones of control with only appropriate ports open. A secure channel is implemented using Transport Layer Security (TLS) between the external Web clients and the Web server to take care of security in the insecure Internet.

Removal of Siebel Application Interface Dependency on Oracle Database Client

As of Siebel CRM 19.11 Update, Siebel Application Interfaces not co-located with migration servers no longer require the Oracle Database Client, which contains the Oracle LDAP Client co-located. As a result, the implications for the following deployment scenarios are:

- Application Interfaces servicing the migration server retain database access so there is no change for this deployment — you must continue to install the database client.
- All other Application Interfaces do not require database access and do not require the Oracle database client.

Existing deployments can either continue to run as previously deployed or adhere to the new guidelines.

Network Authentication and Monitoring

The following authentication practices are recommended to secure your network:

- Maintain and implement authentication information centrally in a Web single sign-on (SSO) environment, then copy the information to the demilitarized zone. It is recommended that the authentication information in the demilitarized zone is read-only, is encrypted while stored, and is encrypted when transferred between the authentication database and other components.
- Maintain access to the internal resources from any external network on the least-privilege principle to protect the internal network from being compromised.
- Allow services through the firewall only from specific IP addresses to specific IP addresses, depending on the business requirement.
- Deploy network-based Intrusion Detection Systems (IDS) in stealth mode within the zones of control, and restrict access to log files and to methods of setting log levels so that intruders cannot cover their tracks.

  Network-based IDS can be deployed to provide identification and notification capabilities and can be used to complement firewalls in thwarting attacks. Implement a real-time monitoring mechanism to react to any critical penetration attempts in a timely manner.
- Setup and maintain host-based IDS on bastion hosts (for example, email relay) with appropriate monitoring mechanisms in place to react to access violations. Deploy host-based IDS on all key computers to defend against common and company-specific violations from insiders and outsiders. Host-based IDS can help with monitoring and reporting user and network activity, auditing system configurations and vulnerabilities, checking file integrity, recognizing attack patterns, and auditing user activity for policy violations.
- Use scanning tools to find common security violations.
- Add all networking patches.
- Enable auditing and track users' login activity.

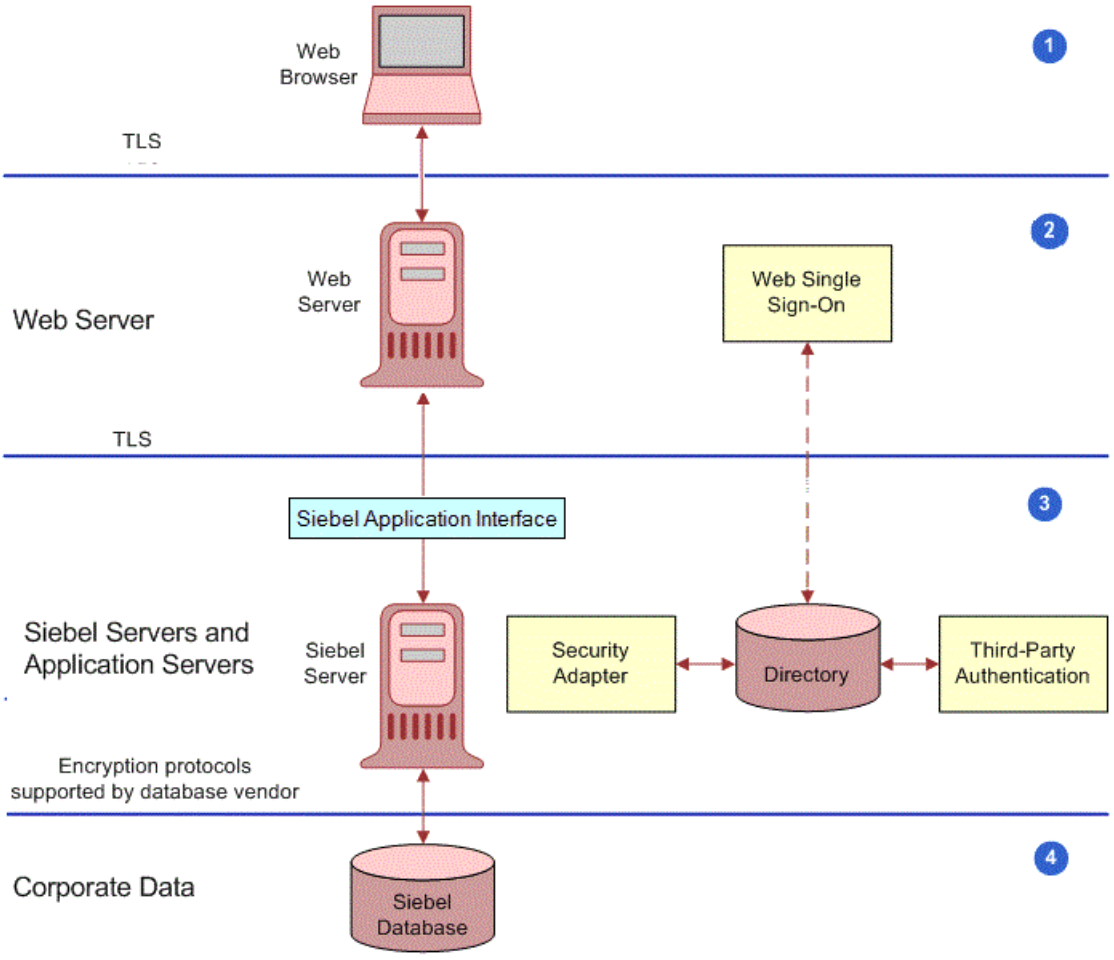
  For information on configuring and using Siebel Audit Trail, see *Siebel Applications Administration Guide* and *Implementing Auditing*.

Enabling Encryption of Network Traffic

If a Siebel CRM deployment over the Internet does not implement encryption between users' browsers and the Web server or between the Web server and application server, then such a deployment is susceptible to network sniffing and compromising of sensitive data. Implementing encryption for all network traffic and for all sensitive data prevents network sniffing attacks.

In Siebel CRM, 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.

The following figure shows the types of encryption available for communications within the Siebel environment. Encryption protects confidentiality along the entire data communications path, from the Web client browser to the Web server, to the Siebel Server, and back again. It is recommended that TLS 1.2 encryption is enabled where possible.



This figure shows that communications encryption is available in the following areas within the Siebel environment:

1. Between client browser to Web server

2. Between Web server to Siebel Server
3. Between Siebel Server to database
4. For database storage

For additional information on encryption options available, see the following topics:

- *Enabling Encryption Between the Web Client Browser and Web Server*
- *Enabling Encryption Between the Web Server and Siebel Server*
- *Enabling Encryption Between the Siebel Server and Siebel Database*
- *Enabling Encryption for Security Adapters*
- *About Using TLS with Siebel Enterprise Application Integration (EAI)*

Enabling Encryption Between the Web Client Browser and Web Server

Siebel CRM runs using the Siebel Web Client in a standard Web browser. When a user accesses a Siebel application, a Web session is set up 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 use of TLS for Web server and Siebel Web Client communications is transparent to Siebel CRM. For information on configuring TLS for Web server communications with the browser, see the vendor documentation.

You can specify the Web pages (known as views) within a Siebel application that are to use TLS.

Enabling Encryption Between the Web Server and Siebel Server

Siebel CRM components communicate over the network using a Siebel TCP/IP-based protocol for connections. You can secure connections using TLS. This technology allows data to be transmitted securely between the Web server and the Siebel Server.

Enabling Encryption Between the Siebel Server and Siebel Database

For secure transmission between the Siebel database and the Siebel Server, data can be encrypted using the proprietary security protocols specific to the database in use. For additional information, see your RDBMS vendor documentation.

Enabling Encryption for Security Adapters

You can implement TLS encryption for connections between a Siebel LDAP security adapter and a certified LDAP directory. By enabling encryption for the Siebel security adapter, a secure connection is established between the Siebel application and the directory server.

The procedure for implementing encryption for a security adapter varies according to the type of security adapter you implement. The following parameter must be set:

- To configure encryption for the LDAP security adapter, set the SslDatabase parameter value for the LDAP Security Adapter profile or named subsystem to the absolute path of the Oracle wallet directory.

For detailed information on implementing communications encryption for a security adapter, see *Installing and Configuring Oracle LDAP Client Software*.

About Using TLS with Siebel Enterprise Application Integration (EAI)

It is recommended that Siebel Business Applications external interfaces (EAI), which use Web services to send and receive messages over HTTP, encrypt communications using the TLS protocol.

The Siebel EAI HTTP Transport business service lets you send XML messages over HTTP to a target URL (Web site) and uses the Siebel Web Engine (SWE) to provide inbound messaging from an application that uses HTTP.

For outbound messages, Siebel CRM supports client authentication for TLS-based communications (mutual authentication) using the EAI HTTP Transport business service. For information on configuring mutual authentication, see *Transports and Interfaces: Siebel Enterprise Application Integration* and *Configuring TLS Mutual Authentication for SHA-2 Certificates Using EAI HTTP Transport*.

To enable TLS for inbound messaging using the EAI HTTP Transport business service, see *Communications Encryption*.

Securing the Siebel Web Server

Because a Web server is one of the most exposed and intruder-targeted elements in a network, securing the Web server is a priority. Before using your Web server in a Siebel CRM deployment, secure your Web server by applying vendor-recommended security procedures and practices as described in your Web server documentation. Then consider implementing the recommendations outlined in this topic.

Implementing a Proxy Server

Deploy a reverse proxy server in the demilitarized zone to protect the Web server from attacks relating to denial of service and directory traversal. For additional information, see *Proxy Servers*.

Monitoring Disk Space

Monitor the disk space available on your Siebel Web server. If the Web server is allowed to reach the disk space limit, then denial of service events can occur when the Siebel Server or Siebel Web clients connect to the Siebel Web server. For information on the tools that are available to monitor disk utilization for your Web server, see your Web server vendor documentation. For additional information on denial of service attacks, see *Preventing Denial of Service Attacks*.

Removing Unnecessary Subdirectories (Windows)

See the vendor-specific security documentation for information on removing unnecessary subdirectories in a Windows environment.

Encrypting Communications to the Web Server

It is recommended that you secure all communications between the Siebel Web Client, the Web server and the Siebel Server using TLS. For additional information on encrypting communications, see *Enabling Encryption of Network Traffic*.

Seeded Tomcat Web Server User

The Tomcat Manager UI is given access to userid: sadmin and password: sadmin by default (that is, out-of-the-box). The information is stored here: `"..\conf\tomcat-users.xml"`. It is recommended that you review this information and change the user authentication credentials for Tomcat Manager UI to protect from unwanted access.

Securing the Siebel Server

The following recommendations can enhance the security of your Siebel Servers.

Encrypting Communications to the Siebel Server

Enable encryption between the Web server and Siebel Server and between the Siebel Server and the Siebel database. For additional information on encrypting communications, see *Enabling Encryption of Network Traffic*.

To disable specific ciphers in Siebel EAI in Microsoft Windows, set the following in the windows registry, for UNIX please refer vendor specific document to disable cipher:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvid ers\SCHANNEL\Ciphers]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvid ers\SCHANNEL\Ciphers\cipher name]
"Enabled"=dword:00000000
```

Restricting Siebel Server Access

To restrict privileges to Siebel Server processes, assign an operating system account that is specific to the Siebel Server. Make sure this account has access only to files, processes, and executable files required by Siebel CRM.

- In Windows operating system environments, remove or limit the use of shared folders.
- In UNIX operating system environments:
  - Do not make the Siebel Server account the root administrator.
  - Disable UNIX r-services (for example, rlogin, rshell, rexec, rcp).

    R-services allow users to log in to and run various commands on a remote host computer. Before you can run the r-services on a remote host, you are required to provide authentication to access the host *unless* the local computer is listed in the .rhosts file, in which case authentication is not required. Therefore to provide the appropriate level of access and control to the Siebel Server, it is recommended that you disable the usage of r-services. Once you have disabled r-services, .rhosts files are not required and can be removed.

Encrypting the jndi.properties File

The user credentials in the jndi.properties file are stored in clear text format. To fix this, it is recommended that you encrypt the jndi.properties file as shown in the following procedure.

To encrypt the jndi.properties file

1. Set up the Siebel Server and the JMS server.
2. Create a named subsystem based on JMSSubsys.
3. Encrypt the jndi.properties file using the batch script files.

   Note the following:

   - The batch script files include the following: EncodeJndiProperties.sh, EncodeJndiProperties.bat, Siebel.jar, and ClientAppEAIJMSBsvDll.
   - The batch script files use the java-based encryption utility, com.siebel.eai.jms.EncodeJndiProperties, to encrypt the jndi.properties file and set the following properties in the JMSSubsys subsystem:
     - **JNDIEncryptionCheck.** Boolean value used to verify whether the jndi.properties file is encrypted (True) or not (False). The default value for JNDIEncryptionCheck is True.
     - **JNDIEncryptionSeed.** Seed value used to encrypt and decrypt the password.
   - The prerequisites for running the batch scripts include:
     - **<JNDI file name>** The full path to the jndi.properties file which is to be encrypted.

- **<Encryption seed>** The encryption seed for encrypting the jndi.properties credentials.
- **<Gateway Name>** The gateway name.
- **<Gateway Port>** The gateway port.
- **<Siebel Enterprise>** The Siebel enterprise name.
- **<Username>** The username to connect to the gateway.
- **<Password>** The password to connect to the server.
- **<Name Subsystem>** The named subsystem to set the seed for decryption.
- The batch scripts expect the user to set the SIEBEL_ROOT and JAVA_HOME environment variables.

4. Check the jndi.properties file to confirm that the password is actually encrypted.
5. To confirm that the setup works, use the Business Service simulator to run a test to set messages to the JMS server using the named subsystem created earlier in this procedure.

Securing the Siebel Client

The following general guidelines are applicable for securing all client computers that access Siebel CRM. For specific information on security recommendations for mobile clients, see *Securing Mobile Clients*.

Deploying Siebel Open UI

You can optionally deploy Siebel CRM 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.

Siebel Open UI has the following characteristics:

- Limited attack surface. 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.
- Transparent technology. Because the Siebel Open UI client is built entirely on standards, a variety of modern inspection tools can be used to validate the security compliance of your implementations.
- Compatibility with Data Execution Prevention features and virtualization. Because the Siebel Open UI client is a scripted client, it is fully compatible with Data Execution Prevention features for software or hardware, and compatible with virtualization features.
- Siebel Open UI clients enforce session security by requiring that session IDs can only be passed in session cookies. Siebel Open UI clients do not support cookieless mode.

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

Encrypting Communications for Web Clients

It is recommended that you secure all communications between the Siebel Web Client and the Web server using TLS, if support for this protocol is provided by your Web server. Encryption is not set by default. For additional information, see *Enabling Encryption Between the Web Client Browser and Web Server*.

Providing Physical Security for the Client Device

The physical security of the client device is handled outside of Siebel CRM. You can use utilities that provide computer-level security by enforcing computer passwords or encrypting the computer hard drive. Most leading mobile devices have user-enabled passwords.

It is recommended that you use a two-factor authentication approach for network components; this is a security process that confirms user identities using something users have and something they know. Requiring two different forms of electronic identification reduces the risk of fraud and protects against password attacks.

Defining a Policy for Unattended Personal Computer Sessions

Users should not leave workstations unattended while they are logged in to Siebel CRM. Doing so makes their computer potentially accessible to unauthorized users. Define a corporate policy for handling unattended PC sessions. Oracle recommends using password-locked screen saver features on all PCs.

Keeping Browser Software Updated

Update browser software when new versions are released; new releases often include additional security features. If you are using Internet Explorer, then check the Microsoft Web site for the latest browser security patches.

Certain Siebel CRM features and functions work in conjunction with security or other settings on the Web browser. Some of the security features provided by supported browsers and operating systems are not supported when used with Siebel CRM.

Detailed information about the browser settings used in deploying Siebel clients is provided in *Siebel System Administration Guide* . For more information about the settings in your Web browser, see the documentation that came with your browser.

Updating Security Patches

To protect against malicious software (malware), apply security patches provided by the desktop operating system provider on a regular basis. The same is true of patches released by antivirus software suppliers, and by companies that provide other third-party software products supported by Siebel CRM.

Securing Mobile Clients

Oracle provides a suite of mobile solutions that allow remote access to data within Siebel CRM. These solutions support a variety of mobile platforms, including smartphones, tablets, and laptop computers (running Siebel Mobile applications or Siebel Mobile Web Client). The following topics provide information about securing mobile devices running Siebel CRM:

- *Securing Siebel Remote*
- *Securing Mobile Devices Running Siebel CRM*

Securing Siebel Remote

Oracle's Siebel Remote enables a Siebel Mobile Web Client (MWC) that typically operates remotely in disconnected mode to connect to a Siebel Server so that the local client database can be synchronized with the enterprise Siebel database. Making the Siebel Remote architecture as secure as possible involves implementing security strategies for the following areas:

- *Securing the Synchronization Framework*
- *Encrypting Data in the Local Database and File System*
- *Defining Password Management Procedures*

Securing the Synchronization Framework

This topic outlines issues to consider and provides recommendations for securing the synchronization framework for Siebel Remote.

In addition to implementing the suggestions in this topic, make sure that you assign the least privileges required to the Siebel service owner account on the Siebel Server that runs the Synchronization Manager component. For additional information, see *Assigning Rights to the Siebel Service Owner Account*.

Authenticating the Mobile Web Client

By default, the Synchronization Manager does not authenticate incoming Remote client requests to make sure that the client is valid. It is recommended that you configure your Siebel application to require that client requests are authenticated by setting the value of the Authentication Method parameter of the Synchronization Manager to one of the supported authentication methods:

- Database
- LDAP

The synchronization session takes place through a fixed port that is dedicated to the Synchronization Manager; the default TCP/IP port number is 40400. The port number is set on the Synchronization Manager Server component and is then open in any firewall. Therefore, it is recommended that you change the default value of the port.

Encrypting Communications

The synchronization session can be managed using unencrypted communications, but it is recommended that you implement TLS encryption.

To use encryption, both the Siebel Server and the Remote client must enforce encryption in their connection parameters. To enable encryption, set the Encryption Type parameter of the Synchronization Manager Server component to TLS and change the DockConnString parameter in the [Local] section of the client .cfg file to the same value. For additional information, see *Siebel Remote and Replication Manager Administration Guide* .

Encrypting DX Transaction Files

Siebel Remote allows Mobile Web Clients to connect to a Siebel Server and exchange updated data and files during the synchronization process. The updated data is sent to or retrieved from the server in the form of .dx transaction files.

To protect your data, encrypt the .dx files using any suitable third-party utility, such as Pretty Good Privacy (PGP), when the files are removed from the `\docking` folder for any reason. To secure the .dx files within the `\docking` folder during run time, operating system-level encryption techniques can be used, for example, Microsoft Windows Encrypting File System, so that encryption and decryption are performed dynamically.

> **CAUTION:** Implementing operating system-level encryption on the `\docking` folders can adversely affect data replication.

Using a VPN When Synchronizing Through the Internet

It is recommended that every synchronization session occur within the corporate firewall. If your deployment of Siebel CRM must support synchronization through the Internet from outside the firewall, then it is recommended that you use a Virtual Private Network (VPN).

If there is a firewall on the network between the synchronization client and the Siebel Server, or between the VPN server and the Siebel Server, then the port for synchronizing with the Siebel Server must be opened on the firewall,

and this port must be a port other than port 80. If a VPN connection is not used, then it is possible that your Internet Service Provider (ISP) or another host on the route might block communications on this particular port. For additional information, see *Siebel Remote and Replication Manager Administration Guide* .

Encrypting Data in the Local Database and File System

The Siebel Mobile Web Client uses a local database to store data for user access and uses a local Siebel File System to store files. This topic outlines recommendations for securing both.

Local Database

Two local database template files are provided with Siebel CRM for use with Siebel Remote. These templates provide the starting point to generate your own database template:

- **sse_utf8.dbf.** A template that is not encrypted.
- **sse_encr.dbf.** A template that is encrypted with standard Sybase encryption.

By default, the template that defines the local database schema is not encrypted. It is recommended that you use the encrypted local database template to encrypt the entire local database, thereby providing a layer of security against unauthorized access to the local database.

To use an encrypted database template for mobile clients, the Generate New Database and Database Extract tasks must be configured and run using the sse_encr.dbf template. For information, see *Siebel Remote and Replication Manager Administration Guide* .

Local Siebel File System

If the local Siebel File System is used to store highly sensitive data, then it is recommended that you encrypt the local Siebel File System, either using third-party products or encryption features provided by your operating system.

Defining Password Management Procedures

When using the Siebel Mobile Web Client, secure access to the Siebel Server and to data on the local database by implementing password management procedures as follows:

- Implement the following password functionality for local database authentication provided by Siebel CRM:
  - Lock applications after a given number of failed-access attempts.
  - Disable passwords after a given period.
  - Check password formats based on specified rules.
  - Reset user passwords. The administrator performs this task.
- To guard against unauthorized administrative access to the local database, change the local database DBA password from the default value, which is the first eight characters of the Siebel Enterprise name.

  Specify a password for the local DBA by modifying the value of the New DBA Password parameter when generating a new database template.
- Enable password hashing. For information on this task, see *About Configuring Password Hashing for Users*.

Securing the Siebel Document Server

Siebel Correspondence, Siebel Presentations, and Siebel Proposals all use the Siebel Document Server to generate Microsoft Word and Microsoft PowerPoint documents through the Web. All document templates come in through the Siebel Server. As such, the Siebel Server controls security and represents the only client that interacts directly with the Siebel Document Server. For more information about Siebel Document Server, see *Siebel Correspondence, Proposals, and Presentations Guide* .

Perform the steps in the following procedure to secure the Siebel Document Server.

To secure the Siebel Document Server

- Set up the appropriate permissions on the Siebel Document Server.

  It is recommended that only the user who authenticates as the Siebel service owner is given access to the Siebel File System and the ability to execute permissions on the Siebel Document Server. For additional information, see *Securing the Siebel File System*.
- Set a high-security level for macros.

  It is recommended that you set a high-security level for macros so that untrusted macros cannot be executed by the Siebel Document Server. This setting prevents the execution of malicious code in a document.
- Implement an antivirus policy.

  Make sure an antivirus policy is in place for computers that supply templates to the Siebel Document Server. By default, the operating system does not check for viruses or malicious code in a file. It is recommended that you check for viruses on all the templates that are submitted to the Siebel Document Server.
- Microsoft provides some standard utilities in the Resource kit to lock down security on a generic Microsoft Windows computer. It is recommended that tools, such as C2.exe be implemented to secure such an environment. These tools are readily available from Microsoft.

Securing Email Communications

This topic provides information on securing the Email server and email communications in a Siebel environment.

Siebel Email Response allows organizations to manage and respond to a large volume of incoming email. Siebel Email Response works in conjunction with the Siebel Communications Server and your third-party email server to process email. Both Siebel Email Response and Siebel Communications Server are installed with the Siebel Server.

The Siebel Communications Server uses communications driver files to communicate with the email system and to support inbound and outbound email processing. Oracle supports the Internet SMTP/POP3 Server and the Internet SMTP/IMAP Server for use with email servers that support the SMTP protocol for outbound email messages, or the POP3 or IMAP protocol for inbound email.

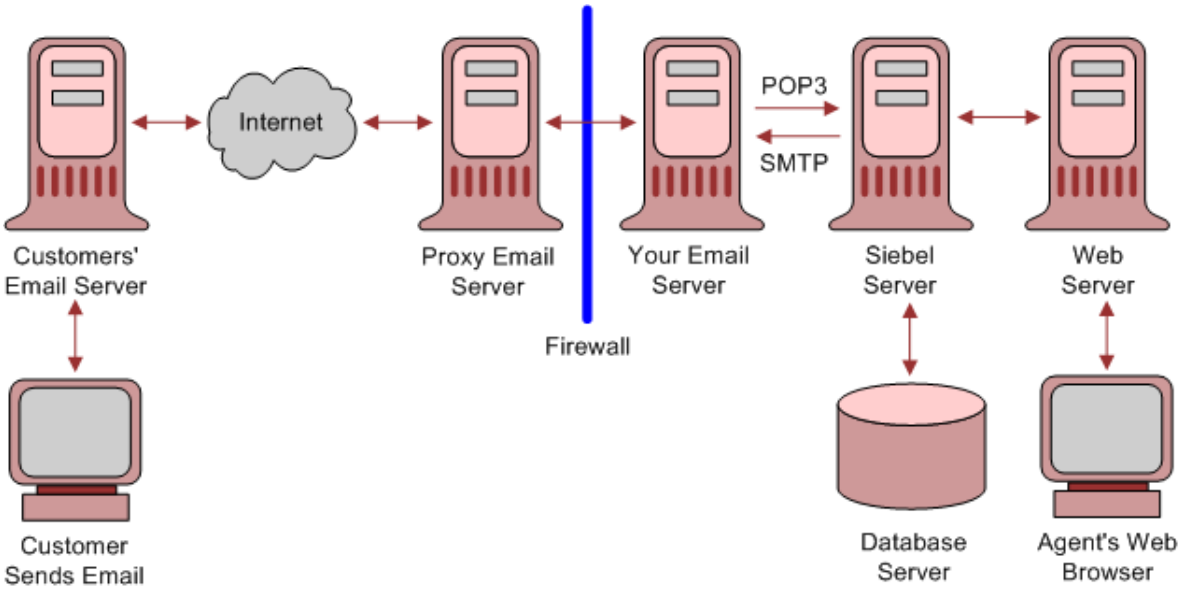
Implement the recommendations in the following topics to increase the security of your Siebel email environment:

- *Securing the Email Server*
- *Encrypting Communications Between the Siebel Server and the Email Server*
- *Deleting Processed Email Messages*

Securing the Email Server

The Siebel Email Response workflow begins when a customer sends an email to your company over the Internet. The email passes through the customer's email server and communicates with your email server, which receives the email and passes it to the Communications Inbound Receiver (CIR) on the Siebel Server.

To secure your environment, it is recommended that you deploy a proxy email server (SMTP Proxy) to process all incoming emails and a dedicated email server to process only the mailboxes used by Siebel Email Response on the Siebel Server. The following figure shows the recommended placement of email servers, with your Siebel Email Server secured behind the firewall.



Encrypting Communications Between the Siebel Server and the Email Server

The Siebel Communications Server uses the Internet SMTP/POP3 Server and the Internet SMTP/IMAP Server communications driver files to support Siebel email processing. Configuring parameters for the driver files allows you to determine email processing behavior for your environment.

To provide secure transmission of email data between the Siebel Server and the email servers, it is recommended that you enable TLS communications for SMTP, IMAP, and POP3 sessions. The following procedure describes how to enable a TLS connection for the Internet SMTP/POP3 or the SMTP/IMAP Server driver.

To enable TLS communications for SMTP, IMAP and POP3 sessions

1. Navigate to the Administration - Communications screen, then the Communications Drivers and Profiles view.
2. In the Communications Drivers list, select either the Internet SMTP/IMAP Server Driver or the Internet SMTP/POP3 Server Driver.
3. Click the Profiles view tab then, in the Profiles list, select the relevant profile.

4. In the Profile Parameter Overrides list, add new records as required for the following parameters and set the value of each to TRUE:

   You can also enable a TLS connection for the Internet SMTP/POP3 or the SMTP/IMAP Server drivers provided you are using Microsoft Exchange Server as your email server. Enable TLS using the following parameters:

   - Enable TLS for IMAP
   - Enable TLS for POP3
   - Enable TLS for SMTP
   - Enable TLS for Backup SMTP

For information on setting the SMTP/POP3 or SMTP/IMAP Server driver parameters to enable TLS, see *Siebel Email Administration Guide* .

Deleting Processed Email Messages

In a Siebel production environment, it is recommended that once incoming and outgoing email messages have been processed, they are deleted from the Siebel Server. The following parameters for the Internet SMTP/POP3 Server and the Internet SMTP/IMAP Server driver files determine whether or not messages are stored after processing:

- Delete Processed Messages

  Incoming email messages retrieved from the IMAP or POP3 server are saved to the Incoming Email directory as temporary files where they remain until they are processed. If you set the Delete Processed Messages parameter to TRUE (recommended), then the temporary files are deleted from the directory when the messages have been processed. If the Delete Processed Messages parameter is FALSE, then the processed temporary files are stored in the Processed Email directory.

- Save Sent Messages

  Whether or not copies of email messages that have been sent are saved on the Siebel Server is determined by the value set for the Save Sent Messages parameter. If the parameter is set to TRUE, then sent messages are saved to the Sent Email directory after processing. If the Save Sent Messages parameter is FALSE (recommended), then sent messages are not saved.

To prevent email messages from continuing to be stored on the Siebel Server after they have been processed, perform the steps in the following procedure.

To delete processed email messages

1. Navigate to the Administration - Communications screen, then the Communications Drivers and Profiles view.
2. In the Communications Drivers list, select either the Internet SMTP/IMAP Server Driver or the Internet SMTP/POP3 Server Driver.
3. Click the Profiles view tab and, in the Profiles list, select the profile you want to configure.
4. In the Profile Parameter Overrides list, add two new records using the values shown in the following table:

Name	Value
Delete Processed Messages	TRUE
Save Sent Messages	FALSE

For additional information on setting the SMTP/POP3 or SMTP/IMAP Server driver parameters, see *Siebel Email Administration Guide* .

Securing the Siebel Reports Environment

Siebel CRM uses Oracle BI Publisher to generate Siebel reports. In a disconnected Siebel Reports environment, user authentication mechanisms aren't required.

In the Siebel Reports connected environment, Oracle BI Publisher is installed separately from Siebel CRM and access to the BI Publisher Server is authenticated. To authenticate user access to the BI Publisher Server in a Siebel Reports connected environment, you can implement one of the following:

- **Siebel Security Model.** This model provides authentication using the EAI Application Object Manager.
- **LDAP security model.** This model provides authentication against a directory.

For information on the methods available to authenticate user access to the BI Publisher Server in a Siebel Reports connected environment, see *Integrating Oracle Publisher with Siebel*.

Guidelines for Providing Additional Security for Oracle BI Publisher

To provide additional security for Oracle BI Publisher, the following steps are also recommended:

- **Change default ports to nonstandard ports.** As with other components, the Oracle BI Publisher installation is configured to run on a default set of ports.
- **Implement operating system-level encryption to dynamically encrypt Oracle BI Publisher configuration files.** Encrypting the configuration files protects them from being read by every user who has access to the BI Publisher Server.

Securing the Operating Systems

This topic contains recommendations for securing your operating system. Securing your operating system contributes to the overall level of security that applies to Siebel CRM.

Securing operating systems is the first step towards safeguarding the Siebel CRM deployment from intrusion. Workstations and servers are typically installed with a multitude of development tools and utilities. Securing an operating system involves the removal of all nonessential tools, utilities, and other system administration options. This process also requires that all appropriate security features are activated and configured correctly, and includes the following tasks:

- Protecting files and resources
- Restricting accounts and services to those who need them
- Applying and maintaining patches and product updates
- Performing maintenance activities, such as running security software

Note: Before implementing the security recommendations for operating systems described in this topic, perform all the security steps outlined in your operating system documentation. Security guidelines for operating systems are generally available on vendor Web sites.

Protecting Files and Resources

Protect files and resources in your operating system environment as follows:

- Set up access restrictions to executable files, data files, Web pages, directories, and administrative tools as follows:
    - On each server that is a part of a Siebel deployment, restrict local user access to Siebel directories to Siebel administrators only. This restriction prevents insiders with access to the computer, but without Siebel administrator privileges, from accessing sensitive information that can be used to gain, or elevate Siebel privileges, thereby allowing more significant security violations to occur.
    - For Siebel deployments that store highly sensitive data or that have other high-security requirements, it is recommended that you encrypt the Siebel File System and all server disks containing Siebel CRM data, either using third-party products or encryption features provided by your operating system.
    - If you configure Siebel-specific environment variables that include sensitive data on a computer hosting a module in a Siebel deployment, for example, if you have implemented a Siebel Product Configuration Application Object Manager on a dedicated Siebel Server, then encrypting the server disks is also recommended.

      For information on deploying the Siebel Configurator, see *Siebel Deployment Planning Guide* . For information on setting Siebel-specific environment variables, see *Siebel System Administration Guide* .
- Audit file permissions, file ownership, and file access.
- Restrict access to accounts and services.

  Controlling access is an important element in maintaining security. The most secure environments follow the least-privilege principle, which grants users the least amount of access that still enables them to complete their required work. Set up hosts to allow only those services (ports) that are necessary and run only with the fewest possible services. Eliminate services with known vulnerabilities.
- Run the checksum utility on system files when installed and check for Trojan malware frequently. (A Trojan is software that appears legitimate but which contains malicious code that is used to cause damage to your computer.) Check user file systems for vulnerabilities and improper access controls.
- Verify operating system accounts and make sure they have passwords that are difficult to guess.
- Automatically disable accounts after several failed login attempts.
- (UNIX) Limit root access.
- Manage user accounts:
    - Do not share user accounts.
    - Remove or disable user accounts upon termination.
    - Require strong passwords.
    - (Windows) Disable automatic logon.
    - (UNIX) Use a restricted shell.
    - (UNIX) Disable login for well-known accounts that do not need direct login access (bin, daemon, sys, uucp, lp, adm).
- Restrict guest accounts:
    - As with any account, create a guest account only for the time required and remove the account when it is no longer required.

- Use a non-standard account name for the account; avoid the name guest.
- Use a strong password.
- (UNIX) Use a restricted shell. If reasonable, give the account an 077 unmask.

Restricting EAI File Transport File System Access

The EAI File Transport Business Service reads and writes files by using the “FileName” input argument. The paths supplied to the FileName parameter for reading and writing are validated against the directories specified in the “EAIFileTransportFolders” enterprise parameter .

Siebel CRM restricts both read and write access to explicitly permitted directories.

The default permitted directories are the Siebel temporary directory, the xsd . smartanswer and xmlp directories (under SIEBEL_HOME), and canonical operating system paths configured for the Siebel File System. Additional directories must be configured in the "EAIFileTransportFolders" enterprise parameter.

The configured directories are treated as an allowlist. To allow the EAI File Transport Business Service to access a directory, configure the directory itself or a parent directory that is intended to contain all allowed files. Use the most specific directory that satisfies the integration requirement.

Configure the EAIFileTransportFolders Enterprise Parameter

If an integration uses the EAI File Transport Business Service to read from or write to any directory other than the default permitted directories, then the directory must be added to "EAIFileTransportFolders" enterprise parameter.

Access is retained for the following default directories:

- The Siebel temporary directory.
- The xsd directory under SIEBEL_HOME.
- The smartanswer directory under SIEBEL_HOME.
- The xmlp directory under SIEBEL_HOME.
- Canonical operating system paths configured for the Siebel File System.

Examples of directories that still require explicit configuration include:

- A custom inbound or outbound integration directory.
- A directory under SIEBEL_HOME other than xsd. smartanswer and xmlp
- A directory under a Siebel File System location that cannot be resolved as a canonical operating system path.
- Any external shared directory that is not configured as a Siebel File System root.

Configure only directories that the EAI File Transport Business Service must access. Do not configure broad directories such as a drive root, SIEBEL_HOME, or the root of a shared file system unless there is a documented business requirement, and the operating system permissions are restricted appropriately.

Configure Allowed Folders Using Server Manager

Use Siebel Server Manager to set the EAIFileTransportFolders enterprise parameter for directories that you wish to add. Specify absolute paths. Separate multiple directories with semicolons.

On Windows (example):

```
srvrmgr -g gateway_host:gateway_port -e enterprise_name -u user_name -p password
change enterprise param EAIFileTransportFolders="D:\Siebel\eai_in;D:\Siebel\eai_out"
```

On UNIX or Linux (example):

```
srvrmgr -g gateway_host:gateway_port -e enterprise_name -u user_name -p password
change enterprise param EAIFileTransportFolders="/siebel/eai/in;/siebel/eai/out"
```

If a value is already configured in the list for the parameter, preserve the existing entries and append the new directory, separated by a semicolon.

After changing this enterprise parameter, restart the affected Siebel Server components, such as the Application Object Manager or EAI Object Manager components that invoke the EAI File Transport Business Service.

Accessing the XSD Directory

Access to the xsd, smartanswer and xmlp directories under SIEBEL_HOME is retained after Siebel 26.10. For example, if SIEBEL_HOME is D:\Siebel\siebsrvr, then the EAI File Transport Business Service can read from and write to this directory without adding it to EAIFileTransportFolders:

```
D:\Siebel\siebsrvr\xsd
```

If you want to use a different XSD staging directory outside SIEBEL_HOME\xsd, then that directory must be configured in EAIFileTransportFolders.

Accessing the Siebel File System Attachment Directory

For example, if the Siebel File System is configured as \\fileserver\siebelfs$, then the EAI File Transport Business Service can access files under the file system root, including att, after the path is canonicalized:

```
\\fileserver\siebelfs$\att
```

If the Siebel File System is configured as an abstract value such as FSM, and a supported integration must access the att directory by path, configure the actual operating system path:

```
change enterprise param EAIFileTransportFolders =\\fileserver\siebelfs$\att
```

Use the narrowest path possible. If only one integration staging directory is required, configure that staging directory instead of the entire Siebel File System.

Important Considerations

- Parent-directory path components such as .., ..\, and ../ are not allowed to be accessed by using the EAI File Transport Business Service.
- EAI File Transport Business Service compares canonical paths with the configured allowed folders.
- The operating system directory must exist and be accessible to the Siebel Server process account.
- Operating system permissions still apply. The Siebel Server process account must have the required read or write permissions for the configured directory.
- Configuring a directory in EAIFileTransportFolders enterprise parameter does not bypass Siebel access control, responsibility configuration, business service access control, or operating system access control.
- For Siebel File System content, use standard Siebel File System and attachment APIs where possible. Direct EAI File Transport access to Siebel File System directories is intended only for integrations that explicitly require file-path-based access.

Siebel File System Paths

The EAI File Transport Business Service can permit the Siebel File System by default only when the Siebel File System value resolves to one or more canonical operating system paths. If the file system is configured as an abstraction that does not resolve to a local or shared operating system path for the Siebel Server process, then the EAI File Transport Business Service cannot canonicalize it and cannot use it as a default allowed folder.

For example, the following values can be canonicalized if the paths exist and the Siebel Server process account can access them:

```
D:\Siebel\FileSystem
\\fileserver\siebelfs$
/siebel/filesystem
```

The following values require caution because they are not direct operating system folder paths for EAI File Transport validation:

```
FSM
FileSystem
$FileSystem
```

If the Siebel File System configuration uses an abstract value, configure the actual operating system directory in the EAIFileTransportFolders parameter when direct EAI File Transport Business Service access is required.

Securing the Siebel File System

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

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

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

To provide additional security for the Siebel File System, implement the following recommendations:

- When creating the shared directory for the Siebel File System, append a dollar sign ($) to the end of the share name; this hides the shared directory on the network. For example:

  ```
  \\servername\siebelfs$
  ```

- Use third-party utilities to encrypt the file system or individual folders within the file system.
- Make sure that the Siebel application does not provide direct user access to the Siebel File System by restricting access rights to the Siebel File System directory to the Siebel service owner and the administrator. For information, see *Assigning Rights to the Siebel File System*.
- Restrict the types of files that can be saved in the Siebel File System as described in *Excluding Unsafe File Types from the Siebel File System*.

Assigning Rights to the Siebel File System

This topic describes how to restrict access rights to the Siebel File System directory to the Siebel service owner and the administrator.

The processes and components of the Siebel Server use the Siebel service owner account to operate. Do not give the Siebel service owner account permission to access any directory other than the Siebel File System directory and the Siebel Server directories.

The following procedures describe how to assign rights to the Siebel File System on Windows and UNIX platforms.

Assigning Rights to the Siebel File System on Windows

Use the following procedure to assign the appropriate rights to the Siebel File System on Windows.

To assign the appropriate rights to the Siebel File System on Windows

1. In Windows Explorer, navigate to the Siebel CRM directory, for example, SBA_82.
2. Right-click the Siebel CRM directory, and select the Sharing and Security option.
3. Click the Security tab.
4. Select the Advanced option.
5. Deselect the Inherit from parent permissions check box.
6. When prompted, select the Remove option.
7. Check the Replace permission entries on all child objects option.
8. Click Add and assign full control permissions to administrators and the Siebel Service account. Administrators require full rights on the Siebel File System to perform backup or recovery tasks
9. Click OK.

   The file permissions are replicated on all child objects.
10. Repeat this procedure for the Document Server directory. Assign file system rights through the Microsoft Management Console and the security template snap-in.

Assigning Rights to the Siebel File System on UNIX

Use the following procedure to assign the appropriate rights to the Siebel File System on UNIX.

To assign the appropriate rights to the Siebel File System on UNIX

1. Log in as root to the file system server.
2. Using the appropriate administrative tools for your UNIX operating system, verify that only the Siebel Service account and the Siebel administrator have read, write, and execute permissions to the Siebel File System directory; remove permissions to the Siebel File System directory for all other users.

   For example, run the following command to remove all permissions (read, write, and execute) to the Siebel File System directory for all users and groups except the owner of the Siebel File System directory (Siebel Service account):

   ```
   chmod -R go-rwx FileSystemDirectory
   ```

   where `FileSystemDirectory` is the name of the Siebel File System directory.

Excluding Unsafe File Types from the Siebel File System

You can prevent files with a specific file extension from being saved to the Siebel File System by enabling the File Ext Check system preference. This topic describes how to implement file extension checking, and how to specify the file types you want to exclude from the Siebel File System.

When you select a file type to be excluded, Siebel Application Object Manager components are prevented from adding any files with that file extension to the Siebel File System, including files from external sources, such as Siebel CRM Desktop, or files from a custom integration point which the Enterprise Application Integration (EAI) Application Object Manager might attempt to add.

> **Note:** Files with file extensions that you choose to exclude that are added to the Siebel File System before you implement file extension checking are not removed from the system. You must review and remove these existing files manually, if required.

Potentially Unsafe File Types

The purpose of excluding files with specific file extensions from the Siebel File System is to protect your Siebel CRM implementation from viruses or other malicious code potentially contained in these files. Executable files, such as batch files and program execution files, which are designed to run tasks automatically, are the most obvious types of files you might want to exclude.

This table shows a list of executable files on Windows and UNIX.

Extension	Operating System
bat	Windows
bin	Windows and UNIX
cmd	Windows
com	Windows
csh	UNIX
exe	Windows
inf	Windows
jse	Windows
ksh	UNIX
reg	Windows
run	UNIX

Extension	Operating System
sh	UNIX
vbe	Windows
vbs	Windows

Enabling File Extension Checking

Perform the steps in the following procedure to enable file extension checking.

To enable file extension checking

1. Log in to a Siebel application on the Siebel Server.
2. Navigate to Administration - Application, and then the System Preferences view.
3. In the System Preferences list, either query for the system preferences shown in the following table or create the system preferences if they do not already exist, then enter values similar to those shown.
4. Stop then restart the Siebel Server for the new system preference values to take effect.

System Preference Name	System Preference Value
DCK:Flag For File Ext Check	Enter either Y or N to indicate whether or not you want to enable file extension checking. The default value is N.
DCK:Excluded File Ext	Enter the file extensions you want to exclude in the following format: **`file extension1,file extension2,file extensionn`** For example: **`bat,bin,cmd,com,csh,exe,txt,gif,jpg`** You can enter up to 100 characters in the System Preference Value field. If you want to specify additional file extensions to exclude, then create one or more DCK:Excluded File Ext N system preference entries.
DCK:Excluded File Ext N	If you want to exclude file extensions that cannot be accommodated in the DCK:Excluded File Ext system preference, then use this system preference to specify the additional file extensions. • In the System Preference Name field, change the value of N to a number between 1 and 9, starting with 1 and increasing incrementally up to 9 with each additional DCK:Excluded File Ext N entry you create.

System Preference Name	System Preference Value
	• In the System Preference Value field, enter the additional file extensions you want to exclude in the following format: `file extension1,file extension2,file extensionn` You can enter up to 100 characters in the System Preference Value field. **Note:** If the DCK:Excluded File Ext system preference does not exist, the DCK:Excluded File Ext N system preference is not processed.

About File Extension Checking on the Siebel Mobile Web Client

You can configure file extension checking on the Siebel Server and on Siebel Mobile Web Clients. To implement new system preference values defined on the Siebel Server on the Siebel Mobile Web Client, synchronize the Siebel Mobile Web Client with the Siebel Server, then stop and restart the Siebel Mobile Web Client.

The file extension checking settings you specify at the Siebel Server level take precedence over Siebel Mobile Web Client settings. For example, if the file extension .exe is among the list of excluded file extensions on the Siebel Server, but is not excluded by the Siebel Mobile Web Client, when the Siebel Web Client connects to the Siebel Server to synchronize the local database, the following occurs:

- All attachment records with the .exe file extension are rejected for synchronization with the enterprise database
- A delete operation for each attachment record of type .exe is generated

During the next synchronization session, the delete operations for the rejected attachment records are executed on the Siebel Mobile Web Client and all the attachment records with the extension .exe are deleted.

Assigning Rights to the Siebel Service Owner Account

Siebel CRM is installed using the Siebel service owner account. This account must belong to the Windows domain of the Siebel Enterprise Server (Windows environments) or to the users group of the Siebel Enterprise Server (UNIX environments) and must have full write permissions to the Siebel File System.

Implement the following recommendations for the Siebel service owner account:

- Make sure a strong password has been set for the Siebel service owner account.

  For information on changing the password for the Siebel service owner account, see *Changing and Managing Passwords*.
- Set the user account policy to lock the account after three unsuccessful login attempts.
- Assign appropriate rights for the account as described in the following procedures.

For information on creating the Siebel service owner accounts, see *Siebel Installation Guide* .

Assigning Rights to the Siebel Service Owner Account on Windows

The following procedure describes how to assign rights for the Siebel service owner account on Windows.

To assign rights to the Siebel service owner account (Windows)

1. From the Start menu, select Settings, Control Panel, Administrative Tools, and then choose Local Security Policy.
2. Select Local Policies.
3. Click User Rights Assignments.
4. Assign the following rights to the Siebel service owner account:
    - Act as part of the operating system
    - Lock pages in memory
    - Bypass traverse checking
    - Log on as a service
    - Replace a process level token
    - Deny logon locally

    Do not assign the Siebel service owner account any rights other than those listed. Use the local security policy editor to assign user rights for the Siebel service owner account.

    The Siebel service owner account must be part of the Local Administrator Group (not the Local Users Group), otherwise the Siebel Server service will not start. The Siebel service owner account might be the same administrator account under which Siebel CRM modules are installed, or a different account that is part of the administrator group.

Assigning Rights to the Siebel Service Owner Account on UNIX

The following procedure describes how to assign rights for the Siebel service owner account in a UNIX environment.

To assign rights for the Siebel service owner account (UNIX)

1. Log in as root on the Siebel application server.
2. Using the appropriate administrative tools for your UNIX operating system, for example, the System Management Interface Tool (AIX), select the user who runs the Siebel service.
3. Check that the Siebel service does not run as the root user.

> **Note:** You must set the execute bit for the `/siebsrvr/webmaster` directory for the Siebel service to function. The Siebel service account requires permission to run the `netstat` command to perform the installation successfully. Otherwise, the installation fails.

Applying Patches and Updates

Keep track of updates, service packs, hot fixes, and patches. Evaluate the need for patches before installing them on production systems. Test patches on development or staging systems, not on production systems, because security patches can disable services or introduce additional vulnerabilities. Set up a process for testing and implementing any updates for Siebel CRM that are released. See the Oracle Critical Patch Updates and Security Alerts Web site at

http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Securing the Siebel Database

This topic outlines recommendations for securing your Siebel database after you have performed the security procedures prescribed by your database vendor. For information on these procedures, refer to your relational database management system documentation. Information about the following is included in this topic:

- *Restricting Access to the Siebel Database*
- *Reviewing Authorization Policies*
- *Protecting Sensitive Data in the Siebel Database*
- *Maintaining Database Backups*

Restricting Access to the Siebel Database

Sensitive user information, such as credit card numbers, customer details, email IDs, and so on, is usually stored in the database that an application is using. It is important to classify the data that is stored in the database and to implement a role-based access system.

Define stringent policies for Siebel database access both at the account-login level and at the network-visibility level. Only assign authorized users, for example, approved database administrators (DBAs), system accounts for root usage and remote access to the server.

Define access rules so that users cannot log in to the Siebel database and run queries. Follow these guidelines for the operating systems:

- **Windows.** Add all general users to the Public group in the Siebel database and assign appropriate rights.
- **UNIX.** Do not grant database administrator privileges to general users.

For additional information, see your RDBMS documentation.

Reviewing Authorization Policies

Implement the following recommendations:

- Restrict access to SQL trace and log files.

  In a production environment, do not run Siebel CRM with a high level of logging, for example, use log level 2, not 5.
- Restrict remote access to the operating system, such as through Telnet (Terminal Network), and restrict remote access diagnostics programs.
- Limit access to the data dictionary files; these files store metadata about schema definitions, visibility rules, and other items.

Protecting Sensitive Data in the Siebel Database

It's recommended that you protect sensitive application data in the Siebel database by encrypting the data. You can choose to encrypt the following:

- Specific database fields
- Specific database tables
- The entire database

Siebel CRM supports field-level encryption of sensitive information stored in the Siebel database, for example, credit card numbers or national identity numbers. You can configure Siebel CRM to encrypt field data before it's written to the Siebel database and decrypt the same data when it's retrieved. This configuration prevents attempts to view sensitive data directly from the Siebel database.

Siebel CRM supports data encryption using Advanced Encryption Standard (AES). By default, data encryption isn'tconfigured. It's recommended that you set data encryption for business component fields using Siebel Tools. For information on encrypting data, see *Communications and Data Encryption*.

When field-level encryption is implemented, data isn't decrypted until it's displayed by a user who has the necessary privileges to view the data. The data remains encrypted even when it's loaded into memory, which increases data security. However, using field-level encryption affects performance.

As an alternative to field-level encryption, you can secure sensitive data using products such as the following:

- **Transparent Data Encryption.** If you're using a Microsoft or Oracle database with Siebel CRM, then you can use the Transparent Data Encryption feature to encrypt data in the Siebel database. Oracle databases support the use of Transparent Data Encryption to encrypt data at the column and tablespace level. Microsoft databases support the use of Transparent Data Encryption to encrypt data at the cell and database level.
  Transparent Data Encryption encrypts data when it's written to the database and decrypts it when it's accessed by Siebel CRM. Application pages are decrypted as they're read and are stored in memory in clear text.
  Because the data isn't encrypted when it's being sent to Siebel CRM, you must also enable TLS to protect communications between the server and clients. The performance impact of implementing Transparent Data Encryption is minimal.
- **Oracle Database Vault.** If you're using an Oracle database with Siebel CRM, then you can use Oracle Database Vault to restrict access to all the schemas and objects in your application database, or to individual objects and schemas by users, including users with administrative access to the database.
  Oracle Database Vault lets you define a Realm, a protection boundary, around all or some objects in your database. The database administrator can work with all the objects within the Realm but can't access the application data that they contain. This restriction protects your data from insider threats from users with extensive database privileges.

Maintaining Database Backups

Implement the following database backup policies:

- Back up the Siebel database at regular intervals and store the backups securely for the period required by your organization’s retention policies.
- Limit access to the backups to authorized users.

- Encrypt Siebel database backups.
- Secure the devices on which the Siebel database backups are stored.

Securing Siebel Business Applications

This topic describes how to protect Siebel CRM by configuring the security features. It includes the following topics:

- *About Securing Applications*
- *Guidelines for Deploying Siebel CRM*
- *About Disabling Siebel Components*
- *About User Authentication*
- *Implementing Password Management Policies*
- *Reviewing Special User Privileges*
- *About Implementing Authorization and Access Control*
- *Implementing Personal Visibility for the User Profile View*
- *About Securing Application Data During Configuration*
- *About Message Broadcasting*
- *About Securing Third-Party Applications*

About Securing Applications

Securing applications requires analysis, monitoring, and testing. Protecting applications is crucial because an attacker who has taken over an application can run commands with the privileges of that application. Often application-to-application security is minimal and privileges are high because these are assumed to be trusted sources. Many applications run with superuser (root) privileges, which increases the risk of serious damage if a vulnerability is exploited.

Web applications are the leading entry for most hackers and have more vulnerabilities than other applications. Web server and application server configurations play a key role in the security of a Web application. These servers are responsible for serving content and calling applications that generate content. In addition, many application servers provide several services that Web applications can use including data storage, directory services, email, messaging, and so on.

Several server-configuration problems can threaten a Web site, for example:

- Server-software configurations that permit directory listing and directory traversal attacks
- Unnecessary default, backup, or sample files including scripts, applications, configuration files and Web pages
- Improper file and directory permissions
- Unnecessary services enabled, including content management and remote administration
- Default accounts and passwords
- Administrative or debugging functions that are enabled or accessible
- Poorly configured TLS certificates and encryption settings
- Use of self-signed certificates to achieve authentication

- Use of default certificates

You can detect many of these problems with security-scanning tools. These configuration problems can compromise a Web application and successful attacks can also result in the compromise of back-end applications, including databases and corporate networks.

A strong Web application is typically deployed on a secure host (server) in a secure network using secure design and deployment guidelines. Because of the dependencies on the network environment, Web application security must be addressed in multiple layers, including securing the network, host, and application.

Guidelines for Deploying Siebel Business Applications

This topic provides guidelines for minimizing security vulnerabilities when deploying Siebel CRM. Consider the following:

- **Verify that the environment in which Siebel CRM is to be deployed is secure.** Verify that the underlying platform (operating system, Web server, and database server) upon which Siebel CRM resides or is connected to has been secured using the respective vendor's security guides and has been checked against your organization's security policy.
- **Do not configure an email relay service or other communications service on any of the computers where Siebel CRM resides.** If email is needed, then permit only outgoing email to notify administrators of any critical events. With applications such as Siebel Email Marketing, configure the Siebel Server to forward the emails to an email relay service on another server in the demilitarized zone, which can forward the emails to the appropriate destination. For additional information, see *Siebel Marketing Installation and Administration Guide* .
- **Enforce a server-management policy.** For example, system administrators log in to servers using their respective personal user IDs and password (with administrative privileges) instead of the default administrator accounts.
- **Delete optional learning aids. For example, delete the sample Siebel database and demo data.** For information on deleting the sample Siebel database, see *Siebel Installation Guide* .
- **Disable or uninstall optional Siebel CRM components that are not required in your environment.** For information, see *About Disabling Siebel Components*.
- **Install application-specific patches.** For additional information on the patches available with Siebel CRM, see *Critical Patch Updates for Siebel CRM*.
- **Store all application-specific files in a directory.** Limit the attack surface to this directory and any subdirectories it contains.
- **Add application-layer authentication.**

About Disabling Siebel Components

Most of the components required to run Siebel CRM are common to all Siebel Business Applications. However, the components that are required in a specific Siebel environment vary according to factors such as the following:

- Whether mobile clients are supported.
- The features provided by the Siebel application, for example, Siebel Sales uses a number of components that are not required by applications such as Oracle's Siebel Marketing or Oracle's Siebel Employee Relationship Management application.

During the Siebel Server configuration process, you specify the components and component groups you want to enable for a Siebel Server. It is not necessary to run all components on all Siebel Servers in an Enterprise. Verify that only the components or component groups you require on each Siebel Server are enabled; disable or unassign component groups that are not required.

The following are some examples of Siebel Server components that do not have to be enabled on all Siebel Servers in an Enterprise:

- **SvrTblCleanup.** The SvrTblCleanup component deletes completed and expired Server Request records for all Siebel Servers in a Siebel Enterprise from the S_SRM_REQUEST table. Enable this component on only one Siebel Server in a Siebel Enterprise.
- **SCBroker**. Disable the SCBroker component on Siebel Servers that host only batch mode components, for example, Workflow components.
- **SRProc.** Disable the Server Request Processor (alias SRProc) component on Siebel Servers that run only Application Object Manager components and that do not run batch mode components.

Components can be disabled using the Siebel Administration - Server screens or the srvrmgr command-line interface. For information on enabling and disabling components, see *Siebel System Administration Guide* .

About User Authentication

Siebel CRM has an open authentication architecture that integrates with your selected authentication infrastructure. Siebel CRM supports the following types of user authentication:

- A database security adapter for database authentication
- An LDAP security adapter for LDAP authentication
- Web Single Sign-On (SSO)
- Custom security adapter

  You can develop a custom security adapter using a security adapter SDK, which allows you to implement authentication using products such as RACF, CA-ACF2 or CA-TopSecret.

It is recommended that you implement LDAP authentication or Web SSO authentication. It is simpler to maintain these methods of authentication and to apply account policies to them. For a comparison of the benefits and disadvantages of the supported authentication mechanisms, see *Security Adapter Authentication*.

Implementing Password Management Policies

It is important to implement a password management policy so that only authorized users can access Siebel CRM. The details of the policy are likely to vary across Siebel implementations, depending on the language and character set in use in a Siebel environment, and depending on the business needs of users. However, a set of rules need to be defined, implemented, and checked each time a new password is created or modified.

Implement the password management recommendations in the following topics:

- *General Password Policies*
- *Defining Rules for Password Syntax*
- *About Configuring Password Hashing for Users*

General Password Policies

Implement the following general password management policies:

- Determine a password expiry period (except for the Siebel administrator).
- Determine the number of password failures allowed before an account is locked.
- Implement password syntax rules. See *Defining Rules for Password Syntax*.
- Implement password hashing. For additional information, see *About Configuring Password Hashing for Users*.
- Change the password of the Siebel administrator account regularly.
  During the Siebel CRM installation process, the Siebel administrator account (SADMIN) is created. You are required to specify a password for this account before you install and configure the Siebel database components. Change the password for the administrator account at regular intervals. For information on this task, see *Changing and Managing Passwords*.
- Change the password for Siebel utilities after installation.

A number of Siebel command-line utilities can be used during the installation and configuration of Siebel CRM, for example:

- srvrmgr
- srvrcfg
- srvredit

When starting any of these utilities, you must specify the Siebel administrator user name and password in the command line as command flags. In a Siebel deployment with high-security requirements, it is recommended that you change the Siebel administrator user name and password used for these utilities after you have completed the Siebel implementation process.

Defining Rules for Password Syntax

To make sure that the passwords in your Siebel deployment are difficult to guess and are capable of withstanding brute-force attacks, define rules for your organization relating to password syntax. It is recommended that you implement password syntax rules similar to the following:

- The password value must not be the same as the user name.
- Password values must include a variety of characters within the supported character set, for example:
  - Both alphabetic and numeric characters are required.
  - A special character is required, such as a symbol, an accented character, or a punctuation mark.
  - At least one uppercase and one lowercase letter is required.
  - Specify illegal values, for example, no more than one space character is permitted, or no more than 2 repetitions of the same character are permitted.
- Password values must be a minimum length, usually 8 characters.

In general, Siebel CRM does not provide support for either implementing password syntax rules or for verifying them. However, the following options exist:

- For the Siebel Mobile Web Client, the following options for managing the passwords of Remote clients are available:
  - Application lockout after a specified number of consecutive, unsuccessful login attempts
  - Password expiration after a defined interval

- Password syntax check
- User password reset by the administrator

For information on setting these options, see *Siebel Remote and Replication Manager Administration Guide* .

- Users who have previously self-registered on a Siebel customer or partner application who forget their passwords can get new passwords by clicking the Forgot Your Password? link in the login dialog box. You can configure the length (maximum and minimum characters) of the passwords generated by your Siebel application for such users. For additional information, see *Defining Password Length for Retrieved Passwords*.

About Configuring Password Hashing for Users

Password hashing is a critical tool for preventing unauthorized users from bypassing Siebel CRM and logging in to the Siebel database directly. It also prevents passwords intercepted over the network from being used to access Siebel CRM, because an intercepted hashed password is itself hashed when a login is attempted, leading to a failed login.

Password hashing is not enabled by default in Siebel CRM. It is recommended that you enable password hashing after installing Siebel if appropriate for your environment.

Password hashing is enabled by setting the value of the Hash User Password parameter to True and hashing each user password using the hashpwd.exe utility. For detailed information on enabling password hashing, see *Configuring User Password Hashing*.

Reviewing Special User Privileges

Within Siebel CRM, special users are defined with specific roles within the application. Data to support these special user accounts is included in the seed data installed with Siebel. You can change special user account names after installation, or delete the relevant seed data for a special user account if you do not need the functionality it provides. Do not, however, disable the Siebel administrator (SADMIN) or guest user accounts. For more information about the defined special users and privileges for Siebel CRM, see *Special Users and Privileges*.

About Implementing Authorization and Access Control

This topic describes the mechanisms that you can use to restrict access to data and Siebel CRM functionality for authenticated users after they have accessed Siebel Business Applications.

Siebel CRM uses two primary access-control mechanisms to determine the privileges or resources that a user is entitled to within Siebel Business Applications:

- **View-level access control.** Manages the functions that a user can access.
- **Record-level access control.** Manages the data items that are visible to each user.

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 a Siebel application a user can access. This access is based on the functions assigned to that user. In Siebel CRM, these functions are called *responsibilities*. Responsibilities define the collection of views to which a user has access. Each user's primary responsibility also controls the user's default screen tab layout and tasks.

You can choose to store users' Siebel responsibilities as roles in a directory attribute instead of in the Siebel database if you are using LDAP or custom security adapters, or if you are using Web SSO authentication.

Record-Level Access Control

Record-level access control assigns permissions to individual data items within an application. This access level allows you to configure a Siebel application so that only authenticated users who need to view particular data records can access that information.

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

Adhere to the following general guidelines when authorizing access to views and records:

- Grant privileges to positions and responsibilities rather than to individual named users, and grant necessary privileges only.
- Limit access to the user profiles and position lists.
  For additional information, see *Implementing Personal Visibility for the User Profile View*.
- Lock accounts after invalid login attempts.

For additional information on view and data access control, see *Configuring Access Control*.

Implementing Personal Visibility for the User Profile View

This topic outlines how to strengthen the security of the User Profile View by enforcing personal access control to the view. This ensures that access to the data in the view is restricted to the user whose person record is associated with the data in the database. To enforce personal access to a view, you must set the Visibility Type of the view to Personal. This task is described in the following procedure.

> **Note:** It is recommended that you set the Visibility Type to Personal for all View applets that contain sensitive information.

To implement personal visibility to the User Profile View

1. Start Siebel Tools.
2. In the Object Explorer, click the View object type.
   The Views list appears.
3. Query for the User Profile Default View view.
4. Confirm that the property settings are set as follows:
   - **Visibility Applet.** Set to User Profile Form Applet.
   - **Visibility Applet Type.** Set to Personal.
5. In the Object Explorer, expand the View object type, select View Web Template, expand the View Web Template object type, and then select the View Web Template Item object type.
6. In the Object List Editor, select the User Profile Form Applet object.
7. Lock the object, then change the property setting to the following:
   Applet Visibility Type. Set to Personal.

8. Navigate to Business Component in the Object Explorer.
9. Query for Employee.
10. Lock the object.
11. In the Object Explorer, expand the Business Component object, then select the BusComp View Mode object.
12. Create a new record with the following property values.

Field	Value
Name	Personal
Owner Type	Person
Visibility Field	Row Id

13. Update the repository and deliver the updates.

For more information on configuring access control, see *Configuring Access Control*.

About Securing Application Data During Configuration

This topic outlines recommendations for securing Siebel CRM data when performing configuration tasks. In addition to applying critical patch updates, encoding relevant data, and implementing secure coding practices, perform the recommendations in the following topics:

- *About Using Web Services*
- *About Defending Data from HTML Injection*
- *About Using External Business Components*
- *About Using HTTP Methods*

About Using Web Services

When creating, implementing, and publishing Web services, implement the WS-Security UserName Token mechanism to pass user credentials (Username and Password) to Web services. Passing the user name and password in the Web service URL is not supported.

Using the WS-Security UserName Token mechanism means that user names and passwords do not have to be passed to Web services in the URL and a session cookie does not have to be passed with the HTTP request. For additional information on the WS-Security UserName Token, see *Integration Platform Technologies: Siebel Enterprise Application Integration* .

When you create an inbound Web service based on a Siebel business service or a Siebel workflow process, make sure that the Web service is secure. Siebel CRM does not verify the security of inbound Web services you create.

> **Note:** Web services exposed by Siebel do not prevent XML entity injection attacks. This must be considered in customization. External entities defined in XML are not resolved and external entity resolution is disabled by default.

About Defending Data from HTML Injection

This topic describes measures you can take to protect Siebel application data from HTML injection attacks.

Displaying HTML Content

Siebel CRM allows you to display HTML content in fields in the user interface. When using Control objects that are field values, you can set the value of the HTML Display Mode property to control how the field value is displayed in the user interface. You can specify the following values for the HTML Display Mode property:

- **EncodeData.** If the field value contains HTML reserved characters, then they are encoded before they are displayed so that the HTML displays as text in the user interface and is not executed as an HTML command. It is recommended that you set the HTML Display Mode property to EncodeData for each Control object to ensure executable statements are not included in Siebel data records.
- **DontEncodeData.** Use this value only when the value of the field is HTML text and you want the HTML to be executed. Selecting this value is not recommended because the HTML text can be the object of malicious interference.
- **FormatData.** This value is used when description or comment fields are in read-only layout. Setting FormatData to TRUE causes data to be formatted in HTML. For further information, see *Siebel Object Types Reference* .

Oracle recommends that you review all Control objects whose HTML Display Mode property is set to either DontEncodeData or FormatData, and consider changing the value of the property to EncodeData. The following SQL commands can be used to return a list of Control objects that have the HTML Display Mode property set to a value of either FormatData or DontEncodeData:

```
SELECT
 HTML_DISPLAY_MODE
FROM
 SIEBEL.S_CONTROL
WHERE
 HTML_DISPLAY_MODE = 'FormatData' OR
 HTML_DISPLAY_MODE = 'DontEncodeData'
```

Review the list of Control objects returned in the query. You cannot change the value of the HTML Display Mode property to EncodeData for all Control objects in one operation from within the Siebel application. The property must be set for each control individually.

If you choose another method of changing the HTML Display Mode property to EncodeData for all the Control objects returned in the query, then consider the consequences carefully before proceeding. It is recommended that you contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance with this task.

Specifying Trusted Server Names

To strengthen your Siebel application and data against attacks, you can specify the name of each of the host servers that are authorized for use with the Siebel application. The following procedure describes how to specify the names of these trusted servers.

To specify the names of trusted servers

1. Start Siebel Tools.
2. In the Object Explorer, select the Application object type.

   The Applications list appears.
3. Query for the name of your Siebel application in the Object List Editor.

For example, for the Siebel Call Center application, query for Siebel Universal Agent.

4. Lock the application object.
5. In the Object Explorer, expand the Application object type, then select the Application User Prop object type.

   The Application User Props list appears.
6. In the Object List Editor, add an application user property for each server used by the Siebel application. For example:

```
Name: AllowedServerNamesUrl0 value:server_name1
Name: AllowedServerNamesUrl1 value:server_name2
```

7. Update and publish all Siebel repository changes and deliver them to the Siebel runtime repository.

About Using External Business Components

External business components are used to access data that resides in a non-Siebel table or view using a Siebel business component. When configuring external business components, you must specify the data source for the external table that contains the data you want to access.

To prevent users having to log in when accessing the external data source, for each data source accessed by an external business component, specify the data source user name and password details using the DSUsername and DSPassword values when configuring the data source named subsystem. The DSUsername and the DSPassword parameters are activated only when using the database security adapter. For information on configuring external business components, see *Integration Platform Technologies: Siebel Enterprise Application Integration* .

About Using HTTP Methods

The HTTP protocol supports a number of methods that are used to specify the operation to be performed on a resource on the Web. Siebel CRM supports the HTTP GET and POST methods only. All other HTTP methods are blocked to maximize the security of your Siebel application. For information on using the HTTP GET and POST methods with Siebel CRM, see *Transports and Interfaces: Siebel Enterprise Application Integration* .

You can allow access to a blocked method for HTTP GET access using the GETEnabledMethods user property. For information about using the GETEnabledMethods user property, see *Configuring Siebel Open UI* .

About Message Broadcasting

Siebel message broadcasting functionality allows Siebel administrators to display important information directly in the message bar of users' screens. The text of a message broadcast can be up to 2,000 characters in length and can contain HTML tags, which are treated as HTML code on the message bar.

Message broadcasting is available for employee applications but not for customer or partner applications. By default, message broadcasting is enabled, although the administrator can enable or disable it. In environments with very high security requirements, it is recommended that message broadcasting be disabled. For information on disabling message broadcasting, see *Siebel Applications Administration Guide* .

About Securing Third-Party Applications

Secure third-party applications by making sure that all the software is updated with the latest software versions and security patches. For additional information on securing third party products, see the vendor-specific documentation.

Implementing Auditing

This topic contains recommendations for implementing auditing in a Siebel CRM deployment so that suspicious activities are detected. It contains the following topics:

- *Operating System Auditing*
- *Database Auditing*
- *Siebel CRM Event Logging*
- *About Siebel Audit Trail*

Operating System Auditing

Implement the following operating system auditing recommendations:

- Use platform-level auditing to audit login and logout events, access to the file system, and failed object access attempts.
- Back up log files and regularly analyze them for signs of suspicious activity.
- Secure log files by using restricted access control lists, and relocate system log files away from their default locations to make sure attackers cannot cover their tracks.

For more information on operating system auditing, see your operating system documentation.

Database Auditing

Implement the following database auditing recommendations:

- Enable Siebel Audit Trail to audit access to specific data fields or objects in the Siebel database. Enabling Siebel Audit Trail produces a log file of all the events that have occurred, which allows the Siebel database administrator to review the events and detect any suspicious activities. For further information, see *About Siebel Audit Trail*.
- You can also implement 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.

For more information on configuring database auditing, see your database vendor documentation.

Siebel CRM Event Logging

Configure event logging for the Siebel Server and server components to monitor the internal operation of Siebel Business Applications. You can specify the type and extent of the information logged for a specific Siebel Server or component event by choosing a log level for the event, for example, you can choose to only log error messages or to log detailed information relating to an event.

The following table shows Siebel Server and component event log levels. The log level determines the amount of information that is written to the log file and the severity of the event logged. For example, if you set the log level to a low number, then only information relating to the most severe events is logged. If you set the log level to a high number, then less severe events are also logged and more information is written to the log for each event.

Event Log Level	Description
0	Fatal events are logged.
1	Error messages and fatal events are logged.
2	Warning messages are logged in addition to error messages and fatal events.
3	Informational messages are written to the log files in addition to all the messages logged for log levels 0-2.
4	Detailed information is written to the log files for all items logged for log levels 1-3.
5	Diagnostic information is written to the log files as well as all the information logged for log levels 1-4.

Implement the following recommendations when configuring event logging:

- Verify that Siebel CRM does not log excessive or sensitive information by default, for example, session IDs.
- In a production environment, do not set event log levels for Siebel Server components to verbose levels; the recommended log levels are 2 (Warnings) or 3 (Informational). Do not log sensitive information at the maximum logging settings.

Event logging is configured using the Siebel Administration - Server Configuration screens or the srvrmgr command-line interface. For detailed information on setting event logging for Siebel Server and server component events, see *Siebel System Monitoring and Diagnostics Guide* .

About Siebel Audit Trail

Siebel Audit Trail creates a history of the changes that have been made to data in Siebel CRM. Audit Trail functionality is enabled in Siebel CRM by default.

Siebel CRM supports various degrees of auditing:

- At the simplest level, each data record contains the following fields, which store the date and time of each change made to the record, and values identifying the user who made the change:
  - CREATED
  - CREATED_BY
  - LAST_UPD
  - LAST_UPD_BY

  With additional configuration, you can generate an activity for additional levels of auditing. This configuration is best used when there are limited needs for auditing, for example, just a few areas to track.

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

- Siebel CRM maintains an audit trail of information that tells when business component fields have been changed, who made the change, and the value of the field before and after the change. 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 the fields.

  You can also configure Siebel Audit Trail to determine the scope of the audit. You can choose to audit all activity, or to limit the scope of auditing to those operations performed by certain responsibilities, positions, or employees.
- Using Siebel Workflow, you can configure workflow processes to save information on changes to specific business components.
- You can also attach scripts to the business component Write_Record event and save information about the transaction.

> **Note:** Be aware that enabling high levels of auditing, for example, log level 5, can have an adverse impact on performance.

Restrict access to the audit records, and archive and delete audit records regularly. For information on configuring and using Siebel Audit Trail, see *Siebel Applications Administration Guide* .

Performing Security Testing

This topic describes how to test the security of your Siebel CRM deployment. It includes the following topics:

- *About Performing Security Assessments*
- *About the Common Vulnerability Scoring System*
- *Using Masked Data for Testing*

About Performing Security Assessments

Carry out security-risk assessments of your Siebel CRM installation and infrastructure (for example, the operating system and third-party products) periodically to make sure that security policies are being adhered to and to rectify any

security vulnerabilities that are identified. In particular, perform extensive security testing of any customizations you make to Siebel CRM before you implement the customizations in a production environment.

It is recommended that you scan your Siebel CRM deployment periodically using vulnerability assessment tools to locate security weaknesses. Use a focused approach for risk mitigation rather than focusing on the identification of every possible attack which can be time-consuming. Various tools are available for performing vulnerability assessments:

- Public domain tools, for example, Nessus, Nmap, COMRaider, FileFuzz, and CIS Tools (www.cisecurity.org).
- Other commercially available tools for which an up-to-date vulnerability database is maintained by the vendors. The following tools are generally available for testing system security:
  - WebInspect
  - NTOSpider

About the Common Vulnerability Scoring System

You can use the Common Vulnerability Scoring System (CVSS) to determine the characteristics and severity of a security vulnerability and to assess its impact on your environment. The CVSS is an open, industry-standard method used to score system vulnerabilities.

In the CVSS, vulnerabilities are assessed on three measures: base properties, temporal properties, and environmental properties. The resultant composite score represents the overall risk posed by the vulnerability in your environment. Using the CVSS can help you determine the severity of vulnerabilities that you find and therefore help determine the priority given to resolving them.

The CVSS is maintained by the Forum of Incident Response and Security Teams (FIRST). For additional information on using the CVSS, go to the FIRST Web site at

http://www.first.org/cvss/

A calculator for scoring vulnerabilities using the CVSS method is available from the National Vulnerability Database Web site at

http://nvd.nist.gov/cvss.cfm

Using Masked Data for Testing

If making a copy of the data in your Siebel production database for security testing or development purposes, then mask sensitive data.

Data masking hides sensitive information by replacing it with similar-looking but nonauthentic data. Effective methods of data masking protect the original data by ensuring it cannot be recovered from the masked data while providing a version of the data that is functionally equivalent for testing purposes. Data, such as personal details and credit card information, must always be masked when used outside the production environment.

Siebel CRM does not provide data masking features; this functionality is provided by the RDBMS vendor. The Oracle Data Masking pack for Oracle Enterprise Manager provides data masking capabilities. If you are using an MS SQL or DB2 RDBMS, then refer to the vendor documentation for information on data masking products.

Methods of Masking Data

When using a copy of production data for testing or development purposes, you have to mask sensitive data but also ensure that the original data is not changed so much in the masking process that it no longer allows a valid test of the functionality being verified.

The most appropriate method of masking data, without substantially changing it, varies according to the type of the data. The following are some methods that can be used for masking different types of data:

- **Numbers, such as credit card numbers and product numbers.** Rotate the numbers in the original data, and add a random value.
- **Dates and times.** Add or subtract a fixed amount of time to the original date or time value. Make sure that the result of the operation is still a valid date or time, and that start dates in the original data still occur before end dates in the original data.
- **Names, such as customer names or personal names.** Replace characters in names in the original data using a fixed or random substitution scheme. Be careful that the substitution does not increase the length of the resultant name values or buffer overflows can occur.
- **Status values, such as Active or Suspended.** Change each of the values to some other value picked from a list of known values. For example, a customer's status can be changed from Active to Suspended, but not to Inactive if the term Inactive is not recognized by the application.

Supported Security Standards

This topic provides information about the way in which Siebel CRM supports the requirements of several security standards. It includes the following topics:

- *Payment Card Industry Data Security Standard*
- *Common Criteria for Information Technology Security Evaluation*
- *Federal Information Processing Standard (FIPS)140*

Payment Card Industry Data Security Standard

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of standards developed to enhance the security of credit card data in organizations that process such data. Developed by the PCI Security Standards Council, the standards are designed to prevent credit card fraud by implementing consistent data-security measures, which include requirements relating to network management, security policies and procedures, and data-access management.

PCI DSS compliance is required of all organizations that store, process, or transmit credit cardholder data. The PCI DSS currently outlines six basic principles for compliance, supported by more detailed subrequirements for compliance.

The following table lists the PCI requirements and the ways in which Siebel CRM supports these requirements.

Note: Siebel CRM and its features do not currently meet certain audit-related PCI DSS 3.1 compliance standards. The following PCI DSS 3.1compliance standard items are not covered by Siebel audit trail:

- System components.
- All actions taken by any individual with root or administrative privilege.
- Invalid logical access attempts.
- Use of and changes to identification and authentication mechanisms (including but not limited to new account creation and privilege elevation) and all changes, additions, or deletions to accounts with root or administrative privileges.

PCI DSS Principle	PCI DSS Requirement	Siebel CRM Support for PCI DSS
Build and maintain a secure network.	Do the following: • Install and maintain a firewall to protect cardholder data. • Do not use vendor-supplied default passwords.	Siebel CRM supports the deployment of firewalls, reverse proxy servers, and Network Address Translation devices to protect application data from intrusion. During the installation of Siebel CRM, warnings are issued if the password specified for the user ID used to start services and processes is the same as the user ID. The installer can use any user ID and password that have the appropriate privileges to perform the task it is required to perform (such as administrator privileges to start services).
Protect cardholder data.	Do the following: • Protect stored cardholder data. • Encrypt transmission of cardholder data across open, public networks.	Siebel CRM allows customers to encrypt sensitive information stored in the Siebel database, cardholder data, and other data transmitted across networks.
Maintain a vulnerability management program.	Do the following: • Use and regularly update antivirus software on all computers commonly affected by malware. • Develop and maintain secure computer systems and applications.	These requirements are customer-governance issues. Oracle recommends that you implement them. For help with security-governance issues, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.
Implement strong access control measures.	Do the following: • Restrict access to cardholder data by business need-to-know. • Assign a unique ID to each person with computer access.	Siebel CRM provides multitiered access-control mechanisms so that only those users with appropriate rights have access to the data. This control includes view-level access control and record-level access control. Each Siebel application user is assigned a login ID, a primary position, and a responsibility in the Siebel application. These security attributes provide the user with the appropriate access rights to the Siebel application.

PCI DSS Principle	PCI DSS Requirement	Siebel CRM Support for PCI DSS
	• Restrict physical access to cardholder data.	Users do not have direct access to the Siebel database; only the Siebel application has access to it. To prevent users from circumventing application-security protocols if database security is used, then Siebel user passwords can be hashed. Enabling password hashing makes sure that the password used to access the Siebel database is not the same password that the user uses to access the Siebel application. In addition, using an LDAP, Single Sign-On, or custom-security adapter to access Siebel CRM requires that user database access is managed through a shared application credential, and not through a user ID and password.
Regularly monitor and test networks.	Do the following: • Track and monitor all access to network resources and cardholder data. • Test security systems and processes regularly.	To maintain data continuity and monitor activity on a Siebel CRM site, you can configure Siebel Audit Trail. This feature allows you to maintain an audit trail of information that indicates when business component fields have been changed, who made the change, and what has been changed. These requirements are customer-governance issues. Oracle recommends that you implement them. For help with security governance concerns, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.
Maintain an information security policy.	Maintain a policy that addresses information security.	This requirement is a customer-governance issue. Oracle recommends that you implement it. For help with security governance concerns, contact your Oracle sales representative for Oracle Advanced Customer Services to request assistance.

Common Criteria for Information Technology Security Evaluation

The Common Criteria for Information Technology Security Evaluation (Common Criteria) is an international technical standard that allows for security evaluations of computer products and technology. By providing an independent evaluation of a product's ability to meet specific security requirements, Common Criteria certification allows purchasers of IP products and technologies to make more informed decisions.

Siebel CRM version 7.8.2 obtained Common Criteria certification in January 2006. The security architecture of subsequent releases of Siebel CRM is unchanged from that release. The Validation Report for Siebel Business Applications Common Criteria certification is available on the Certified Products page of the Common Criteria Web site at

http://www.commoncriteriaportal.org/

For more information on Siebel CRM support for the Common Criteria standard, see 1363489.1 (Article ID) on My Oracle Support.

Federal Information Processing Standard (FIPS) 140

The United States government Federal Information Processing Standard (FIPS) 140 outlines the minimum security requirements for cryptographic modules (both hardware and software) that are used to protect sensitive information.

It is recommended that you verify that the cryptography module used in the applications in your implementation have FIPS 140-1 or FIPS 140-2 certification.

Default Port Allocations

This topic lists the default port allocations used by Siebel CRM. The port allocations that are assigned by default during the installation of Oracle's Siebel Business Applications for the Siebel Server and Siebel Web server are shown in the following table. It is recommended that you change the default ports used by these components.

Note: In a Siebel CRM deployment, DNS servers use User Datagram Protocol (UDP) port 53 and Kerberos defaults to port 88.

Siebel Component	Port Number	Comments
Web Server	80 and 443	Port 80 is used for standard Web traffic. If encryption is implemented, then port 443 is used.
Gateway	2320	Load-balancing components use port 2320.
Siebel Server	2321	SCBroker listens on port 2321. For information on SCBroker, see *Siebel System Administration Guide* and *Siebel Deployment Planning Guide* .
Siebel Server	49150 and higher (dynamic allocation of ports) 49149 and lower (static allocation of ports) 49152 to 49250 (dynamic ports listening on Siebel Servers)	Siebel CRM uses dynamic allocation of ports for the server-based components. Static port allocation is also supported. The dynamic port allocation starts from port number 49150 onwards. If you choose to assign static ports to the components, then make sure that you choose ports less than port number 49150. Dynamic ports can go up to port number 65535. These ports have to be opened on Siebel Servers. The system administrator allocates a port to a specific Siebel component.
Synchronization Manager	40400	None.
Enterprise Application Integration (EAI) Server	Allocated by the system administrator.	None.

Siebel Component	Port Number	Comments
SMTP Mail Server	25	None.
FTP Port	21	Ports must be opened for the Siebel EAI and Workflow components. The system administrator allocates these ports.
Lightweight Directory Access Protocol (LDAP) Server	389 and 636	None.
Siebel Server or Siebel database	1521	Port 1521 is used for communications between the Siebel Server and Oracle database.
Siebel Server or Siebel database	1433	Port 1433 is used for communications between the Siebel Server and Microsoft SQL Server database.
Siebel Server or Siebel database	5000	Port 5000 is used for communications between the Siebel Server and IBM DB2 database for Linux, UNIX, and Windows.
File Server	139 Transmission Control Protocol (TCP) 137 and 138 User Datagram Protocol (UDP)	Port numbers for communications between the Siebel Server and the Siebel File System and Database Server are dependent on the file system type. The default TCP port number is 139. The default User Datagram Protocol (UDP) port numbers are 137 and 138.
Search Server	2048	None.