



Siebel eBusiness Applications 安全指南

版本 7.7
2004 年 3 月

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

版权所有 © 2004 Siebel Systems, Inc.

保留所有权利。

美国印制

未与 Siebel Systems, Inc. 预先达成协议或获得书面许可，不得以任何方式复制、传播或在检索系统中存储本出版物的任何部分，包括但不限于影印、摄影、磁性介质或其它记录。

Siebel、Siebel 徽标、TrickleSync、Universal Agent 和此处引用的其它 Siebel 名称均是 Siebel Systems, Inc. 的商标，并且可能在某些管辖区内注册。

其他产品名称、称号、徽标和符号可能是其各自所有者的商标或注册商标。

产品模块和选项。本指南包含对可选模块以及您可能尚未购买许可证的模块的说明。Siebel 的“示例”数据库还包含与这些可选模块相关的数据。因此，您的软件实施可能与本指南中的说明有所不同。要了解关于您所在组织已购买的模块的更多信息，请向您的公司采购员或您的 Siebel 销售代表咨询。

美国政府限制权利。根据《美国联邦购买条例国防补充规定》所发布的“程序”、“辅助程序”和“文档”均为商用计算机软件（如 DFARS 227.7202 所述之“商用计算机软件”、“商用计算机软件文档”及此类物品），以任何方式使用、复制、公开此“程序”、“辅助程序”和“文档”应受制于适用 Siebel 许可协议中相关内容约束。美国政府对此类“程序”、“辅助程序”和“文档”的所有其它使用、复制和公开应受制于适用的 Siebel 许可协议和以下法律文件中相关内容的约束：FAR 52.227-19 中“商用计算机软件 — 有限权利（1987 年 6 月）”子章节、FAR 52.227-14 中“数据权利 — 诸论”，如有必要，还应包括 Alternate III（1987 年 6 月）。合约商/许可人为 Siebel Systems, Inc., 2207 Bridgepointe Parkway, San Mateo, CA 94404。

所有权信息

Siebel Systems, Inc. 将本文档及 Siebel eBusiness Applications 在线帮助中包括的信息视为保密信息。您对此类保密信息的访问和使用受以下文档中的条款和条件约束：(1) 已执行或您同意遵循的适用的 Siebel Systems 软件许可协议，以及 (2) 本文档中包含的所有权和限制权利通告。

目录

第 1 章：本版本的最新资讯

第 2 章：关于 Siebel 应用程序的安全性

整体安全概念 15

行业的安全标准 16

Siebel 安全体系结构 17

用于安全系统访问的用户验证 17

安全适配器 SDK 19

用于数据保密性的端对端加密 20

控制数据访问 21

数据连续性审计 22

用于防止入侵的安全物理部署 23

移动解决方案的安全性 23

Web 浏览器的安全设置 24

安全性参考的书目 24

配置安全性的指示 25

第 3 章：更改或添加口令

更改缺省口令 27

在 Microsoft Windows 上更改系统管理员口令 28

在 UNIX 上更改 Siebel 管理员口令 29

更改表所有者 (DBO) 口令 30

有关更改口令的疑难解答，请检查失败的服务器任务 31

添加用于更新 Web 服务器静态文件的口令 32

管理 eapps.cfg 文件中的加密口令 33

第 4 章：物理部署和审计

关于 Siebel 网络 35

防火墙和代理服务器支持 37

Siebel 服务器负载平衡在网络安全性方面的角色 39

端口号 39

限制访问	40
数据连续性审计	41
保护 Siebel 报表服务器	42
Siebel 报表服务器组件	42
为提高安全性配置 Siebel 报表服务器	42
保护 Siebel 文档服务器	43

第 5 章：通讯和数据加密

加密类型	45
配置安全通讯	48
为 Siebel Enterprise 和 SWSE 配置加密	48
为 Siebel Enterprise 或 Siebel 服务器配置 SSL 加密	49
为 SWSE 配置 SSL 加密	52
为 Web 客户机配置加密	54
为移动 Web 客户机同步配置加密	55
配置数据加密	57
使用密钥数据库管理器	58
数据加密的升级问题	61
配置业务组件加密	62
Unicode 支持的安全注意事项	64

第 6 章：安全适配器验证

关于用户验证	65
验证策略的比较	66
关于 Siebel 安全适配器	67
配置数据库验证	68
关于 LDAP/ADSI 安全适配器验证	69
LDAP/ADSI 验证流程	70
LDAP/ADS 目录的要求	70
安装 LDAP Client 软件	72
使用 SSL 的安全 LDAP 的考虑事项	73
在 Windows 上安装 IBM LDAP Client 和 GSKit	73
在 Solaris 上安装 IBM LDAP Client 和 GSKit	76
在 AIX 上安装 IBM LDAP Client 和 GSKit	80
在 HP-UX 上安装 IBM LDAP Client 和 GSKit	83
安装和配置 IBM GSK iKeyMan	87
使用 IBM GSK iKeyMan 生成 CMS 文件	88

实施 LDAP/ADSI 安全适配器验证	90
使用 LDAP/ADSI 配置实用程序	91
关于专用 Web 客户机的配置	93
配置 LDAP/ADSI 安全适配器的过程	93
设置安全适配器验证：方案	97
创建数据库登录	98
设置 LDAP/ADS 目录	98
在 LDAP/ADS 目录中创建用户	99
在 Siebel 数据库中添加用户记录	100
编辑 eapps.cfg 文件中的参数	101
使用 Siebel Server Manager 编辑参数	101
编辑应用程序配置文件中的参数	105
设置专用 Web 客户机的系统首选项	106
重新启动服务器	106
测试 LDAP/ADSI 验证系统	106
配置口令散列处理	109
口令散列处理的登录方案	110
口令散列处理的使用准则	110
配置用户口令和证书口令散列处理	111
运行口令散列处理实用程序	112
安全适配器部署选项	113
配置应用程序用户	114
配置 Checksum 验证	115
配置安全适配器的安全通讯	116
配置共享数据库帐户	116
配置适配器定义的用户名	117
配置匿名用户	118
配置在目录中定义的角色	119
安全适配器和 Siebel 专用 Web 客户机	120
移动 Web 客户机同步的验证	122

第 7 章：Web 单一登录验证

关于 Web 单一登录	125
实施 Web SSO 验证	126
设置 Web SSO：方案	127
实施 Web SSO 的流程	128
创建被保护的虚拟目录	128
创建数据库登录	130
设置 Active Directory Server	130

在目录中创建用户	131
在 Siebel 数据库中添加用户记录	132
编辑 eapps.cfg 文件中的参数	133
编辑名称服务器参数	134
编辑应用程序配置文件中的参数	135
重新启动服务器	136
测试 Web SSO 验证	136
数字认证验证	137
用户身份的来源	138

第 8 章：Siebel Web Server Extension 的安全功能

配置安全视图	139
登录功能	140
Cookie 和 Siebel 应用程序	143
会话 Cookie	144
自动登录证书 Cookie	145
Siebel QuickStart Cookie	145
为 Siebel 应用程序启用 Cookie	146

第 9 章：用户管理

关于用户注册	147
配置匿名浏览	148
关于匿名浏览和未注册的用户	148
实施匿名浏览	148
为匿名浏览或显式登录配置视图	149
关于自行注册	150
实施自行注册	152
修改匿名用户记录	152
为自行注册设置配置参数	153
激活自行注册的工作流程过程	153
修改自行注册视图和工作流程	154
管理重复的用户	158
管理“忘记口令”	161
忘记口令的用户体验	161
忘记口令的体系结构	162
修改“忘记口令”工作流程过程	163
修改工作流程过程以查询 NULL 字段	163
修改工作流程过程以请求其它标识数据	164

用户的内部管理	166
将用户添加到 Siebel 数据库中	167
添加新雇员	167
添加新的合作者用户	169
添加新的联系人用户	169
将联系人提升为联系人用户	171
用户记录的“新职责”字段	171
用户的授权管理	172
授权管理的用户验证要求	172
授权管理的访问注意事项	172
注册联系人用户 — 授权管理	173
注册合作者用户 — 授权管理	174
维护用户资料	176
编辑个人信息	176
更改口令	176
更改活动职位	177

第 10 章：配置访问控制

关于访问控制	179
当事方的访问控制	181
数据的访问控制	183
访问控制机制	185
关于个人访问控制	185
关于职位访问控制	186
关于单一职位访问控制	186
关于团队（多职位）访问控制	187
关于经理访问控制	187
关于组织访问控制	188
关于单一组织和多组织访问控制	189
关于子组织访问控制	190
关于全部访问控制	191
关于访问组访问控制	191
对访问控制的计划	192
访问控制和业务环境结构	192
对部门的计划	194
对组织的计划	194
对职位的计划	195
对职责的计划	196

实施访问控制	197
应用程序和访问控制	197
设置部门、组织和职位	198
职责和访问控制	200
业务组件视图模式	203
业务组件视图模式字段	204
子视图访问控制属性	206
视图访问控制属性	208
灵活构建视图示例	211
实施访问组访问控制	212
应用访问组访问控制的方案	213
用户的体验	216
管理任务	218
管理数据目录	218
管理职位、组织、家庭和用户列表	218
管理访问组	220
将访问组与数据关联	222
通过职责管理选项卡布局	224
管理选项卡布局	224
分配主要职责	225
导出和导入选项卡布局	225
通过职责管理任务	226
清除高速缓存的职责	227
附加访问控制机制	227
配置弹出式子视图和选择子视图的可视性	227
配置向下搜索	229
当事方数据模型	230
当事方如何相互关联	231
人员（联系人）数据模型	232
用户数据模型	233
雇员数据模型	234
职位数据模型	235
客户数据模型	236
部门数据模型	237
组织数据模型	238
合作者组织数据模型	239
家庭数据模型	240
用户列表数据模型	241
访问组数据模型	242

附录 A：安全问题疑难解答

用户验证问题 243

用户注册问题 244

访问控制问题 246

附录 B：与验证有关的配置参数

eapps.cfg 文件中的参数 247

Siebel 网关名称服务器参数 251

Siebel 应用程序配置文件参数 256

系统首选项 260

附录 C：Seed 数据

Seed 雇员 261

Seed 用户 262

Seed 职责 262

Seed 职位和组织 263

Seed 数据库登录 263

附录 D：Siebel Financial Services 的附录

Siebel Financial Services 应用程序 265

Siebel Financial Services 的用户验证 266

注册和管理 Siebel Financial Services 的用户 268

Seed 数据 268

未注册的用户和匿名浏览 269

自行注册 269

内部管理用户 270

用户的外部管理 270

维护用户资料 270

Siebel Financial Services 的基本访问控制 271

访问控制机制 271

管理访问组访问控制 271

Siebel Financial Services 应用程序的配置文件名 273

Siebel Financial Services 的 seed 数据 274

Seed 用户 274

Seed 职责 275

索引

1

本版本的最新资讯

Siebel eBusiness Applications 安全指南，版本 7.7 中的最新资讯

第 11 页的表 1 列出本版本文档中描述的为支持 7.7 版软件所作的更改。

表 1. Siebel eBusiness Applications 安全指南，版本 7.7 中的新产品功能

主题	说明
第 33 页的“管理 eapps.cfg 文件中的加密口令”	存储在 eapps.cfg 文件中的口令现在已被加密。您可以使用 encryptstring.exe 实用程序手动为此类口令加密。
第 37 页的“防火墙和代理服务器支持”	Siebel 高交互应用程序现在可以支持反向代理 Web 服务器配置。
第 39 页的“Siebel 服务器负载均衡在网络安全性方面的角色”	Siebel 服务器可以使用 Siebel 负载均衡或第三方负载均衡器来平衡 Siebel 服务器的负载。 另请参阅 <i>部署计划指南</i> 。
第 39 页的“端口号”	应用程序对象管理器 (AOM) 现在使用静态端口。
第 48 页的“配置安全通讯”	SSL 配置实用程序（适用于 SISNAPI）现在与 Siebel 软件配置实用程序（适用于 Enterprise 或 SWSE）相集成。它还可以作为一个独立实用程序运行。
第 57 页的“配置数据加密”	Siebel Strong Encryption Pack 现在包括三个级别的 AES 数据加密：128 位、192 位和 256 位。系统支持三个升级方案以获得更高级别的数据加密。 “密钥数据库管理器”实用程序现在支持 AES 加密。业务组件字段配置现在支持通过“AES 加密器”业务服务执行的 AES 加密。 杂乱算法已从内部代码引用中删除。
第 6 章“安全适配器验证”	安全适配器的参数已从配置文件移到 Siebel 网关名称服务器，并且通过 Siebel Server Manager 进行配置。（配置文件仍然用于移动和专用 Web 客户机。） 安全适配器和验证管理器不再是 AOM 的一部分，安全适配器被定义为企业资料（指定子系统）。 数据库验证现在使用安全适配器结构（数据库安全适配器是缺省值）。 以前版本中与安全相关的一些配置参数和系统首选项现在已经废弃。
第 72 页的“安装 LDAP Client 软件”	现在部署任何 LDAP 安全适配器要求安装 Siebel Systems 提供的 IBM LDAP 客户机软件。
第 91 页的“使用 LDAP/ADSI 配置实用程序”	LDAP/ADSI 配置实用程序已得到增强。

表 1. Siebel eBusiness Applications 安全指南, 版本 7.7 中的新产品功能

主题	说明
第 109 页的“配置口令散列处理”	<p>现在可以通过安全适配器配置和执行口令散列处理（适用于用户或证书）。</p> <p>hashpwd.exe 实用程序替换了 encrypt.exe，并且提供 RSA SHA-1 散列算法支持。客户可以将口令转移到 RSA SHA-1 算法。（现有客户仍然可以使用以前的杂乱算法。）</p>
第 114 页的“配置应用程序用户”	<p>如果使用 LDAP/ADSI 安全适配器，该应用程序用户不再可选。</p>
第 122 页的“移动 Web 客户机同步的验证”	<p>使用同步管理器的移动 Web 客户机同步现在可以根据需要使用安全适配器验证。</p> <p>适用于移动 Web 客户机的数据库验证选项现在使用数据库安全适配器。</p> <p>另请参阅 <i>Siebel Remote and Replication Manager Administration Guide</i>。</p>
第 7 章 “Web 单一登录验证”	<p>Microsoft Windows 集成身份验证现在可以部署为 Web 单一登录 (Web SSO) 的备选项。</p>
第 143 页的“Cookie 和 Siebel 应用程序”	<p>eapps.cfg 文件中用于会话跟踪和 cookie 管理的配置参数现在已被修改。</p>
第 189 页的“关于单一组织和多组织访问控制”	<p>现在可以为多组织可视性配置值列表。</p>
第 224 页的“通过职责管理选项卡布局”	<p>现在可以通过职责配置缺省的选项卡布局 and 任务。（选项卡布局功能已在 7.5.3 版添加。）</p>
第 226 页的“通过职责管理任务”	<p>您可以将视图指定为对与其关联的职责只读。</p>
第 227 页的“清除高速缓存的职责”	<p>管理员可以清除高速缓存的职责。</p> <p>角色（Siebel 应用程序功能）现在已废弃。角色的功能现在已包括在职责中。</p>

本手册中未介绍的 7.7 版与安全相关的更改

7.7 版与安全相关的以下更改未包括在 *Siebel eBusiness Applications 安全指南*。这些更改在 *Siebel Bookshelf* 中的其它书籍中有介绍。

- **本地数据库口令管理和本地数据库加密。** 移动用户现在可以更改自己的本地数据库口令，此更改独立于与 Siebel Remote 服务器同步时使用的口令。本地数据库口令现在可以通过 RSA SHA-1 算法进行散列处理。

移动用户的本地数据库现在可以通过 SQL Anywhere 的标准 Sybase 加密进行加密。

有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

- **用于电子邮件集成的 SSL。** 现在可以使用 SSL 与电子邮件服务器进行通讯。

有关详细信息，请参阅 *Siebel Communications Server 管理指南*。

- **NULL 口令警告。** Siebel Enterprise Server 配置现在要求用户指定口令，不允许使用 NULL 口令。

有关详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

- **支持用于 Web 服务的 UserNameToken。** Siebel EAI 现在支持 UserNameToken 元素，这是一个包括在 WS-Security 规范中的安全机制。此功能允许 Siebel 应用程序以符合标准的方式，通过 Web 服务发送和接收证书。

有关详细信息，请参阅 *Integration Platform Technologies: Siebel eBusiness Application Integration Volume II*。

2

关于 Siebel 应用程序的安全性

本章概括地介绍了 Siebel eBusiness Applications 的可用安全资源以及如何配置安全性的信息。它包含以下主题：

- 第 15 页的“整体安全概念”
- 第 16 页的“行业的安全标准”
- 第 17 页的“Siebel 安全体系结构”
- 第 24 页的“安全性参考的书目”
- 第 25 页的“配置安全性的指示”

整体安全概念

在评估组织的安全需要以及评估安全产品和政策时，负责安全的经理必须系统地确定安全要求，并且制定满足这些要求的相应方法。

要制定有效的安全计划，经理必须考虑以下事项：

- 哪些类型的行为或安全攻击可以对组织所拥有的信息安全构成威胁？
- 哪些机制可用于检测、防止出现安全漏洞或从安全漏洞恢复？
- 哪些服务可用于增强组织中数据处理系统和信息传输的安全性？

安全服务的分类包括：

- **保密性。**保密性确保只有适当的当事方才有权读取所存储和传输的信息。
- **验证。**验证确保正确地识别消息或电子文档的来源，以保证身份正确。
- **完整性。**完整性确保只有授权的当事方才可以修改计算机系统资产和传输的信息。
- **认可。**认可要求消息的发送方和接收方都不能拒绝传输信息。
- **访问控制。**访问控制要求对信息资源的访问权限可以由目标系统控制。

本指南介绍了可通过 Siebel 网络提供的安全服务。提供这些服务是为了反击安全攻击，并且采用一种或多种安全机制来提供此类服务。

行业的安全标准

Siebel eBusiness Applications 严格遵守公共安全标准，以促进将其应用程序集成到客户环境中。Siebel Systems 不是特定安全组件的供应商，然而，Siebel Systems 将 Siebel 应用程序设计为让客户可以选择一个最能满足其特定业务需要的安全基础设施。

注释：有关所支持或通过验证可以与 Siebel eBusiness Applications 一起使用的第三方产品的详细信息，请参阅 Siebel SupportWeb 上的[系统要求和支持的平台](#)。

支持的标准包括：

- **LDAP/ADSI。** Siebel Systems 提供了与轻型目录访问协议 (LDAP) 和活动目录服务接口 (ADSI) 的预配置集成，以便对用户进行验证。有关详细信息，请参阅第 19 页的[“适用于 LDAP/ADSI 验证的安全适配器”](#)和第 6 章[“安全适配器验证”](#)。
- **SSL 加密和验证。** 使用所支持的 Web 服务器的安全套接层 (SSL) 功能，对 Siebel eBusiness Applications 组件（即 Siebel 服务器和 Web 服务器）之间的通讯提供的保护。有关详细信息，请参阅第 48 页的[“配置安全通讯”](#)。

Siebel 服务器与目录服务器之间的通讯可以使用 SSL。有关详细信息，请参阅第 116 页的[“配置安全适配器的安全通讯”](#)。

Siebel 服务器与电子邮件服务器之间的通讯可以使用 SSL。有关详细信息，请参阅 *Siebel Communications Server 管理指南*。
- **X.509 认证。** Siebel 应用程序使用所支持的 Web 服务器的 SSL 功能，根据 X.509 客户机认证启用验证。有关详细信息，请参阅第 137 页的[“数字认证验证”](#)。
- **RSA SHA-1 口令散列处理。** Siebel 用户口令可以使用 RSA SHA-1 算法进行散列处理。有关详细信息，请参阅第 109 页的[“配置口令散列处理”](#)。
- **RSA 通讯加密。** Siebel 组件之间的通讯可以使用 RSA 加密算法进行加密。有关详细信息，请参阅第 48 页的[“配置安全通讯”](#)。
 - 对于所支持的 UNIX 平台、Windows 平台或交叉平台环境，Siebel Systems 支持 RSA Bsafe。RSA Bsafe 通过 FIPS 140-1 认证。
 - 对于所支持的 Windows 平台，Siebel Systems 支持 Microsoft Crypto。（如果将 Siebel 服务器和 Web 服务器安装在运行 Microsoft Windows 的同一台机器上，您则不能使用 Microsoft Crypto。只有在运行 Microsoft Windows 的不同机器上运行这些组件时，才能使用 Microsoft Crypto。）
- **AES 和 RC2 数据加密。** Siebel 数据可以使用高级加密标准 (AES) 或 RC2 进行加密。AES 和 RC2 支持多种密钥长度。如果加密长度超过 56 位 RC2，您必须安装 Siebel Strong Encryption Pack。有关详细信息，请参阅第 57 页的[“配置数据加密”](#)。

为了增强 Siebel 应用程序部署的安全性，Siebel Systems 已经与其他行业领先的安全供应商结成联盟。这些供应商已作为安全软件合作者列在 Siebel Web 页的[“联盟”](#)部分。

Siebel 安全体系结构

Siebel 安全体系结构的组件包括：

- 用于安全系统访问的用户验证
- 用于数据保密性的端对端加密
- 用于适当数据可视性的验证
- 用于数据连续性的审计追踪
- 用于防止入侵的安全物理部署
- 移动设备的安全性
- Web 浏览器的安全设置

用于安全系统访问的用户验证

Siebel Systems 开发了一个开放式验证体系结构，它与客户选择的验证基础设施相集成。有关详细信息，请参阅第 6 章“安全适配器验证”和第 7 章“Web 单一登录验证”。

Siebel Systems 支持以下三个用户验证类型：

- Siebel 提供的数据库安全适配器，适用于数据库验证
- Siebel 提供的 LDAP 或 ADSI 安全适配器，适用于 LDAP/ADSI 验证
- Web 单一登录 (Web SSO)

客户还可以使用安全适配器 SDK 开发定制的安全适配器。

无论用户是从 LAN、WAN 还是远程访问 Siebel 应用程序，这些验证机制都适用。第 18 页的图 1 显示了 Siebel 站点内三个主要用户验证类型的逻辑视图。

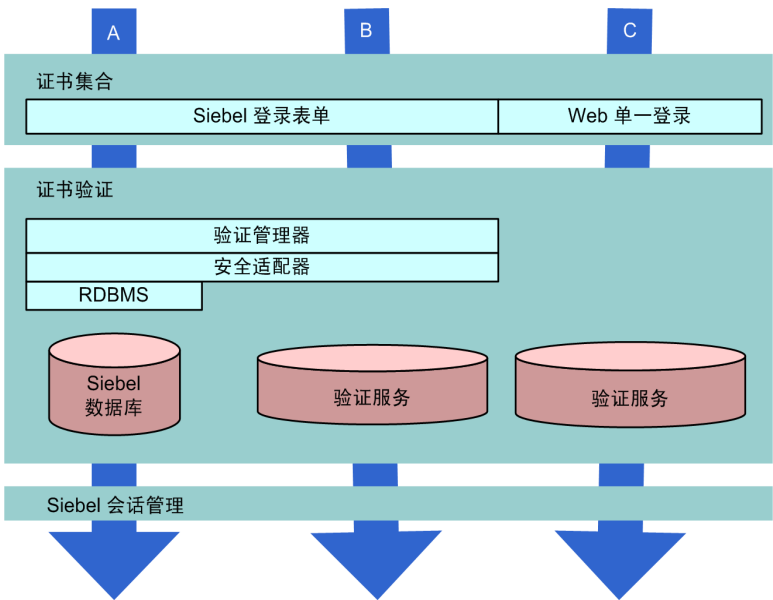


图 1. Siebel 站点内用户验证方法的逻辑图表

适用于数据库验证的安全适配器

Siebel Systems 提供了一个用于收集和验证证书的数据库安全适配器机制。缺省的登录表单用于收集 Siebel 用户名和口令证书。安全适配器用于与数据库的基本安全系统配合使用，共同对用户的证书进行验证。

通过数据库验证之后，每位用户必须具备有效的数据库帐户，才能访问 Siebel 应用程序。数据库管理员 (DBA) 必须添加所有的用户数据库帐户。数据库验证部署支持口令散列处理，以防止遭受黑客攻击。

任何 Siebel 应用程序都可以使用数据库验证，此验证被配置为缺省值。然而，Siebel Systems 提供的一些功能，例如支持用户自行注册的工作流程过程或忘记口令时获取口令的方案（客户应用程序中的通用功能），要求使用 LDAP 或 ADSI 安全适配器验证。因此，数据库验证很少用于客户应用程序。

注释： Siebel 用户名和口令的准确而有效的字符集取决于基本验证系统。有关数据库验证的信息，请参阅 RDBMS 供应商的文档。

适用于 LDAP/ADSI 验证的安全适配器

对于雇员或客户应用程序，Siebel Systems 包括预配置的安全适配器接口，以允许组织外化 LDAP 或 ADS 目录中的证书验证。接口与安全适配器连接，其中包含针对特定的验证服务对证书进行验证的逻辑。

注释： Siebel 用户名和口令的准确而有效的字符集取决于基本验证系统。如果是 LDAP/ADSI 验证，请参阅供应商的文档，例如以下列出的某个文档。

因此，Siebel Systems 客户可以使用轻型目录访问协议 (LDAP) 或活动目录服务接口 (ADSI) 等安全标准对用户证书进行验证。

Siebel Systems 还开发了适用于领先验证服务的安全适配器：

- LDAP 安全适配器集成当前通过认证，并获得 IBM Directory Server、Novell NDS eDirectory 和 Sun ONE Directory Server 的支持。
- ADSI 安全适配器集成通过认证，并获得 Microsoft Active Directory 的支持。

有关支持的附加安全供应商的信息，请参阅第 19 页的“安全适配器 SDK”。

Web 单一登录

Siebel Systems 向客户提供了跨多个 Web 应用程序启用单一登录的功能 — 也称为 Web 单一登录 (SSO)。Siebel Systems 提供了一个可配置机制以实现与 Web SSO 基础设施的通讯、识别用户以及让用户登录到 Siebel 应用程序。

通过 Web SSO，可以独立于 Siebel 应用程序对用户进行验证，例如，可以通过第三方验证服务或 Web 服务器进行验证。

注释： Siebel 用户名的准确而有效的字符集取决于基本验证系统。有关 Web SSO 的信息，请参阅供应商的文档。

Siebel Systems 已经与行业领先的 Web SSO 集成安全供应商结成联盟。这些供应商已作为安全软件合作者列在 Siebel Web 页的“联盟”部分。

安全适配器 SDK

Siebel Systems 提供了 Siebel 安全适配器软件开发人员套件 (SDK)，以允许公司构建附加的安全适配器。此类附加适配器可以支持其它的验证技术，例如，数字认证、生物识别或智能卡。

例如，您可以为 RSA Secure ID token 等设备（一种便携式设备，用于向用户提供一分钟后会发生变化的密钥）创建一个安全适配器。在为该设备部署安全适配器时，用户只有同时提供了当前显示的密钥以及用户的口令或其它证书，才能获得对 Siebel 应用程序的访问权限。

安全适配器接口对于 Siebel 体系结构至关重要，这是因为对于大多数 Siebel Systems 客户来说，验证已经成为一项企业决策，而不是特定于应用程序的决策。验证服务可以是 Siebel Enterprise 中的共享资源，从而实现用户的集中管理。

从 7.7 版开始，基本 SDK 以 IBM SDK（而不是 Netscape SDK）为基础。

Siebel 安全适配器 SDK 在 Siebel SupportWeb 上的 *Siebel 安全适配器软件开发人员套件 7* 中有介绍。

用于数据保密性的端对端加密

存储的数据可以在字段级别有选择地进行加密，并且可以对该数据的访问权限加以保护。此外，此类数据还可以转换为加密形式，以便通过网络进行传输。通讯加密可以保护此类数据不被擅自访问。传输的数据必须得到保护，以避免遭受入侵技术（例如，嗅探程序）攻击，入侵技术是指可捕获数据并监控网络活动的技术。

端对端加密在整个数据路径中提供数据的保密性：从客户机浏览器到 Web 服务器，再到 Siebel 服务器，然后到数据库，最后返回。第 20 页的图 2 显示了可用于 Siebel 环境中通讯的加密类型。

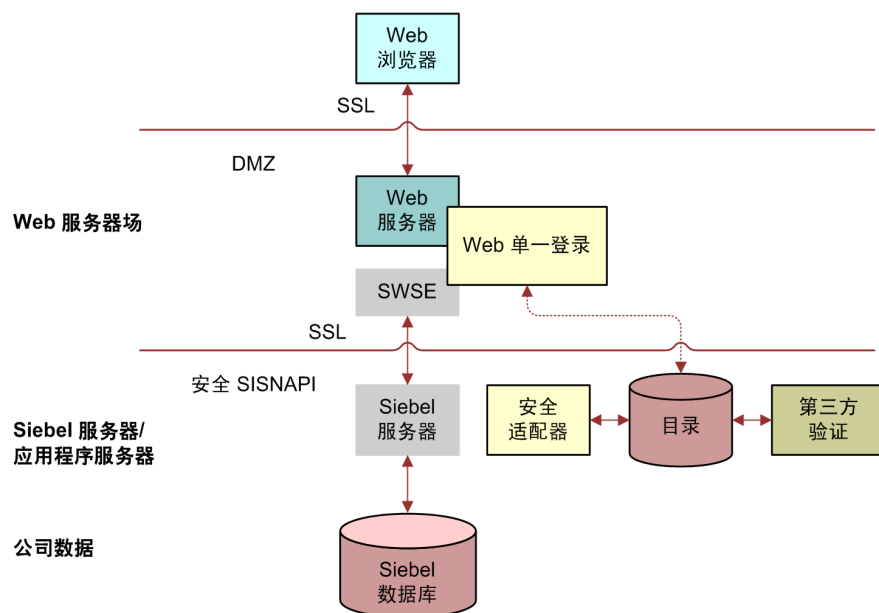


图 2. Siebel 环境中的通讯加密

客户机浏览器到 Web 服务器

Siebel 应用程序使用 Siebel Web 客户机在标准 Web 浏览器中运行。在用户访问 Siebel 应用程序时，系统将通过浏览器与 Siebel 服务器之间的 Web 服务器在两者之间建立一个 Web 会话。安全套接层 (SSL) 用于在传输敏感数据时防止会话被劫持。Siebel 应用程序支持 128 位 SSL 数据加密，这是一个特别安全的 Internet 通讯保护级别。

使用 SSL 的客户可以配置在下列方案中 Siebel 应用程序中的哪些 Web 页（称为视图）将使用 SSL：

- 只在登录视图使用 SSL 以保护口令传输。请参阅第 140 页的“登录功能”。
- 将 SSL 用于附加的特定视图（只能用于标准交互应用程序的选项）。请参阅第 139 页的“配置安全视图”。
- 将 SSL 用于整个应用程序。请参阅第 139 页的“配置安全视图”。

Web 服务器到 Siebel 服务器

Siebel 软件组件使用 Siebel 基于 TCP/IP 的协议通过网络进行通讯，该协议称为 SISNAPI（Siebel Internet 会话 API）。客户可以选择使用安全套接层 (SSL) 或者 RSA 或 Microsoft Crypto API 的嵌入式加密对 SISNAPI 加以保护。这些技术使数据可以在 Web 服务器与 Siebel 服务器之间安全地进行传输。

有关详细信息，请参阅第 48 页的“配置安全通讯”。

Siebel 服务器到数据库

为了保护数据库与 Siebel 服务器之间的传输，您可以使用特定于客户所使用数据库的独有的安全协议对数据进行加密。

数据库存储

Siebel 应用程序允许客户对数据库中存储的敏感信息进行加密，以避免在未访问 Siebel 应用程序时查看这些信息。客户可以配置 Siebel 软件，以便在将数据写入到数据库之前先对数据字段加密，然后在检索相同数据时再对数据解密。这样可以防止试图直接从数据库中查看敏感数据。Siebel 应用程序支持使用 AES 和 RC2 算法对数据进行加密。

有关详细信息，请参阅第 57 页的“配置数据加密”。

控制数据访问

授权是指用户在 Siebel 应用程序中享有的权限或资源。即使在验证的用户当中，组织总是希望限制系统数据的可视性。Siebel 应用程序使用两种主要的访问控制机制：

- 视图级别访问控制，用于管理用户可以访问哪些应用程序功能。
- 记录级别访问控制，用于管理每位用户可以看到哪些数据项。

访问控制向 Siebel 客户提供了统一的管理，用于管理数百万个用户对数百万个内容项的访问。

有关详细信息，请参阅第 10 章“配置访问控制”。

视图级别访问控制

组织通常围绕功能进行排列，并且具有要分配一个或多个功能的雇员。视图级别访问控制确定用户可以根据为其分配的功能访问 Siebel 应用程序的哪些部分。在 Siebel 应用程序中，这些功能称为**职责**。

职责定义了用户有权访问的视图集合。分配了一个职责的雇员可能无权访问与另一个职责集关联的 Siebel 应用程序部分。例如，通常系统管理员有能力查看和管理用户资料，而其他雇员则没有此能力。

每位用户的主要职责还控制用户的缺省屏幕选项卡布局 and 任务。

记录级别访问控制

记录级别访问控制将权限分配给应用程序中的单个数据项，从而允许 Siebel 客户仅为那些需要查看特定数据记录的已验证的用户授予访问信息的权限。

Siebel 应用程序使用三种记录级别的访问权限：职位、组织和访问组。在将特定职位、组织或访问组分配给数据记录时，只有该职位、组织或访问组中的雇员可以查看此记录。

- 职位代表的是组织结构中的位置，与职称非常类似。通常，单个雇员担任一个职位；然而可能有多个雇员共同担任一个职位。职位访问权限允许 Siebel 客户将用户分类，以便可以将这些用户之间的结构用于对数据的访问。

例如，主管可能有权访问其下属具有访问权限的许多数据；这一点同样适用于同一位经理的其他下属。

- 同样，组织（例如，代理的分支机构或公司的部门）是一组映射至公司实际结构的职位。分配给某个组织中某个职位的那些雇员被授予对已分配给该组织的数据的访问权限。您可以设置数据的可视性，以限制雇员访问自己组织之外的数据。
- 访问组是结构较少的用户或用户组集合，例如一个任务组。用户组可以基于用户的一些共同属性，也可以特别进行创建，以将不同组织的用户聚集在一起并为其授予访问相同数据的权限。

数据连续性审计

Siebel Systems 支持各种程度的审计。

- 在最简单级别，每个数据记录都具有创建日期和最后更新者字段（时间和人物）。通过附加配置，您可以为附加的审计级别生成活动。如果存在有限的审计需要（只有一些区域需要跟踪），这是最适于使用的级别。
- Siebel 应用程序可以维护信息的审计追踪，指明何时已经更改了业务组件字段，谁更改了这些字段以及做了哪些更改。审计追踪是一个可配置功能，它让用户可以选择要审计的业务组件和字段，并且确定审计的范围。
Siebel 客户可以选择审计所有的活动，或将审计的范围限定为由某些职责、职位或雇员执行的那些操作。Siebel 应用程序还允许客户审计特定的数据字段或对象。
- Siebel 客户也可以依靠随所有支持的数据库提供的数据库审计功能。所有的供应商都支持高级别的审计：B3 或 C2 Orange 登记级别。（数据库审计要求提供附加的空间和安全人员以复审审计信息。）
- 您可以使用 Siebel Workflow 配置工作流程过程，以保存关于对特定业务组件所做更改的信息。
- 您还可以将脚本附加至业务组件 Write_Record 事件，并且保存有关交易的信息。

有关详细信息，请参阅第 41 页的“数据连续性审计”。

用于防止入侵的安全物理部署

必须对作为 Siebel 应用程序主机的物理设备的访问加以保护。如果这些设备受到威胁，这些机器上的所有应用程序的安全性都会受到威胁。您可以将提供机器级别安全性的实用程序用于 Siebel 应用程序中，这些实用程序对 Siebel 应用程序是透明的，它们是通过强制使用机器口令或对机器的硬盘加密来提供安全性的。

在 Siebel 应用程序部署中，Web 服务器位于 *非军事区* (DMZ)。防火墙之外的客户机通过安全连接访问 Web 服务器和 Siebel 服务器。

- 在雇员应用程序部署中，客户机以及服务器通常位于防火墙的后面。
- 在客户或合作者应用程序部署中，或者在访问应用程序的雇员位于防火墙之外的雇员应用程序部署中，Siebel 服务器部署在附加防火墙的后面。

Siebel Systems 还支持反向代理配置，以进一步增强 DMZ 安全性。越来越多的防火墙供应商提供了虚拟专用网络 (VPN) 功能。VPN 为需要远程访问的用户（例如雇员）提供了一个连接至 Siebel 应用程序的保护方式。

Siebel eBusiness Applications 与行业领先的第三方供应商密切配合，以提供附加的物理安全措施，例如，攻击防护、数据备份和灾难恢复。例如，HTTP 负载平衡通过处理 TCP 连接并且在传入的攻击到达 Siebel 服务器之前捕获这些攻击来提供保护，防止受到拒绝服务攻击。而且，只需要在 Web 服务器与 Siebel 服务器之间的防火墙打开一个 IP 地址和一个端口即可。

Siebel Systems 体系结构利用了高可用性技术的优势，例如 Microsoft Cluster Services，这些技术通过在多个系统之间分摊负载，使多台计算机作为一台计算机工作。高可用性技术满足了故障转移和灾难恢复管理的需要。有关详细信息，请参阅 *部署计划指南*。

有关详细信息，请参阅第 4 章“物理部署和审计”。

移动解决方案的安全性

Siebel Systems 提供了一整套移动解决方案，以允许远程访问 Siebel eBusiness Applications 中的数据。这些解决方案支持各种移动平台，包括无线电话、掌上设备和膝上型电脑（运行 Siebel 移动 Web 客户机）。

Siebel Systems 为使用这些设备访问 Siebel 应用程序的客户提供了安全性，并且与其它类型移动设备的联盟合作者通力合作。

- 有关 Siebel Wireless 应用程序安全问题的信息，请参阅 *Siebel Wireless Administration Guide*。
- 有关 Siebel Handheld 应用程序安全问题的信息，请参阅 *Siebel Bookshelf* 上使用 Siebel Handheld 客户机的特定 Siebel 产品的文档。
- 有关可安装在膝上型电脑等移动设备上的 Siebel 移动 Web 客户机安全问题的信息，请参阅第 55 页的“为移动 Web 客户机同步配置加密”和第 122 页的“移动 Web 客户机同步的验证”。

有关附加移动 Web 客户机安全问题的信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

保护实时无线通讯

Siebel Wireless 通过启用浏览器的移动设备，提供了对 Siebel 应用程序的实时无线访问。以 XML 或 HTML 格式产生的 Siebel Wireless 视图通过 Siebel 支持的 Web 服务器发送到无线网络，然后最终发送到请求者已启用浏览器的无线设备。

在此企业解决方案中，Web 服务器和 Siebel 服务器位于 Siebel 客户的防火墙内部，因此可以保护数据的安全性，并且使用标准协议保护无线网络之间基于浏览器的数据传输。

可用于保护数据的方法有多种，包括适用于无线设备的无线传输安全层（与安全套接层 (SSL) 等效）以及第三方产品，其中又包括通过 RIM 移动数据服务实行的三重 DES（数据加密标准）加密。

在 RIM BlackBerry 无线掌上设备上使用 Siebel 应用程序时，数据通过无线数据网络传送，并且在安全的 BlackBerry Enterprise Server 与移动数据服务的共同配合下进行路由。在 BlackBerry 掌上设备与公司基础设施之间传输的所有数据都通过三重 DES 进行加密。这些数据在从来源到目标的整个传输路径中始终加密。

移动设备用户验证

移动设备本身必须是安全的。如果无线设备或掌上设备落入坏人之手，组织需要确保敏感数据不会受到危害。Siebel 应用程序与这些设备中嵌入的安全性完全兼容，因为验证通常是一项设备级别的决策，而不是特定于应用程序的决策。

Web 浏览器的安全设置

Siebel eBusiness Applications 中的某些特点和功能与 Web 浏览器的安全性或其它设置相结合使用。

有关在部署 Siebel 客户机时使用的浏览器设置的详细信息，请参阅 *Siebel System Administration Guide*。

注释：有关 Web 浏览器设置的详细信息，请参阅浏览器附带的文档和 Siebel SupportWeb 上的 [系统要求和支持的平台](#)。

安全性参考的书目

有关管理网络安全以及行业安全趋势的详细信息，请查阅以下书籍和 Web 站点。

书籍

Stallings, William. *Cryptography and Network Security: Principles and Practice*, 1999 年第二版。Prentice Hall, <http://www.prenhall.com>。

Garfinkel, Simon with Gene Spafford. *Web Security, Privacy & Commerce*, 2002 年 1 月第二版。O'Reilly & Associates, Inc., <http://www.oreilly.com>。

Northcutt, Stephen, et al. *Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems*, 2002 年 7 月第一版。New Riders Publishing, <http://www.newriders.com>。

Web 站点

安全协会和安全标准委员会的一些有用 Web 站点包括：

- 卡内基梅隆大学的 CERT 协调中心 <http://www.cert.org>。
- Sun Microsystems 的安全页 <http://www.sun.com/software/security/>。
- Microsoft 安全及隐私主页 <http://www.microsoft.com/security/>。

注释：网址可能会随时更改。如果以上所列的 URL 不再有效，请尝试使用搜索引擎找到新的网址。

配置安全性的指示

本小节总体概括地介绍了您可以为利用 Siebel Business Applications 的安全资源优势而执行的任务。请将本小节用作设置 Siebel 环境安全性的设置清单。

每项任务都包括一个用于提供如何执行该任务详细信息的指示器。指示器包括对本指南后面章节以及 *Siebel Bookshelf* 上其它文档的参考。

- 1** 在安装 Siebel 软件期间，请为防火墙访问计划 Siebel 服务器和第三方 HTTP 负载均衡器 TCP 端口的使用。请参阅第 4 章“物理部署和审计”。另请参阅 *部署计划指南* 和适用于您正在使用的操作系统的 *Siebel 安装指南*。
- 2** 在安装 Siebel 站点之后，请更改 Siebel 帐户的缺省口令。有关详细信息，请参阅第 3 章“更改或添加口令”。
 - 更改 SADMIN 口令。
 - 添加用于更新 Web 服务器图像的口令。
- 3** 确保已对通讯和重要数据进行加密。请参阅第 5 章“通讯和数据加密”。
- 4** 实施安全适配器验证或 Web 单一登录以便验证用户。有关详细信息，请参阅第 6 章“安全适配器验证”和第 7 章“Web 单一登录验证”。
- 5** 设置访问控制系统，以便控制用户对数据记录和 Siebel 应用程序视图的可视性。有关详细信息，请参阅第 10 章“配置访问控制”。
- 6** 启用审计追踪功能，以监控数据库更新和更改。请参阅第 41 页的“数据连续性审计”。另请参阅 *应用程序管理指南*。
- 7** 确保移动 Web 客户机和 Siebel 站点之间的通讯是安全的。

为移动 Web 客户机启用加密。请参阅第 55 页的“为移动 Web 客户机同步配置加密”。

对于其它的移动 Web 客户机安全问题（例如，更改本地数据库的口令和对本地数据库进行加密），请参阅 *Siebel Remote and Replication Manager Administration Guide*。

3

更改或添加口令

本章提供了有关如何更改缺省口令的准则。它包括以下主题：

- 第 27 页的“更改缺省口令”
- 第 32 页的“添加用于更新 Web 服务器静态文件的口令”
- 第 33 页的“管理 eapps.cfg 文件中的加密口令”

注释：有关通过安全适配器配置和使用散列用户口令和数据库证书口令的信息，请参阅第 109 页的“配置口令散列处理”。

更改缺省口令

Siebel eBusiness Applications 随附的 Siebel 数据库服务器安装脚本和 seed 数据将在您的站点创建多个缺省帐户。这些帐户用于管理和维护 Siebel 网络。为了保证站点的安全性，请确保更改这些帐户的缺省口令。

注释：有关更改移动 Web 客户机上本地数据库管理口令的信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

后面的小节包括了有关更改帐户口令的过程。在更改缺省口令之前，请检查以下几点：

- 对于最终用户，Siebel 应用程序中（“用户首选项”屏幕，“用户资料”视图）“口令”和“验证口令”字段的可用性由以下几项因素决定：
 - 对于使用 LDAP 或 ADSI 验证的环境，基本安全机制必须允许实现该功能。另请参阅第 70 页的“LDAP/ADSI 目录的要求”。此外，LDAP 或 ADSI 安全适配器的“传播更改”参数（别名为 PropagateChange）必须是 TRUE（缺省值为 TRUE）。对于 Siebel 专用 Web 客户机，系统首选项 SecThickClientExtAuthent 也必须是 TRUE。有关详细信息，请参阅第 6 章“安全适配器验证”。
- 对于使用数据库验证的环境，数据库安全适配器的传播更改参数（别名为 DBSecAdpt_PropagateChange）必须为 TRUE。在名称服务器中为此参数定义的缺省值是 TRUE，在专用 Web 客户机的应用程序配置文件中为同一个参数定义的缺省值是 FALSE。有关详细信息，请参阅第 6 章“安全适配器验证”。
- 本节中的过程介绍了如何在 Enterprise 级别更改用于指定口令的参数。如果您在该级别设置和更改口令，所做的更改将在组件级别中继承。

然而，如果您在组件级别设置口令参数，从这一时刻起，只能为该组件更改此口令。除非在组件级别删除覆盖，否则在 Enterprise 级别更改口令不会导致在组件级别继承新口令。

有关详细信息，请参阅 *Siebel System Administration Guide*。
- 如果您要将第三方负载均衡器用于 Siebel 服务器负载均衡，请确保设置了负载均衡器的管理口令，同时确保负载均衡器产品的管理用户界面受到严格保护。

在 Microsoft Windows 上更改系统管理员口令

Siebel 数据库服务器安装脚本将创建 Siebel 管理员帐户，您可以使用该帐户执行管理任务。该帐户的缺省用户 ID 和口令分别是 SADMIN 和 SADMIN（区分大小写）。您应该更改该帐户的口令。

您可能还需要更改 Siebel 服务所有者帐户的口令，Siebel 服务所有者是指启动 Siebel 服务器系统服务的 Windows 用户。

下面分别提供了更改 Siebel 服务所有者帐户口令和 Siebel 管理员数据库帐户口令需要执行的过程。

注释：不要在口令中使用 ' 或 "（单引号或双引号）。由于引号在一些上下文中用作特殊字符，因此，在口令中使用引号可能导致口令被截断。例如，口令 abcde"f 可能被截断为 abcde。

有关在初次使用时设置这些帐户的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

更改 Siebel 服务所有者帐户的口令

使用以下过程，修改 Siebel 服务所有者的口令，Siebel 服务所有者是指启动 Siebel 服务器系统服务的 Windows 用户。

要更改 Siebel 服务所有者帐户的口令

- 1 更改 Siebel 服务所有者帐户的 Windows 域登录口令，Siebel 服务所有者是指启动 Siebel 服务器系统服务的用户。

有关更改域口令的详细信息，请参阅 Windows 文档。

- 2 更改 Siebel 服务器系统服务的口令。

- a 选择“开始”>“程序”>“管理工具”>“服务”。
- b 右键单击“Siebel 服务器系统服务”，并且选择“属性”。
- c 在该服务的“属性”对话框中，单击“登录”选项卡。
- d 在“口令”和“确认口令”字段中输入口令，然后单击“确定”。

注释：在此处指定的口令必须对应于您在步骤 1 中修改的 Windows 域登录口令。

- 3 停止并重新启动 Siebel 服务器系统服务。

有关详细信息，请参阅 *Siebel System Administration Guide*。

更改 Siebel 管理员数据库帐户的口令

使用以下过程，修改 Siebel 管理员数据库帐户的口令。您还必须更改 Siebel Enterprise 的相应口令参数。

要更改 Siebel 管理员数据库帐户的口令

- 1 使用 Siebel Server Manager，更改 Enterprise 的 Siebel 管理员口令。
 - a 登录到 Siebel 雇员应用程序，例如 Siebel Call Center。
 - b 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 服务器配置”>“Enterprise”。
 - c 单击“参数”选项卡。
 - d 在“Enterprise 参数”列表中，选择口令参数。
 - e 在“值”字段中，输入新口令，然后提交记录。
- 2 注销 Siebel 应用程序（所有用户都必须注销）。
- 3 更改数据库中 Siebel 管理员的口令。
有关详细信息，请参阅关于更改口令的 RDBMS 文档。
- 4 停止并重新启动 Siebel 服务器系统服务。
有关详细信息，请参阅 *Siebel System Administration Guide*。

在 UNIX 上更改 Siebel 管理员口令

Siebel 数据库服务器安装脚本将创建 Siebel 管理员帐户，您可以使用该帐户执行管理任务。该帐户的缺省用户 ID 和口令分别是 SADMIN 和 SADMIN（区分大小写）。您应该更改该帐户的口令。

注释：不要在口令中使用 ' 或 "（单引号或双引号）。由于引号在一些上下文中用作特殊字符，因此，在口令中使用引号可能导致口令被截断。例如，口令 abcde"f 可能被截断为 abcde。

有关在初次使用时设置此帐户的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

要更改 Siebel 管理员数据库帐户的口令

- 1 结束所有客户机会话，并关闭 Siebel 服务器。使用以下命令关闭服务器：


```
SIEBSRV_ROOT/bin/stop_server all
```

注释 为了停止 Siebel Enterprise 中的所有 Siebel 服务器，您必须在所有的 Siebel 服务器机器上运行该命令。
- 2 使用 Server Manager 更改 Siebel 网关名称服务器中的口令。
 - a 在 Enterprise 级别登录。


```
srvrmgr -g SiebelGatewayName -e EnterpriseServerName -u UserName -p Password
```
 - b 在 Server Manager 提示符位置输入以下命令：


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

3 在数据库中更改口令。

有关详细信息，请参阅关于更改口令的 RDBMS 文档。

4 停止并重新启动 Siebel 网关名称服务器。

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

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

5 重新启动所有的 Siebel 服务器。为每个适用的 Siebel 服务器执行该步骤。

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

6 连接至 Server Manager，并验证更改的口令：

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

您应该可以使用新口令以 SADMIN 身份登录。

更改表所有者 (DBO) 口令

Siebel 数据库服务器安装脚本还会创建数据库表所有者 (DBO) 帐户，该帐户用于修改 Siebel 数据库表。该数据库帐户的缺省用户 ID 和口令分别是 SIEBEL 和 SIEBEL（区分大小写）。您应该更改该帐户的口令。

表所有者用于通过 Siebel 应用程序生成 SQL 语句引用表名称（例如，SELECT * FROM SIEBEL.S_APP_VER）。

为 Siebel Enterprise 配置名为表所有者（别名为 Tableowner）的相应参数。应用程序对象管理器 (AOM) 等 Siebel 应用程序模块在为数据库操作生成 SQL 时，使用该参数值提供表所有者的名称。您可以在配置 Siebel Enterprise Server 期间指定表所有者的名称，从而为该参数提供值。

相关参数为表所有者口令（别名为 TableOwnPass）。Siebel 应用程序执行的大多数数据库操作都不要求提供表所有者的口令。因此，在配置 Siebel Enterprise Server 期间可以不配置该参数。

然而，如果未定义表所有者口令参数，有时可能需要手动提供表所有者口令。例如，在启动“生成新数据库”或“生成触发器”服务器组件的任务时，需要提供表所有者的名称和口令。

在更改表所有者口令时请注意以下要求：

- 如果您未定义表所有者口令参数，只能在 Siebel 数据库中更改表所有者的口令。（某些操作可能还需要手动提供更改后的口令。）
- 如果您定义了表所有者口令参数，则还必须在更改 Siebel 数据库中的口令时更新该参数的值。

要更改表所有者帐户的口令

- 1 使用 Server Manager，更改 Enterprise 的表所有者口令。
 - a 登录到 Siebel 雇员应用程序，例如 Siebel Call Center。
 - b 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 服务器配置”>“Enterprise”。
 - c 单击“参数”选项卡。
 - d 在“Enterprise 参数”列表中，找到表所有者口令参数（别名为 TableOwnPass）。
 - e 在“值”字段中，输入新值，然后提交记录。
- 2 如果您具有 Siebel 专用 Web 客户机用户，则还需要更改每个应用程序配置文件（例如，Siebel Call Center 的 uagent.cfg 文件）的 [ServerDataSrc] 部分中 TableOwnPass 参数的值。在为每一位用户安装 Siebel 客户机时，必须执行该步骤。
- 3 在数据库中更改口令。
有关更改口令的详细信息，请参阅 RDBMS 文档。
- 4 重新启动 Siebel 服务器。

有关更改口令的疑难解答，请检查失败的服务器任务

在更改 Siebel 管理员 (SADMIN) 口令和表所有者口令之后，请确保所有服务器任务仍在运行。

要检查失败的服务器任务

- 1 在 Siebel 服务器重新启动之后：
 - a 登录到 Siebel 雇员应用程序，例如 Siebel Call Center。
 - b 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 服务器管理”>“服务器”。
 - c 在“Siebel 服务器”列表中，选择适用的 Siebel 服务器。
 - d 单击“任务”选项卡，并检查服务器任务是否出错。
例如，您要运行 Call Center 对象管理器，请检查该组件是否存在出错的任务。
- 2 为每个显示错误的服务器任务同时更新 Siebel 管理员帐户口令以及表所有者口令。
 - a 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 服务器配置”>“Enterprise”。
 - b 单击“组件定义”选项卡。
 - c 选择产生失败任务的组件。
例如，Call Center 对象管理器存在失败的任务，则显示 Call Center 对象管理器组件定义的记录。
 - d 单击“参数”视图选项卡，显示该组件定义的参数。
 - e 为该组件定义的适用参数重新指定口令值。
例如，没有为 Call Center 对象管理器组件定义正确设置口令或表所有者口令参数，这可能就是任务失败的原因。如果确实如此，重新指定正确的值应该可以解决此问题。
- 3 重新启动 Siebel 服务器机器，并再次检查任务是否失败。

添加用于更新 Web 服务器静态文件的口令

作为硬安装流程的一部分，建议管理员定义一个口令，以更新 Web 服务器上高速缓存的图像以及其它与 Siebel 应用程序相关的静态文件。

Siebel 管理员每次重新启动 Web 服务器时，Siebel Web Server Extension (SWSE) 都会与 Siebel 服务器联系并刷新这些静态文件。管理员可能会发现输入 URL 命令是一种刷新文件的更有效方式，特别是在部署多个 Web 服务器时。

注释：设置口令只允许 Siebel 管理员通过访问最初位于 Siebel 服务器上的已更新文件，刷新 Web 服务器上高速缓存的静态文件。如果未设置口令，任何未授权的用户都可以调用 SWE 命令 `UpdateWebImages` 来更新这些文件。

要添加 Web 更新口令，请执行以下操作之一：

- 您可以使用在安装和配置 SWSE 时出现的“Web 更新保护密钥”屏幕。有关详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。
- 您可以在以后通过编辑 `eapps.cfg` 文件中 `webUpdatePassword` 参数的值，添加或更改此口令。该文件位于 `SWEAPP_ROOT\bin` 目录中，其中 `SWEAPP_ROOT` 是 SWSE 的安装目录。

注释：`webUpdatePassword` 参数提供了 Web 服务器安全性，但是与数据库帐户不对应，并且只能存储在 `eapps.cfg` 文件中。

如果 `eapps.cfg` 文件的口令加密生效 (`EncryptedPassword = TRUE`)，SWSE 配置则自动存储指定的 Web 更新保护密钥，作为 `webUpdatePassword` 参数的加密值。如果您手动编辑 `eapps.cfg` 文件，则必须使用 `encryptstring` 实用程序生成加密版本的口令，以便存储在文件中。

如果 `EncryptedPassword = FALSE`，口令不会作为加密值存储。在这种情况下，不能将口令作为加密值输入。

有关 `eapps.cfg` 文件口令加密以及 `encryptstring` 实用程序的详细信息，请参阅第 33 页的“管理 `eapps.cfg` 文件中的加密口令”。

有关管理 Siebel 应用程序的 Web 图像和其它文件的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要编辑 `eapps.cfg` 文件以配置 Web 更新口令

- 1 在您运行 SWSE 配置实用程序时，将自动设置 Web 公共根目录（Siebel 应用程序高速缓存 Web 文件的位置）。或者，您可以通过在 `eapps.cfg` 文件的每个应用程序部分中添加一行来指定此根目录。例如，要为 Siebel eService（适用于 Windows 机器上的 Web 服务器）指定 Web 公共根目录，请添加与此类似的参数：

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

其中 `SWEAPP_ROOT` 是 SWSE 的安装目录，例如 `D:\sea77\SWESApp`，`LANGUAGE` 是应用程序语言，例如，`ENU` 表示美国英语。文件将从 `SIEBSRVR_ROOT\webmaster` 目录的所有特定于语言的子目录复制到该位置，其中 `SIEBSRVR_ROOT` 是 Siebel 服务器的安装目录。

注释：Web 服务器上的目录结构与 Siebel 服务器上的目录结构类似，不同之处在于文件是从其原来的特定于语言的子目录上移。例如，将文件从 `SIEBSRVR_ROOT\webmaster\files\enu` 和 `SIEBSRVR_ROOT\webmaster\images\enu` 复制到 `SWEAPP_ROOT\public\enu\files` 和 `SWEAPP_ROOT\public\enu\images` 中。

为了节省 Web 服务器上的磁盘资源，建议为指定语言的所有应用程序设置相同的 `webPublicRootDir`。

- 2** Web 更新保护密钥（Web 更新口令）可以使用 SWSE 配置实用程序进行设置。或者，您可以通过在 eapps.cfg 文件的每个应用程序部分中添加一行来指定此口令。例如，要指定 Siebel eService 的 Web 更新口令，添加与此类似的参数：

```
[/eservice_enu]
webUpdatePassword = abcdef
```

注释：通常，口令加密适用于 eapps.cfg 文件，这在第 33 页的“管理 eapps.cfg 文件中的加密口令”中有介绍。

然后，Siebel 管理员可以使用该口令，从浏览器中更新高速缓存的静态文件，而不需要重新启动 Web 服务器。例如，指定与以下项类似的 URL：（不管是否使用加密，指定纯文本形式的口令。）

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

管理 eapps.cfg 文件中的加密口令

存储在 eapps.cfg 文件中的口令已被加密。在您配置 SWSE 时，口令以加密的形式被写入到文件中。（您可以根据情况关闭加密，并在该文件中使用纯文本口令。）

AnonPassword 参数的值取决于加密，不管该参数是只出现在 eapps.cfg 文件的 [defaults] 部分中，还是出现在特定于应用程序的部分中。webUpdatePassword 参数的值（Web 更新保护密钥）也被加密。

有关 webUpdatePassword 参数的详细信息，请参阅第 32 页的“添加用于更新 Web 服务器静态文件的口令”。

在您初始配置 SWSE 之后，加密行为取决于 EncryptedPassword 参数的状态。该参数将在您配置 SWSE 时被添加到 eapps.cfg 文件中，并且值为 TRUE。

EncryptedPassword 参数的状态与口令本身的加密状态必须相匹配。也就是说，如果参数为 TRUE，口令参数值必须加密，如果参数为 FALSE，口令则不能加密。

注释：如果 eapps.cfg 文件中不存在 EncryptedPassword 参数，缺省行为与 EncryptedPassword = FALSE 时的行为相同。强烈建议在 eapps.cfg 文件中保持 EncryptedPassword = TRUE。

在使用匿名用户口令时（应用程序登录或匿名浏览会话期间），加密的口令将被解密，并且与数据库帐户的存储值（使用 AnonUserName 参数指定）进行比较。

帐户和口令使用标准的 Siebel 数据库脚本创建，并且在您配置 SWSE 时它们必须已经位于 Siebel 数据库中。如果您在设置系统之后更改该帐户的口令，必须更新存储在 eapps.cfg 文件中的口令。

有关 eapps.cfg 文件中参数的详细信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。

使用 encryptstring 实用程序对口令进行加密

如果使用 Siebel Enterprise 配置实用程序更改匿名用户的口令或 Web 更新保护密钥，此口令将以加密的形式自动被保存。

然而，如果需要在 eapps.cfg 文件中手动添加相应参数的加密值（AnonPassword 或 webUpdatePassword），请使用 encryptstring.exe 实用程序生成加密的值，以作为参数值提供。

注释：如果您希望为不同应用程序的匿名用户使用不同的数据库帐户，则必须手动更新 eapps.cfg 文件。

在安装 Siebel 服务器和 SWSE 时都会安装 encryptstring 实用程序。该实用程序位于 *SIEBSRVR_ROOT\bin* 和 *SWEAPP_ROOT\bin* 目录中，其中 *SIEBSRVR_ROOT* 是 Siebel 服务器的安装目录，*SWEAPP_ROOT* 是 SWSE 的安装目录。

要生成加密的口令值作为输出结果，请输入以下命令：

```
encryptstring clear_text_password
```

例如，如果您要存储加密版本的 GUESTCST，它可能是您最初为匿名用户帐户指定的口令，您将输入以下命令：

```
encryptstring GUESTCST
```

此情况下的命令输出可能类似于 fhYt8T9N4e8se4X3VavTjQXwAEqm。（在每次使用 *encryptstring* 实用程序时，输出的特定值将会变化。）

警告：尽管匿名用户的权限有限制，通常建议在 Siebel 应用程序的生产部署时使用更安全的口令。第 27 页的“更改缺省口令”小节介绍了如何更改数据库帐户以及 Siebel 网关名称服务器上存储的参数相应值的口令。如果是匿名用户帐户，更改口令涉及到更改数据库帐户的口令以及更改 eapps.cfg 文件中的口令，这些在本节的前面已经做了介绍。

4

物理部署和审计

本章介绍了与网络上 Siebel 组件物理部署相关的安全问题。它包括以下主题：

- 第 35 页的“关于 Siebel 网络”
- 第 37 页的“防火墙和代理服务器支持”
- 第 39 页的“Siebel 服务器负载平衡在网络安全性方面的角色”
- 第 39 页的“端口号”
- 第 40 页的“限制访问”
- 第 41 页的“数据连续性审计”
- 第 42 页的“保护 Siebel 报表服务器”
- 第 43 页的“保护 Siebel 文档服务器”

注释：有关其中一些主题的详细信息，请参阅*部署计划指南*和适用于您正在使用的操作系统的*Siebel 安装指南*。

关于 Siebel 网络

在何处、如何布置网络计算资源，以及如何将网络计算资源与 Internet 和本地网上的其它机器协同工作，这些问题对网络安全具有显著影响。

第 36 页的图 3 显示了 Siebel Systems 网络中包括的基本组件。

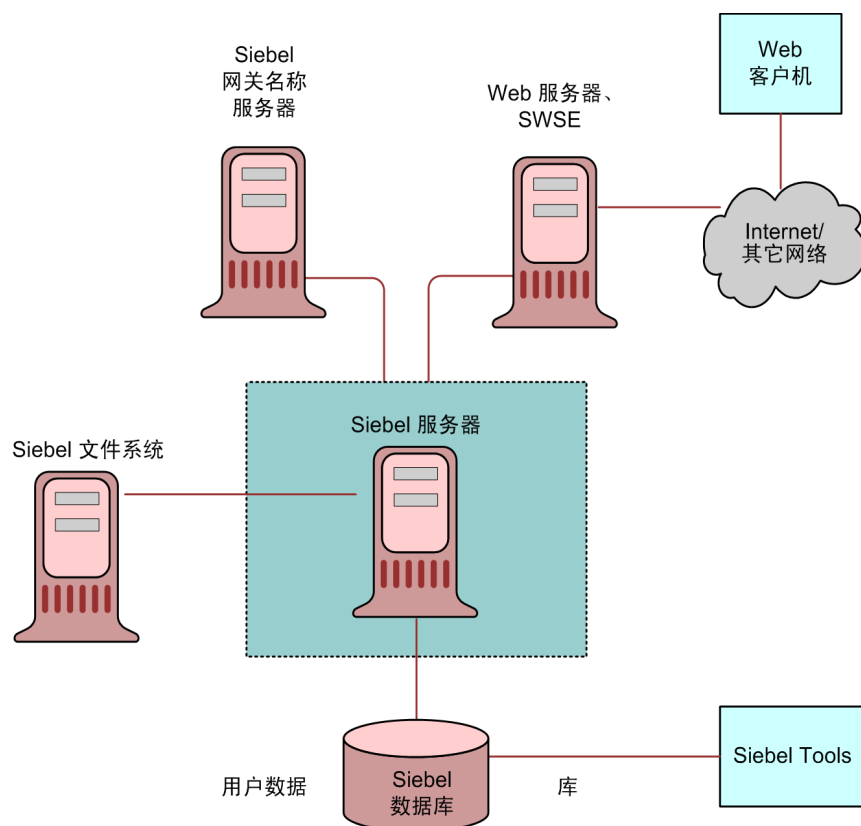


图 3. Siebel 网络组件

防火墙和代理服务器支持

防火墙将公司的外部 Siebel Web 客户机（那些通过 Internet 访问应用程序的客户机）与其内部网络分离，并控制这两个域之间的网络流量。防火墙定义了一个将未授权用户挡在所保护网络之外的聚点，防止易受攻击的服务进入或离开网络，并且防止遭受各种 IP 电子欺骗和路由攻击。

防火墙通常包括以下一项或多项功能：

- **代理服务器。**代理服务器是一个用作中转站的 Web 服务器，用于防止从 Internet 直接连接至您公司的本地网。它对 Internet 屏蔽内部 IP 地址。Siebel 应用程序支持在部署中同时使用正向和反向代理服务器。

反向代理服务器用作中转站，防止从客户机直接连接至 Web 服务器。反向代理服务器通过改写 Web 服务器的 IP 地址，对用户屏蔽内部 IP 地址，以避免将这些地址显示给用户。此外，反向代理服务器还可以高速缓存与最终用户更贴近的数据，从而提高系统性能。

使用标准交互的客户应用程序通常使用反向代理服务器进行部署。而使用高交互的雇员应用程序也可以使用反向代理服务器进行部署。

- **网络地址转换 (NAT)。**NAT 技术在 Internet 连接越过防火墙边界时，透明地改写这些连接的 IP 地址，从而允许本地网中的多台计算机隐藏在 Internet 上的单一 IP 地址后面。
- **虚拟专用网络 (VPN)。**Siebel 应用程序还支持使用虚拟专用网络。VPN 技术让防火墙以外的计算机可以穿过防火墙进行通讯，然后将它们象在防火墙内部连接一样显示在网络中。

VPN 技术让在家办公和出差的雇员可以访问许多公司的 Intranet 资源（例如，电子邮件服务器、文件共享等等），这些资源如果放在防火墙之外则得不到充分保护。

建议的防火墙布局

本节介绍了与 Siebel 网络组件有关的防火墙布局。Siebel 网络通常具有以下四个区域：

- **Internet。**外部 Siebel Web 客户机所在的区域。
- **Web 服务器区域。**Siebel Web 服务器和 Web 服务器负载均衡器所在的区域。Siebel Web Server Extension (SWSE) 安装在 Web 服务器机器上。该区域有时称为 DMZ（非军事区），它是外部网络首先与 Siebel 环境交互的区域。
注释：要处理外部 Siebel Web 客户机与包含 SWSE 的 Web 服务器之间的信息流量，建议您安装反向代理服务器。如果您要部署反向代理服务器，则应该将它布置在 DMZ 中，然后，可以将 Web 服务器和 SWSE 移到防火墙后面自己的区域中，或者移到 Siebel 服务器区域。
- **Siebel 服务器区域。**（有时称为应用程序服务器区域。）该区域中布置的组件包括 Siebel 服务器、Siebel 网关名称服务器、用于 Siebel 服务器的第三方 HTTP 负载均衡器（如果已部署）以及验证服务器（例如，LDAP 或 ADS 目录服务器）。
- **数据服务器区域。**Siebel 数据库、Siebel 文件系统和数据库服务器所在的区域。通常，这是公司大多数重要资产所在的区域。您应该将对此区域的访问只限定为授权的系统管理员和数据库管理员。

Siebel 网络体系结构允许您在每两个区域之间安装防火墙。然而，为获得最佳性能，请不要在 Siebel 服务器区域与数据服务器区域之间，或者在 Siebel 数据库与 Siebel 文件系统之间安装防火墙。第 38 页的图 4 显示了在 Siebel 网络中所建议的防火墙布局。

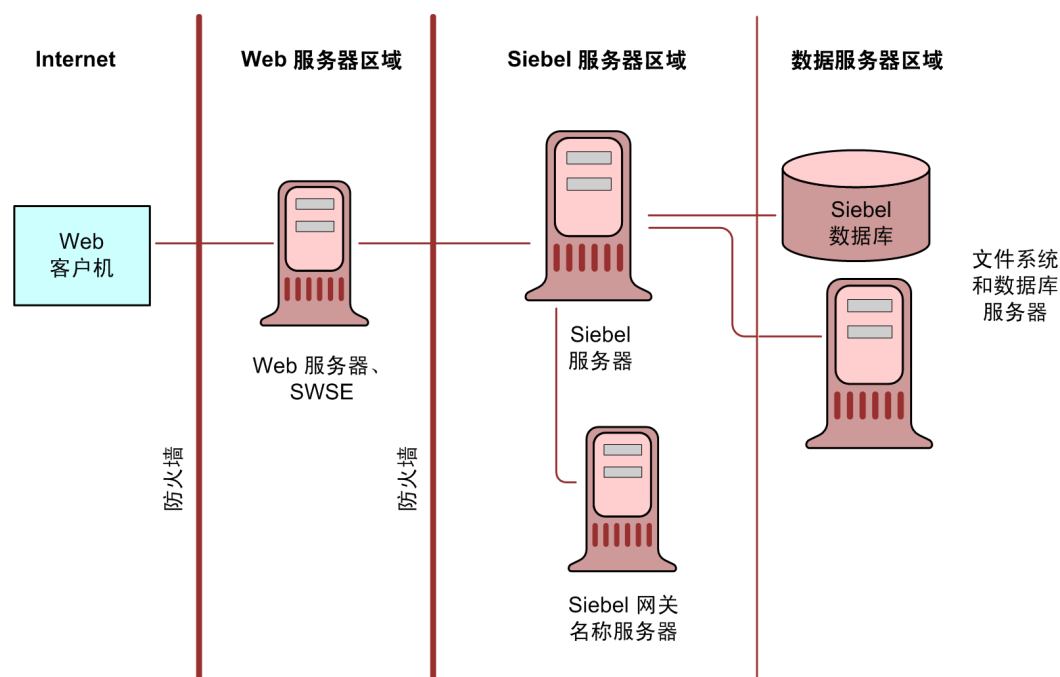


图 4. Siebel 网络中的防火墙

部署通过防火墙访问的 Siebel 应用程序

在跨防火墙部署 Siebel 应用程序时，请验证您的防火墙和代理服务器支持 HTTP 1.1 协议。该协议可以启用诸如内联数据压缩以改善带宽受限环境性能等的功能、cookie 以及其它功能。

如果您的防火墙不支持 HTTP 1.1，而您使用 HTTP 1.0，性能则会降低。如果您未使用 HTTP 1.1，则需要满足以下要求：

- 必须为 SWSE 禁用 Web 服务器压缩。在 eapps.cfg 文件中，将 DoCompression 参数的值设置为 FALSE。（在已知支持或可能支持压缩的环境下使用其它设置。）有关详细信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。
- 确保防火墙可以处理 cookie 包或其它特定于代理的功能，以启用 cookie 的转发。或者，减少或删除 cookie 在 Siebel 应用程序中的使用。有关详细信息，请参阅第 143 页的“Cookie 和 Siebel 应用程序”。
- 确保代理服务器不会将使用 HTTP 1.1 协议的任何标题内容传送给 SWSE。代理必须去除与 HTTP 1.0 不兼容的任何标题内容。

Siebel 服务器负载均衡在网络安全性方面的角色

您可以使用 Siebel 负载均衡或第三方 HTTP 负载均衡器来平衡 Siebel 服务器的负载。

第三方负载均衡器通常可以提供一些附加的安全功能，例如，对于多个 Siebel 服务器，限定将 TCP 端口暴露给单一端口。暴露单一端口让您合并网络访问，从而更好地执行端口监控和保护。它还提供了简化的防火墙配置。您只需要配置一个虚拟端口，而不是多个端口。

大多数第三方负载均衡器提供的附加安全功能包括：

- **拒绝服务 (DoS) 攻击防护。**在 DoS 攻击中，第三方 HTTP 负载均衡器帮助处理 TCP 连接。它可以在传入的攻击到达 Siebel 服务器之前捕获这些攻击。第三方 HTTP 负载均衡器通常具有一个内置机制，用于在入口点挡住 DoS 攻击。
- **虚拟 IP (VIP) 寻址。**第三方 HTTP 负载均衡器使用 VIP 寻址，以防止黑客直接访问 Siebel 服务器。由于 VIP 是一个 IP 别名，因此其物理地址不会被暴露。DMZ 中的 Web 服务器只与 VIP 通讯。
- **TCP 信息交换保护。**TCP 信息交换从第三方 HTTP 负载均衡器重放到 Siebel 服务器，而不是从 Web 服务器直接重放到 Siebel 服务器。

有关为 Siebel 部署配置负载均衡的信息，请参阅 *部署计划指南*。

端口号

进入 Siebel 服务器上的应用程序对象管理器 (AOM) 的网络流量将通过可配置的静态 TCP 端口。每个 Siebel 服务器只在一个 TCP 端口上监听。

有关配置用于 Siebel 应用程序的端口的详细信息，请参阅 *部署计划指南*。另请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

如果您使用 Siebel 负载均衡，AOM 则在每个 Siebel 服务器上的一个 TCP 端口监听是否存在从 Web 服务器到 Siebel 服务器的信息流量。如果您使用第三方 HTTP 负载均衡器，则还可以为从 Web 服务器到 Siebel 服务器的所有此类通讯使用一个单一的 VIP 地址和端口。如果不同的应用程序使用不同的 VIP/端口，您则还可以使用多个 VIP 地址和端口。

缺省情况下，Siebel 服务器配置假设对于所有 AOM，每个 Web 服务器都与一个 VIP 地址和端口通讯。您可以手动更改此项，以支持多个 VIP 地址/端口。

使用端口号的一些重要的计划问题包括：

- 要保护 Web 浏览器与 Web 服务器之间的通讯，请使用 SSL 在安装 SWSE 时指定 HTTPS 端口（缺省值为 443）。
- 如果您要设置用于 Siebel 应用程序的 LDAP/ADS 目录服务器，请使用用于安全传输的端口 636，而不是用于标准传输的端口 389。
- 如果您要使用 TCP/IP 筛选，请确保您所需的任何端口（包括 ServerMgr 端口）都没有被阻塞。如果所需的任何端口被阻塞，Siebel 服务器的状态则为“连接失败”。

- 要允许用户跨过防火墙访问 Siebel 应用程序，请确保 Web 服务器可从外部访问，并且可以使用 SCBroker 端口（Siebel 负载均衡）或第三方 HTTP 负载均衡器用于 TCP 信息流量的虚拟端口与 Siebel 服务器通讯。SCBroker 使用的缺省端口是 2321。
 - 如果您要使用 Siebel 负载均衡，请确保 Web 服务器可以访问每个 Siebel 服务器的 SCBroker 端口。
 - 如果您要使用第三方 HTTP 负载均衡器，请确保 Web 服务器可以与负载均衡器中指定的 VIP 地址和端口通讯。通常，负载均衡器布置在公司的防火墙里面，但是只要防火墙访问设置正确，客户就可以选择应该在何处布置负载均衡器。
- 一旦防火墙访问可用，您就可以使用 Siebel 支持的任何验证方法对用户进行验证。
- 防火墙外面的 Siebel Web 客户机用户（例如，授权供应商（合作者）或客户）可以使用标准 Web 服务器端口（缺省值为 80）访问 Siebel Web 应用程序。您可以配置防火墙，以便它不会通过 80 之外的其它任何端口传送信息流量。如果您的 Web 服务器需要通过 SSL 支持 HTTP，则可以开放端口 443。
- COM 数据控制和 Java DataBean 都使用 SISNAPI 进行通讯。COM 数据控制支持 RSA 和 Microsoft Crypto，但不支持 SSL。Java DataBean 支持 RSA，但不支持 Microsoft Crypto 或 SSL。
- Siebel 服务器与 Siebel 数据库之间通讯时使用的端口号是特定于数据库的。可用于此类通讯的缺省 TCP 端口号如下：
 - Oracle: 1521
 - Microsoft SQL Server: 1433
 - IBM DB2 UDB for Windows 和 UNIX: 5000（Siebel 缺省值）
 - IBM DB2 UDB for z/OS 和 OS/390: 无缺省值
- Siebel 服务器与 Siebel 文件系统和数据库服务器之间通讯时使用的端口号取决于文件系统的类型。缺省的 TCP 端口号是 139。缺省的用户数据报协议 (UDP) 端口号是 137 和 138。UDP 是与 TCP 处于同一级别的网络协议。TCP 和 UDP 都在 IP 顶部运行。
- 对于需要连接到 Siebel 服务器以便使用 Siebel Remote 同步的 Siebel 移动客户机用户，他们可以直接连接至用作 Siebel Remote 服务器的 Siebel 服务器。供移动用户使用的 Telnet 连接可以在 Siebel 环境中配置。然而，由于可能存在安全隐患，建议不要使用此类连接。

限制访问

本节介绍了物理部署与 Siebel 组件交互的产品时的相关安全问题。

客户机设备的实体安全

客户机设备的实体安全问题在 Siebel 应用程序之外进行处理。您可以使用提供机器级别安全性的实用程序，这些实用程序通过强制使用机器口令或对机器的硬盘加密来提供安全性。

大多数行业领先的掌上设备（例如，HP/Compaq 和 RIM 生产的设备）都具有用户启用的口令。例如，RIM 允许用户选择在打开设备时是否需要口令。Siebel Systems 与众多在掌上设备上启用附加安全层的第三方合作者密切合作，合作范围从生物识别验证到无线设备管理。

例如，mFormation Inc. 提供了连续监控无线网络，并在必要时远程删除设备内容的能力，从而防止在设备落入坏人之手时数据被擅自访问。

数据库服务器访问

客户应该在帐户登录级别和网络可视性级别，为数据库访问定义严格的政策。只有授权用户（例如，批准的数据库管理员 (DBA)）才能具有系统帐户（用于 root）以及远程访问服务器的权限。在 UNIX 上，建议您定义 netgroup 以便控制对数据库服务器的访问。

要限制 Siebel 服务器进程的权限，请分配一个特定于 Siebel 服务器的操作系统帐户。该帐户应该只具有访问 Siebel 应用程序所需文件、进程和可执行文件的权限。Siebel 服务器帐户不应该是 root 管理员。

在 UNIX 系统上，.rhosts 文件允许远程的 root 管理员访问其它机器。要提供对 Siebel 服务器的适当的访问和控制级别，建议您尽量不要使用 .rhosts 文件。

Siebel 文件系统访问

Siebel 文件系统由 Siebel 数据库服务器可通过网络访问的共享目录组成，并且包含 Siebel 应用程序使用的物理文件。文件系统用于存储文档、图像和其它类型的文件附件。

Siebel 用户帐户的访问请求由 Siebel 服务器处理，后者然后使用文件系统管理器 (FSM) 服务器组件访问 Siebel 文件系统。FSM 通过与文件系统目录交互来处理这些请求。Siebel Remote 组件还可以直接访问文件系统。其它服务器组件则通过 FSM 访问文件系统。

要防止从 Siebel 应用程序环境之外直接访问 Siebel 文件，则应当只让 Siebel Service 所有者才具有访问 Siebel 文件系统目录的权限。Siebel 服务器进程和组件使用 Siebel Service 所有者帐户操作。

注释：如果是 Siebel 专用 Web 客户机，您可以通过 FSM 或者每个独立客户机的直接连接访问 Siebel 文件系统。有关详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

数据连续性审计

要维护数据的连续性并监控 Siebel 站点的活动，Siebel 应用程序可以维护一份信息的审计追踪，以指明何时已经更改业务组件字段，谁更改了这些字段以及做了哪些更改。

审计追踪是一项可配置的功能，用于建立一个历史记录，其中记录了已对各种 Siebel 应用程序中的各种信息所做的更改。审计追踪是一项记录，用于显示谁访问了项目，执行了什么操作，何时执行了操作，以及如何更改了值。因此，在保证安全而要检查特定记录的历史记录并记下所做的修改以供将来分析和存档时，审计追踪非常有用。审计追踪将记录信息，但不要求与用户交互，也不要求用户输入。

通过使用审计追踪，用户可以跟踪哪一位雇员修改了某个字段，以及更改了哪些数据。呼叫中心用户可以跟踪服务请求的状态更改，或计算处理服务请求花费的时间。例如，用户可以针对“服务请求”屏幕中的某个状态字段激活审计追踪功能。系统会为每一个状态更改创建一项审计追踪记录，并且同时记录时间戳以及做出更改的用户的 ID。

审计追踪的一种更高级用法就是，用户通过执行复杂的查询及时地重新组织在某个时间点存在的记录。公司可以在遵照政府规定的情况下使用审计追踪来跟踪数据历史记录，以分析业绩并提高服务质量。对于要遵照政府规定，使用审计追踪来跟踪对每项记录所做的每个更改的公司，必须考虑在大量执行此类审计时造成的业绩分流后果。

审计追踪适用于每个 Siebel Web 部署和配置选项，包括与移动 Web 客户机同步以及在 Siebel Replication Manager 支持的区域数据库执行复制。审计追踪不仅记录成功提交的交易，而且记录由于冲突而未与服务器同步的交易。

有关配置和使用审计追踪的信息，请参阅 *应用程序管理指南*。

保护 Siebel 报表服务器

本节介绍了保护 Siebel 报表服务器、AOM 与 Siebel Web 客户机之间通讯的信息。请注意以下事项：

- Siebel Reports 不支持使用 LDAP 或 ADSI 执行用户验证。用户必须在 Siebel 应用程序与 Actuate 之间同步才能使 Siebel Reports 正确工作。
- Actuate 组件之间的通讯超出 Siebel 应用程序环境的范围。有关详细信息，请查阅 *Siebel eBusiness Third-Party Bookshelf* 中的 Actuate 产品文档。

有关详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*、*部署计划指南* 和 *Siebel 报表管理指南*。

Siebel 报表服务器组件

Siebel 报表服务器由以下组件组成：

- **Actuate iServer**。管理支持管理、查看、打印、计划和验证报表的所有服务。所有报表属性都存储在 Actuate Encyclopedia 中。
- **Actuate Management Console**。基于浏览器的界面，用于管理一个或多个 Actuate iServer 和 Encyclopedia。（取代 Actuate Administrator Desktop。）
- **Actuate Active Portal**。提供对 Actuate Encyclopedia 中报表的访问权限。用户可以生成、查看、打印和共享报表。
- **Actuate e.Report Designer Professional**（可选）。供专业开发人员建立新报表或定制现有报表使用。Actuate Basic Language 和 Actuate Foundation Class Library 支持新增的高级报告功能。
- **Actuate e.Report Designer**（可选）。让您可以使用其图形用户界面设计并建立报表。该应用程序是对 e.Report Designer Professional 的补充，并且供业务用户设计和分发各种报表使用。不需要编程。该应用程序支持修改复杂的报表和使用库中的组件。

为提高安全性配置 Siebel 报表服务器

为提高安全性配置 Siebel 报表服务器的区域包括：

- Siebel Web 客户机与 Actuate Active Portal 之间的通讯
- 与 AOM 的通讯

Siebel Web 客户机与 Actuate Active Portal 之间的通讯

此通讯在查看报表时进行。在 Siebel Web 客户机与 Actuate Active Portal 通讯时，包含已加密的报表服务器登录参数的 cookie 通过 HTTP 标题进行传送。由于登录参数被加密，因此在缺省情况下，这一部分的通讯是安全的。报表本身以 DHTML 格式通过 Actuate Active Portal 传送到 Siebel Web 客户机。

要保证这一部分的通讯安全，请通过设置以下参数启用 SSL：

Actuate Server Network Protocol Name = HTTPS

有关设置该参数的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南* 中介绍的安装后任务。

有关 cookie 和 Siebel 应用程序的详细信息，请参阅第 143 页的“Cookie 和 Siebel 应用程序”。

与 AOM 的通讯

您可以使用对 Active Portal 的 SOAP 调用，通过适用于 Actuate 的 Siebel 报表适配器（它是 Siebel Web Services Framework 的一部分）启动报表生成，使用 Siebel 应用程序提供的用户证书，建立至 Actuate iServer 的连接。iServer 将建立一个独立的应用程序对象管理器会话，以获得生成报表所需的数据。该通讯被加密。

为 Actuate 服务器连接字符串参数设置所需的加密类型（RSA 或 MSCRYTPO）。例如：

Actuate Server Connect String = RSA

有关设置该参数的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南* 中介绍的安装后任务。

保护 Siebel 文档服务器

本节介绍了保护 Siebel 文档服务器与 Siebel 服务器之间通讯时出现的问题。

有关 Siebel 文档服务器的详细信息，请参阅 *应用程序管理指南*。

- 所有文档模块都通过 Siebel 服务器传入。同样，Siebel 服务器控制安全性，并且仅代表直接与 Siebel 文档服务器交互的客户机或用户。只有按照 Siebel 服务器服务验证的用户才应该具有访问文件系统的权限，以及 Siebel 文档服务器的执行权限。
- Microsoft 在“资源工具箱”中提供了一些标准实用程序，用于保障通用 Microsoft Windows 机器的安全。建议使用 C2.exe 等工具，以保护此类环境的安全。这些工具可以很容易从 Microsoft 获得。
- Microsoft Word 的确支持宏安全性选项。宏安全性应该设置为高，以便文档服务器无法执行不可信的宏。由于提案内部应该不需要宏，因此这应该不是一个问题。
- 确保 Siebel 文档服务器或最终用户使用的模板已得到保护，并且在向 Siebel 文档服务器提供模板的任何机器上落实了病毒防范政策。

5

通讯和数据加密

本章概括地介绍了 Siebel Enterprise 组件之间的通讯路径以及如何配置组件以实现安全通讯的信息。它还介绍了可用于传输和存储 Siebel 应用程序数据的加密技术，并且介绍了适用于 Unicode 环境的一些问题。它包括以下主题：

- 第 45 页的“加密类型”
- 第 48 页的“配置安全通讯”
- 第 57 页的“配置数据加密”
- 第 64 页的“Unicode 支持的安全注意事项”

加密类型

加密是指出于安全考虑而对数据进行编码的一种方法。Siebel 应用程序支持安全 Web 通讯和敏感数据（例如，口令）加密的行业标准。

根据美国的加密技术出口限制规定，Siebel Systems 在产品中只嵌入 56 位密钥的 RC2 加密技术。客户如果要使用 128 位加密密钥的 RC2 或者使用 128 位、192 位或 256 位加密密钥的 AES，可以使用 Siebel Strong Encryption Pack 实现这一点。有关 Siebel Strong Encryption Pack 的详细信息，请转到 Siebel SupportWeb。

为了确保信息私有，Siebel 应用程序在传输和存储数据时使用以下加密技术：

- **用于 Web 客户机连接的 SSL 加密。**为了确保通过 Internet 传输的数据的安全性，Siebel 应用程序使用支持的 Web 服务器平台的安全套接层 (SSL) 功能，保护 Web 浏览器与 Web 服务器之间的数据传输。

Siebel 应用程序可以配置成完全在 HTTPS 下运行、特定页面在 HTTPS 下运行（仅限于标准交互），或者只是在 HTTPS 下处理登录请求。

- **用于 SISNAPI 连接的加密 (SSL、Microsoft Crypto 或 RSA)。**对于 Siebel 组件之间的通讯，Siebel 管理员可以为 SISNAPI（Siebel Internet 会话 API）启用加密。SISNAPI 是基于 TCP/IP 的 Siebel 通讯协议，它为网络通讯提供了安全和压缩机制。

SISNAPI 加密可以基于安全套接层 (SSL) 或 Microsoft Crypto API 或 RSA 算法。多个操作系统平台都支持 SSL 和 RSA。

SSL 还支持在 Web 服务器与 Siebel 服务器之间或在两个 Siebel 服务器之间验证认证。

- **用于 LDAP/ADS 连接的 SSL 加密。**安全套接层 (SSL) 可以用于连接至认可的 LDAP 或 ADS 目录。
- **用于电子邮件服务器连接的 SSL 加密。**使用 Siebel Communications Server 组件，支持对电子邮件服务器连接使用 SSL 加密。有关详细信息，请参阅 *Siebel Communications Server 管理指南*。

- **AES 和 RC2 数据库加密。** Siebel 应用程序允许客户对存储在 Siebel 数据库中的敏感信息（例如，信用卡号、社会保障号、出生日期等等）加密，以避免在未访问 Siebel 应用程序时查看这些信息。

客户可以将 Siebel 软件配置为，在将数据写入到数据库之前先对字段数据加密，然后在检索相同数据时再对数据解密。这样可以防止试图直接从数据库中查看敏感数据。

敏感数据可以通过 AES（高级加密标准）或 RC2 加密，以各种长度的密钥进行加密。您可以使用 Siebel Tools 对业务组件字段启用加密。有关详细信息，请参阅第 57 页的“配置数据加密”。

注释：在字段级别加密的数据不能复制给使用 Siebel Remote 的移动用户，因为这些数据无法在移动 Web 客户机上进行解密和查看。然而，如果移动 Web 客户机的本地数据库基于加密的模板，则可以对本数据库加密。有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

- **RSA SHA-1 口令散列处理。** Siebel 管理员可以启用口令散列处理。散列处理使用单向的散列处理算法。缺省的口令散列处理方法是 RSA SHA-1。（现有客户仍然可以使用以前的杂乱算法。）

口令散列处理使口令对未经授权的外部应用程序无效，并且防止使用 Siebel eBusiness Applications 之外的其它任何程序直接对数据进行 SQL 访问。有关详细信息，请参阅第 109 页的“配置口令散列处理”。

第 47 页的图 5 显示了 Siebel 应用程序环境中的一些可用加密类型。

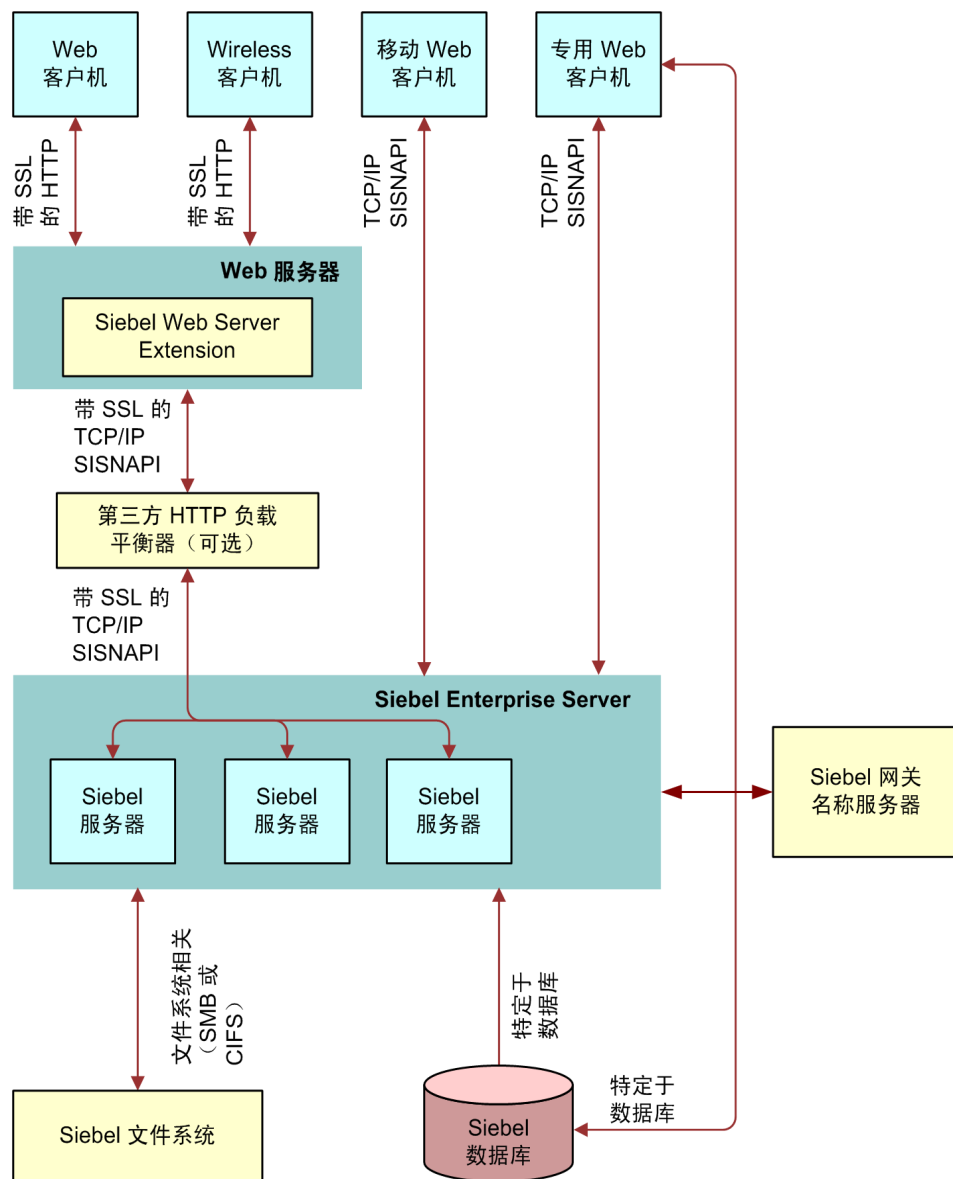


图 5. Siebel 应用程序环境中的通讯加密

配置安全通讯

下面的小节介绍了如何在 Siebel 环境中为组件之间的通讯设置加密。您可以为 Web 服务器、Siebel 服务器与 Siebel Web 客户机之间的数据信息流量配置加密。

注释：本节中介绍的加密选项不用于对数据库中的数据进行加密，这在第 57 页的“配置数据加密”中有介绍。此外，这些加密选项不用于与数据库的通讯。对于此类加密，请向数据库供应商咨询。

为 Siebel Enterprise 和 SWSE 配置加密

在您安装 Siebel Enterprise 或 Siebel Web Server Extension (SWSE) 之后配置这些程序时，请指定为 Siebel 服务器与 Web 服务器 (SWSE) 之间以及在两个 Siebel 服务器之间的通讯使用哪个加密类型。这些模块之间的通讯使用 SISNAPI 协议。

加密类型设置确定在生成的连接字符串中如何为 Siebel 应用程序定义加密。它还与 Siebel Enterprise 参数加密类型的值相对应。

在您初次安装 Siebel Enterprise 或 SWSE 时，出现 Siebel 软件配置实用程序。有关运行此实用程序的信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

通过该实用程序，您可以指定使用安全套接层 (SSL)、Microsoft Crypto 或 RSA 加密。（如果是 SSL，您指定“无”，然后指定是否部署 SSL。）

警告：为 Siebel Enterprise（以及 Siebel 服务器）和 SWSE 设置相同的加密类型。如果您使用不一致的设置，Siebel 模块可能无法相互连接。

在 Siebel 软件配置实用程序中，“加密类型”屏幕显示用于配置加密类型的选项。您可以选择以下某个选项：

- **无。**如果您要使用安全套接层 (SSL)，而不是 Microsoft Crypto 或 RSA 加密，或者不使用加密，请指定该选项。
- **MSCRYPTO。**适用于 Siebel 组件之间通讯的 Microsoft Crypto 加密协议（该选项只适用于 Microsoft Windows 平台）。
- **RSA。**要对 Siebel 组件使用 RSA Security Systems 的 128 位强大加密功能时的一个必需协议。

注释：如果同时在 UNIX 和 Microsoft Windows 平台上安装 Siebel 产品，建议使用跨平台支持的加密方法，例如 SSL 或 RSA。

如果您为加密类型指定“无”，该实用程序则提示您是否要在企业中（适用于 Siebel Enterprise 或 SWSE）部署 SSL。

- 如果您指定部署 SSL，则会出现用于配置 SSL 的其它屏幕（这些屏幕是 SSL 配置实用程序的一部分）。有关详细信息，请参阅下面的小节：
 - 第 49 页的“为 Siebel Enterprise 或 Siebel 服务器配置 SSL 加密”
 - 第 52 页的“为 SWSE 配置 SSL 加密”

在为 Siebel Enterprise 或 SWSE 完成 SSL 配置后，您会返回到 Siebel 软件配置实用程序。（要为所有的 Siebel 服务器完成 SSL 配置，您随后可能需要一次或多次单独运行 SSL 配置实用程序。）

- 如果您没有指定部署 SSL，则不会显示 SSL 配置屏幕，而您将继续在主要的 Siebel 软件配置实用程序中执行配置任务。

Microsoft Crypto 或 RSA 加密的密钥交换

如果您要使用 Microsoft Crypto 或 RSA 加密，下面的步骤介绍了如何在客户机（例如，Web 服务器）与服务器（例如，Siebel 服务器）之间交换 Siebel 加密密钥。

- 1 客户机生成一个私有/公共密钥对。公共密钥作为 Hello SISNAPI 消息中的一部分发送给 Siebel 服务器。
- 2 服务器在收到 Hello 消息时，会生成基于 RC4 的对称会话密钥，并且使用 Hello 消息中的客户机公共密钥为对称的会话密钥加密。加密的会话密钥会作为 Hello Acknowledge 信息的一部分发回给客户机。
- 3 客户机使用私有密钥对服务器生成的会话密钥进行解密。从此时开始，客户机和服务器都使用服务器生成的会话密钥对消息进行加密和解密。
- 4 会话密钥对于整个连接期间一直有效。

注释：如果您要在 Web 服务器与 Siebel 服务器之间或在两个 Siebel 服务器之间使用 SSL 加密，则通过标准的 SSL 信息交换处理密钥交换。

为 Siebel Enterprise 或 Siebel 服务器配置 SSL 加密

本节介绍了如何配置 Siebel Enterprise 或 Siebel 服务器，以便在 Siebel 服务器与 Web 服务器 (SWSE) 之间以及两个 Siebel 服务器之间进行 SISNAPI 通讯时，使用安全套接层 (SSL) 加密和验证。为 SISNAPI 通讯配置 SSL 是可选步骤。

Enterprise 级别的配置适用于企业中的所有 Siebel 服务器。总的来说，在 Siebel 服务器级别应该以不同的方式配置一些设置。

配置 Siebel 服务器与 Web 服务器之间的 SSL 通讯还需要您配置 SWSE 以便使用 SSL，这在第 52 页的“为 SWSE 配置 SSL 加密”中有介绍。

在为 Siebel 服务器和 SWSE 配置 SSL 时，您还可以为相关的模块配置连接验证。换句话说，在一个模块连接至另一个模块时，可能需要使用第三方认证进行模块间的相互验证。

连接验证方案包括：

- Siebel 服务器根据 Web 服务器验证连接。
- Web 服务器根据 Siebel 服务器验证连接。
- Siebel 服务器根据另一个 Siebel 服务器验证连接。

同级验证选项需要首先完成相互验证。

请执行以下过程，在 Siebel 网关名称服务器中添加参数。如果您还为 SSL 配置 SWSE，该过程中提到的名称服务器参数（简称）对应于在 eapps.cfg 文件的 [connmgmt] 部分中添加的参数。或者，可以使用 Siebel Server Manager 设置该过程中提到的名称服务器参数。

关于 SSL 验证使用的认证和私有密钥文件

在您为每个 Siebel 服务器和 SWSE 配置 SSL 验证时，请指定参数值，以分别表示 Siebel 服务器和 SWSE 机器上的认证文件、认证机构文件和私有密钥文件的名称。

您为此使用的认证文件必须由第三方认证机构发行，而且必须向第三方认证机构索取。认证文件必须使用 ASN（抽象语法符号）或 PEM（增强保密邮件）格式。每台机器上的认证必须唯一。认证机构文件确定了发行认证的信任机构。私有密钥文件必须使用 PEM 格式。

认证文件和私有密钥文件通常安装在配置了 SSL 的每台 Siebel 服务器机器和 SWSE 机器上。

您不需要对同一台机器上两个组件之间的通讯进行验证或加密。

为 Siebel 服务器运行 SSL 配置实用程序

本节介绍了为 Siebel 服务器运行 SSL 配置实用程序，即 Siebel 软件配置实用程序（Siebel 服务器 SSL）。您可以使用该过程配置 Siebel Enterprise 或者配置单个 Siebel 服务器。

注释：在执行以下过程时，如果您指定为 Siebel Enterprise 而不是单个的 Siebel 服务器配置 SSL，则 Siebel Enterprise 中的所有 Siebel 服务器将继承所有设置，包括密钥文件名、口令以及认证文件名。您可以稍后再次运行该实用程序，以分别配置单个的 Siebel 服务器，届时您可以指定每个服务器的唯一密钥文件名、口令或唯一认证文件名。为了完整地 Siebel 服务器配置 SSL，您必须多次运行该实用程序。

不管您是以 GUI 模式还是控制台模式运行 SSL 配置实用程序，该实用程序的提示都是相同的。然而，这两种模式下的一些用户界面元素是不相同的。

在 Windows 中，为 Siebel Enterprise 或 SWSE 配置 SSL 时始终使用 GUI 模式。在 UNIX 中，为 Siebel Enterprise 或 SWSE 初始配置 SSL 时使用 GUI 模式。然而，如果您以后在 UNIX 平台上单独运行 SSL 配置实用程序时，将使用控制台模式。

要为 Siebel 服务器启用 SSL 加密

- 1 如果您要配置 SSL 验证，则在开始之前需要获取并安装所需的认证文件。
- 2 如果您要运行主要的 Siebel 软件配置实用程序以配置 Siebel Enterprise 或特定的 Siebel 服务器，请首先指定您要为 Siebel Enterprise 部署 SSL，然后启动 SSL 配置实用程序，这在第 48 页的“为 Siebel Enterprise 和 SWSE 配置加密”中有介绍。
- 3 或者，为了直接在 Siebel 服务器机器上运行 SSL 配置实用程序，请根据以下介绍，直接启动 SSL 配置实用程序：

- 如果是 Microsoft Windows 平台，请打开 MS-DOS 窗口，并输入以下命令（以 GUI 模式运行实用程序）：

```
SIEBSVR_ROOT\bin\ssincfgw.exe -l language -f
SIEBSVR_ROOT\admin\sslsiebsvr.scm -logevents all
```

其中：

- SIEBSVR_ROOT 是 Siebel 服务器的安装目录
- language 是运行 SSL 配置实用程序所要使用的语言（例如，ENU 代表美国英语）

- 如果是 UNIX 平台，请输入以下命令（以控制台模式运行实用程序）：

```
cd SIEBSRVR_ROOT
```

如果是 **Bourne shell** 或 **Korn shell**：

```
./siebenv.sh
```

（确保开始的句点 (.) 与 ./siebenv.sh 之间有空格。）

如果是 **C shell**：

```
source siebenv.csh
```

```
cd SIEBSRVR_ROOT/bin
```

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

其中：

- *SIEBSRVR_ROOT* 是 Siebel 服务器的安装目录
- *language* 是运行 SSL 配置实用程序所要使用的语言（例如，ENU 代表美国英语）

- 4 如果您要单独运行 SSL 配置实用程序（如第 50 页的步骤 3 中所述），请输入适用于所配置组件的 Siebel 网关名称服务器机器的主机名和 Siebel Enterprise 名称。

注释：如果您在运行 Siebel 软件配置实用程序时运行了 SSL 配置实用程序（如第 50 页的步骤 2 中所述），Siebel 网关名称服务器和 Siebel Enterprise 则已经指定，此时将不出现该屏幕。

- 5 指定配置类型：是为 Siebel Enterprise 还是为 Siebel 服务器配置 SSL。（就在该过程之前的注释中介绍了此选择隐藏的问题。）

- 6 如果您要配置 Siebel 服务器，请指定 Siebel 服务器的名称。

注释：如果您指定 Siebel 服务器 SSL，该设置则适用于 Siebel 服务器上的所有组件。您不能在组件级别指定设置。

- 7 指定认证文件和认证机构文件的名称。

名称服务器中的等效参数是 CertFileName（显示名称是认证文件名）和 CACertFileName（显示名称是 CA 认证文件名）。

- 8 指定私有密钥文件的名称以及私有密钥文件的口令，然后确认该口令。

您指定的口令将以加密的形式存储。

名称服务器中的等效参数是 KeyFileName（显示名称是私有密钥文件名）和 KeyFilePassword（显示名称是私有密钥文件口令）。

- 9 指定是否需要同级验证。

同级验证表示只要建立连接，该 Siebel 服务器必须根据客户机（即 SWSE 或连接的另一个 Siebel 服务器）并通过认证进行自我验证。同级验证的缺省设置为 False。

注释：如果您还为连接的客户机（即 SWSE 或连接的另一个 Siebel 服务器）设置同级验证，则必须为 Siebel 服务器设置同级验证。

名称服务器中的等效参数是 PeerAuth（显示名称是同级验证）。

10 指定是否需要同级认证验证。

同级认证验证执行反向 DNS 查找，以便独立验证 Siebel 服务器机器的主机名与认证中的主机名是否相同。同级认证验证的缺省设置是 false。

名称服务器中的等效参数是 PeerCertValidation（显示名称是验证同级认证）。

11 如果您在运行 Siebel 软件配置实用程序时运行了 SSL 配置实用程序，则返回至该流程，这在适用于您正在使用的操作系统的 *Siebel 安装指南* 中有介绍。

12 如果已直接运行 SSL 配置实用程序，请复审设置，完成配置，然后重新启动服务器。

13 如有必要，请为您环境中的每个 Siebel 服务器重复执行该过程。

请确保您还按照第 52 页的“为 SWSE 配置 SSL 加密”中的介绍配置了您环境中的每个 SWSE。

为 Siebel 服务器 SSL 设置附加名称服务器参数

在按照本节中前面的介绍为 Siebel 服务器配置 SSL 之后，请更改以下配置：

- 通过 Siebel Server Manager，将每个 AOM 的通讯传输参数（别名是 CommType）设置为 SSL，即使用 SSL。（缺省设置是使用 TCP/IP。）
- 如果您以前使用 Microsoft Crypto 或 RSA 加密，则通过 Siebel Server Manager，将 Siebel Enterprise 的加密类型参数（别名是 Crypt）设置为无（而不是 MSCRYPTO 或 RSA）。

为 SWSE 配置 SSL 加密

本节介绍了如何配置 SWSE，以便将安全套接层 (SSL) 加密用于与 Siebel 服务器的 SISNAPI 通讯，并根据需要使用验证。

配置 Siebel 服务器与 Web 服务器之间的 SSL 通讯还需要您配置 Siebel Enterprise 或 Siebel 服务器以便使用 SSL，这在第 49 页的“为 Siebel Enterprise 或 Siebel 服务器配置 SSL 加密”中有介绍。

执行该过程将在 eapps.cfg 文件称为 [connmgmt] 的新部分中添加参数。例如，[connmgmt] 部分可能类似于：

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

该过程中提到的 eapps.cfg 文件参数的名称对应于 Siebel 服务器的名称服务器参数。

在运行该实用程序之后，对于任何使用 SSL 连接至 SWSE 的 AOM，您必须修改 ConnectString 参数，以指定 SSL 作为通讯类型（缺省情况下使用 TCP/IP），并指定“无”作为加密类型。例如，对于使用美国英语的 Siebel Sales，请修改 eapps.cfg 文件的 [/sales_enu] 部分中的参数，修改后可能类似于：

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

为 SWSE 运行 SSL 配置实用程序

本节介绍了为 SWSE 运行 SSL 配置实用程序，也就是 Siebel 软件配置实用程序 (Siebel Web Server Extension SSL)。

不管您是以 GUI 模式还是控制台模式运行 SSL 配置实用程序，该实用程序的提示都是相同的。然而，这两种模式下的一些用户界面元素是不相同的。

在 Windows 中，为 Siebel Enterprise 或 SWSE 配置 SSL 时始终使用 GUI 模式。在 UNIX 中，为 Siebel Enterprise 或 SWSE 初始配置 SSL 时使用 GUI 模式。然而，如果您以后在 UNIX 平台上单独运行 SSL 配置实用程序时，将使用控制台模式。

要为 SWSE 启用 SSL 加密

- 1 如果您要配置 SSL 验证，则在开始之前需要获取并安装所需的认证文件。
- 2 如果您要运行主要的 Siebel 软件配置实用程序以配置 SWSE，请首先指定您要为 Enterprise 部署 SSL，然后启动 SSL 配置实用程序，这在第 48 页的“为 Siebel Enterprise 和 SWSE 配置加密”中有介绍。
- 3 或者，为了直接在 Web 服务器机器上运行 SSL 配置实用程序，请根据以下介绍，直接启动 SSL 配置实用程序：

- 如果是 Microsoft Windows 平台，请打开 MS-DOS 窗口，并输入以下命令（以 GUI 模式运行实用程序）：

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

其中：

- SWEAPP_ROOT 是 SWSE 的安装目录
- language 是运行配置实用程序所要使用的语言（例如，ENU 代表美国英语）

- 如果是 UNIX 平台，请输入以下命令（以控制台模式运行实用程序）：

```
cd SWEAPP_ROOT
```

如果是 Bourne shell 或 Korn shell：

```
./siebenv.sh
```

（确保开始的句点 (.) 与 ./siebenv.sh 之间有空格。）

如果是 C shell：

```
source siebenv.csh
```

```
cd SWEAPP_ROOT/bin
```

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

其中：

- SWEAPP_ROOT 是 SWSE 的安装目录
- language 是运行此配置实用程序所要使用的语言（例如，ENU 代表美国英语）

- 4 指定认证文件和认证机构文件的名称。

eapps.cfg 文件中的等效参数是 CertFileName 和 CACertFileName。

- 5 指定私有密钥文件的名称以及私有密钥文件的口令，然后确认该口令。

您指定的口令将以加密的形式存储。

eapps.cfg 文件中的等效参数是 KeyFileName 和 KeyFilePassword。

- 6 指定是否需要同级验证。

同级验证表示只要启动连接，SWSE 必须根据 Siebel 服务器并通过认证进行自我验证。同级验证的缺省设置为 false。

注释：如果您为 SWSE 设置了同级验证，则还必须为连接的任何 Siebel 服务器设置同级验证。

eapps.cfg 文件中的等效参数是 PeerAuth。

- 7 指定是否需要同级认证验证。

同级认证验证执行反向 DNS 查找，以便分别验证 SWSE 机器的主机名与认证中的主机名是否相同。同级认证验证的缺省设置是 false。

eapps.cfg 文件中的等效参数是 PeerCertValidation。

- 8 如果您在运行 Siebel 软件配置实用程序时运行了 SSL 配置实用程序（如第 53 页的步骤 2 中所述），则返回至该流程，这在适用于您正在使用的操作系统的 *Siebel 安装指南* 中有介绍。

- 9 如果已直接运行 SSL 配置实用程序（如第 53 页的步骤 3 中所述），请复审设置，完成配置，然后重新启动 Web 服务器。

- 10 如有必要，请为您应用程序环境中的每个 SWSE 重复执行该过程。

请确保您还按照第 49 页的“为 Siebel Enterprise 或 Siebel 服务器配置 SSL 加密”中的介绍配置了您环境中的每个 Siebel 服务器。

为 Web 客户机配置加密

要使用加密，服务器和客户机都必须在它们的连接参数中强制实行加密。如果这些参数不匹配，则出现连接错误。

Siebel eBusiness Applications 支持下列类型的客户机：

- **Siebel Web 客户机。**该客户机在客户机端的标准浏览器中运行，而且不需要在客户机上安装任何附加的持续软件。

此类客户机使用 Siebel 网关名称服务器中为 Siebel 服务器存储的参数，并且使用 SWSE 和 Siebel 服务器上的配置文件。该 Web 客户机可以自动识别您对 SWSE 或 Siebel 服务器所做的加密设置。

有关详细信息，请参阅第 48 页的“为 Siebel Enterprise 和 SWSE 配置加密”。

- **Siebel 移动 Web 客户机。**该客户机专门用于本地数据访问，而不需要连接至服务器。客户机必须定期使用调制解调器、WAN、LAN 或其它网络访问 Siebel Remote 服务器，以执行数据同步。

有关为移动 Web 客户机与 Siebel Remote 服务器之间的信息传输设置加密的信息，请参阅第 55 页的“为移动 Web 客户机同步配置加密”。另请参阅 *Siebel Remote and Replication Manager Administration Guide*。

- **Siebel 专用 Web 客户机。**该客户机直接连接至 Siebel 数据库以执行所有数据访问。它在本地不存储任何 Siebel 数据。数据库除外，Siebel eBusiness Applications 体系结构的所有层都位于用户的个人计算机上。

- **Siebel Wireless 客户机。**使用 Web 浏览器和 Internet 服务实现的启用了无线技术的移动客户机。有关详细信息，请参阅 *Siebel Wireless Administration Guide* 和 *Siebel Sync Guide*。
- **Siebel Handheld 客户机。**Siebel 移动 Web 客户机的改进版本。在 *Siebel Bookshelf* 中提供了使用 Siebel Handheld 客户机的特定 Siebel 产品的文档。

有关前面介绍的一些 Siebel 客户机类型的详细信息，另请参阅 *部署计划指南*。

关于会话 Cookie

Siebel 服务器中的 AOM 通过 Web 服务器使用 TCP/IP 协议与 Siebel Web 客户机通讯，并建立了一个独立会话与处理每个客户机发来的连接请求。Siebel 应用程序使用会话 cookie 来跟踪会话的状态。

这些会话 cookie 只在浏览器会话期间一直存在，而在浏览器退出或用户注销时被删除。会话 cookie 在登录页启动的用户会话中附加请求和注销操作。

Siebel 应用程序不以纯文本形式在客户机的浏览器中存储会话 ID，而是创建加密的会话 ID，并给加密的会话 ID 附加加密密钥索引。会话 cookie 加密使用缺省的 56 位密钥。

在 Siebel Remote 中，加密算法和密钥交换与基于会话的组件相同。

会话 cookie 加密可防止 *会话电子欺骗*（根据无效的会话 ID 得出有效的会话 ID）。

有关会话 cookie 的详细信息，请参阅第 143 页的“Cookie 和 Siebel 应用程序”。

为移动 Web 客户机同步配置加密

您可以为移动 Web 客户机同步启用加密。在同步期间，DX 文件在 Siebel 服务器与移动 Web 客户机之间传输。DX 文件使用 SISNAPI 消息在 Siebel 服务器与移动 Web 客户机之间传输信息。

Siebel 移动 Web 客户机读取 Siebel 应用程序配置文件（例如，Siebel Sales 使用的 siebel.cfg 文件）中的配置参数，以确定在同步期间要使用的加密类型。加密选项被定义为 DockConnectionString 参数中的一个元素。

注释：安全套接层 (SSL) 不是 Siebel 专用 Web 客户机或 Siebel 移动 Web 客户机上的本地数据库同步所支持的加密方法。

有关 Siebel 移动 Web 客户机和 Siebel Remote 验证的信息，请参阅第 122 页的“移动 Web 客户机同步的验证”。

有关 Siebel 移动 Web 客户机的其它安全问题的信息（包括本地数据库加密），请参阅 *Siebel Remote and Replication Manager Administration Guide*。

要为移动 Web 客户机同步启用加密

- 1 打开您要编辑的 Siebel 应用程序配置文件。您可以使用任何纯文本编辑器更改该文件。

注释：在编辑配置文件时，不要使用在文件中添加附加的非文本字符的文本编辑器。

- 客户机的配置文件存储在客户机的 bin\LANGUAGE 目录中，其中 LANGUAGE 代表安装的语言包，例如，ENU 代表美国英语。
- 在应用程序中执行同步时（使用“文件”>“同步”>“数据库”），请从与应用程序关联的配置文件（例如，Siebel Sales 的 siebel.cfg）中读取配置。

有关处理 Siebel 应用程序配置文件的详细信息，请参阅 *Siebel System Administration Guide*。

- 2 在配置文件的 [Local] 部分中找到 DockConnString 参数。

该参数指定用于与客户机同步的 Siebel 服务器的名称。它使用以下格式：

siebel_server_name:network_protocol:sync_port_#:service:encryption

加密是 DockConnString 参数的第五个元素。该元素表示同步期间使用的加密类型。

以下是 DockConnString 参数值的一个示例：

APPSRV:TCPIP:40400:SMI:RSA

- 3 覆盖缺省值无，并将加密设置为 MSCRYPTO 或 RSA。

您指定的加密必须与 Siebel 服务器使用的加密匹配。如果未指定值（或者值是无），则不启用加密。例如，要配置 RSA 加密，您可以使用以下参数之一：

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

- 4 保存更改并退出文件。

有关编辑 Siebel Remote 和移动 Web 客户机配置文件的详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide* 和 *Siebel System Administration Guide*。

配置数据加密

您可以使用 Siebel Systems 提供的各种备选加密方法，对 Siebel 数据库中的敏感数据加密，例如，客户信用卡号。标准 Siebel eBusiness Applications 为 Siebel 数据库中的数据提供了能够进行 56 位 RC2 加密的选项。

关于 Siebel Strong Encryption Pack

Siebel Strong Encryption Pack 提供了更多的备选安全加密方法，其中包括：

- AES 加密（128，192 和 256 位），使用 AES 加密器
- RC2 加密（128 位），使用 RC2 加密器

AES 加密器和 RC2 加密器作为 Siebel 业务服务提供。（RC2 加密器支持 56 位加密，而不需要您安装 Strong Encryption Pack。）

您使用 Siebel Tools 为业务组件字段配置 AES 或 RC2 加密。有关详细信息，请参阅第 62 页的“配置业务组件加密”。

注释： Siebel Systems 通过单独的发行媒体提供 Siebel Strong Encryption Pack，并且需要将其单独安装到现有的 Siebel 服务器环境中。有关详细信息，请参阅 Siebel SupportWeb 上的 *Siebel Strong Encryption Pack Installation Guide*（适用于您的支持平台）。

警告： 如果要升级加密级别，请确保先阅读第 61 页的“数据加密的升级问题”，然后安装 Siebel Strong Encryption Pack。另请参阅适用于您正在使用的操作系统的 *升级指南*。

如何对数据加密

在为业务组件字段启用加密时，请通过指定的加密器（即 AES 加密器或 RC2 加密器），发送该字段中未加密的数据。加密器使用 keyfile 中存储的加密密钥对数据进行加密。

在对数据进行加密之后，数据被发送回业务组件字段以存储在数据库中。在用户访问该数据时，该加密的数据再次通过加密器发送以进行解密。数据解密时使用 keyfile 文件中曾用于加密的相同加密密钥。然后，解密的数据被发送回业务组件字段以显示在应用程序中。

keyfile 存储了许多用于数据加密和解密的加密密钥。keyfile 的文件名是 keyfile.bin，它位于 Siebel 服务器目录的 admin 子目录中。您可以在 keyfile 中添加附加的加密密钥。出于安全考虑，该文件使用了根据 keyfile 口令生成的加密密钥进行加密。要生成新的加密密钥以便对 keyfile 进行加密，请更改 keyfile 口令。

本节的其它部分介绍了如何使用“密钥数据库管理器”添加加密密钥以及更改 keyfile 口令。

数据加密的要求

字段数据加密要遵循以下限制和要求。

警告：一旦已设置并运行 Siebel 环境，请勿尝试更改加密密钥长度。如果要更改密钥长度，则需要重新生成所有密钥（包括 keyfile），以及对所有的适用数据重新加密，因此最好是在安装期间一次性设置密钥长度。但是，您可以使用支持的机制，明确升级您的加密密钥长度。

- 由于加密和解密对性能有影响，因此只有包含真正敏感数据（例如，信用卡号和社会保障号）的字段才应该加密。
- Siebel Assignment Manager 在分配之前不对数据进行解密。分配规则应该考虑此项限制。
- Siebel EIM 不会对使用 Siebel EIM 从 Siebel 数据库移入或移出的数据进行加密或解密。
- 要配置 128 位 RC2 加密（RC2 加密器）或任何 AES 加密选项（AES 加密器），您必须先安装 Siebel Strong Encryption Pack。Siebel eBusiness Applications 提供了 56 位 RC2 加密，不需要使用 Strong Encryption Pack。
- 在选择记录时，将检索、解密并显示已加密的字段数据。但是，用户不能对这些字段的未加密值执行查询或排序。加密字段的索引列没有提供任何便利，因为只对加密的值编排了索引。
- 加密数据在数据库中所需的存储空间最多可以达到未加密数据所需空间的 2.5 倍。您必须为受影响的列指定适当的数据长度。例如，长度为 10 个字符的数据在加密后可能使用 25 个字符，长度为 30 个字符的数据在加密后可能使用 75 个字符等等。
- 映射至相同数据库列的所有业务组件字段必须启用加密，并且必须使用本小节中介绍的统一的用户属性设置。不支持为不同的字段使用不同的加密算法或不同的密钥长度。
- 存储加密数据的任何业务组件字段必须处于活动状态。
- 移动 Web 客户机或专用 Web 客户机不支持字段级别的 AES 或 RC2 加密。
- Siebel Systems 不为数值数据提供 AES 或 RC2 加密。然而，您可以对数据库中作为字符串存储的任何信息使用加密器。要对计算的数值字段加密，请将该字段映射至字符串字段，然后将字符串字段的加密属性设置为 TRUE。
对于计算的字段，采用“获取值”和“设置值”方法在数值数据与字符串数据之间进行转换。只要业务组件使用计算的字段，加密和解密操作对于该应用程序则是透明的。这种解决办法的唯一限制是不能对计算的字段执行排序和直接查询。

使用密钥数据库管理器

“密钥数据库管理器”实用程序让您可以在 keyfile 中添加新的加密密钥以及更改 keyfile 口令。“密钥数据库管理器”实用程序的文件名是 keydbmgr.exe，它位于 Siebel 服务器目录的 bin 子目录中。

“密钥数据库管理器”程序可以在所支持的所有 Siebel 服务器平台上使用。

运行密钥数据库管理器

在运行“密钥数据库管理器”之前，请确保 Siebel 网关名称服务器正在运行。Siebel 业务组件使用的加密密钥高速缓存版本存储在名称服务器中。

“密钥数据库管理器”自动确定要使用哪一个加密器（RC2 加密器还是 AES 加密器）。

警告：您在更改 keyfile 之前必须先备份该文件。在 keyfile 丢失或被破坏时，如果没有备份的 keyfile，可能无法恢复加密的数据。

要运行密钥数据库管理器

- 1 关闭配置为使用加密的任何服务器组件。
有关关闭服务器组件的信息，请参阅 *Siebel System Administration Guide*。
- 2 从 Siebel 服务器目录的 bin 子目录中，使用以下语法运行 keydbmgr.exe:

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

 有关标志和参数的说明，请参阅第 59 页的表 2。
- 3 在出现提示时，输入 keyfile 口令。
 - 要添加新的加密密钥，请参阅第 59 页的“添加新的加密密钥”。
 - 要更改 keyfile 口令，请参阅第 60 页的“更改 Keyfile 口令”。
- 4 要退出该实用程序，请输入 3。
- 5 重新启动在第 59 页的步骤 1 中关闭的服务器组件。
有关启动服务器组件的信息，请参阅 *Siebel System Administration Guide*。

第 59 页的表 2 列出了“密钥数据库管理器”实用程序 keydbmgr.exe 的标志和参数。

表 2. 密钥数据库管理器标志和参数

标志	参数	说明
/u	<i>db_username</i>	数据库用户的用户名
/p	<i>db_password</i>	数据库用户的口令
/l	<i>language</i>	语种
/c	<i>config_file</i>	应用程序配置文件（例如，Siebel Sales 的 siebel.cfg）的完整路径

添加新的加密密钥

您可以在 keyfile 中添加新的加密密钥。AES 加密器或 RC2 加密器使用 keyfile 中的最新密钥对新数据加密，使用曾用于加密的原始密钥对现有数据解密，即使已经有更新的密钥可用。keyfile 中可存储的密钥数量不受限制。

警告：您在更改 keyfile 之前必须先备份该文件。在 keyfile 丢失或被破坏时，如果没有备份的 keyfile，可能无法恢复加密的数据。

要添加新的加密密钥

- 1 关闭配置为使用加密的任何服务器组件。
- 2 从 Siebel 服务器目录的 bin 子目录中运行 keydbmgr.exe。
有关详细信息，请参阅第 58 页的“运行密钥数据库管理器”。
- 3 要在 keyfile 中添加加密密钥，请输入 2。

- 4 输入一些 Seed 数据以提供用于生成新的加密密钥的随机数据。
密钥的长度至少必须为 7 个字符。
- 5 输入 3，退出该实用程序。
在退出“密钥数据库管理器”实用程序时，请密切监控可能产生的任何错误消息。如果出现错误，您可能需要恢复 keyfile 的备份版本。
- 6 将新的 keyfile 文件复制到 Siebel 服务器目录的 admin 子目录中，从而将该文件分布到所有的 Siebel 服务器中。
- 7 重新启动在 [第 59 页的步骤 1](#) 中关闭的服务器组件。
有关启动服务器组件的信息，请参阅 *Siebel System Administration Guide*。

更改 Keyfile 口令

使用根据 keyfile 口令生成的加密密钥对 keyfile 加密。为了防止擅自访问，您可以使用“密钥数据库管理器”实用程序更改 keyfile 口令。keyfile 将使用根据新的 keyfile 口令生成的新加密密钥重新进行加密。

在初次使用 AES 或 RC2 加密之前，您需要更改 keyfile 口令，因为所有版本的“密钥数据库管理器”实用程序在出厂时随附了相同的缺省口令。缺省的 keyfile 口令是 kdbpass。为了确保文件安全，请考虑定期更改 keyfile 的口令。

警告：您在更改 keyfile 之前必须先备份该文件。在 keyfile 丢失或被破坏时，如果没有备份的 keyfile，可能无法恢复加密的数据。

要更改 keyfile 口令

- 1 关闭配置为使用加密的任何服务器组件。
- 2 从 Siebel 服务器目录的 bin 子目录中运行 keydbmgr.exe 实用程序。
有关详细信息，请参阅 [第 58 页的“运行密钥数据库管理器”](#)。
- 3 要更改 keyfile 口令，请输入 1。
- 4 输入新的口令。
- 5 确认新的口令。
- 6 输入 3，退出该实用程序。
在退出“密钥数据库管理器”实用程序时，请密切监控可能产生的任何错误消息。如果出现错误，您可能需要恢复 keyfile 的备份版本。
- 7 将新的 keyfile 文件复制到 Siebel 服务器根目录的 admin 子目录中，从而将该文件分布到所有的 Siebel 服务器中。
- 8 重新启动在 [第 60 页的步骤 1](#) 中关闭的服务器组件。
有关启动服务器组件的信息，请参阅 *Siebel System Administration Guide*。

数据加密的升级问题

Siebel Strong Encryption Pack 将 Siebel 应用程序升级到 128 位、192 位或 256 位加密。该软件包包括一个升级实用程序（keydbupgrade.exe），该实用程序用于对 keyfile 进行解密（如果以前使用 56 位或 128 位 RC2 密钥加密），然后使用更长的密钥和更安全的加密算法对 keyfile 重新加密。

有关数据加密升级问题的详细信息，请参阅 Siebel SupportWeb 上的 *Siebel Strong Encryption Pack Installation Guide*（适用于您的支持平台）。另请参阅适用于您正在使用的操作系统的 *升级指南*。

支持的数据加密升级方案

下面概括介绍了支持的数据加密升级方案。

■ 从下面的加密升级到 128 位 RC2 加密：

- 没有加密
- 标准加密器加密（基于杂乱算法）
- 56 位 RC2 加密

■ 从下面的加密升级到 128 位 AES 加密：

- 没有加密
- 标准加密器加密（基于杂乱算法）
- 56 位 RC2 加密
- 128 位 RC2 加密

■ 从下面的加密升级到 192 位 AES 加密：

- 没有加密
- 标准加密器加密（基于杂乱算法）
- 56 位 RC2 加密
- 128 位 RC2 加密
- 128 位 AES 加密

■ 从下面的加密升级到 256 位 AES 加密：

- 没有加密
- 标准加密器加密（基于杂乱算法）
- 56 位 RC2 加密
- 128 位 RC2 加密
- 128 位 AES 加密
- 192 位 AES 加密

准备安装 Strong Encryption Pack

在安装 Strong Encryption Pack 之前，请执行以下步骤。

要准备安装 Strong Encryption Pack

- 1 从 Siebel Systems 获取 Siebel Strong Encryption Pack。
- 2 备份现有的 keyfile (keyfile.bin)。
- 3 运行“密钥数据库管理器”(keydbmgr.exe) 并更改 keyfile 口令。
- 4 安装 Siebel Strong Encryption Pack。
有关详细信息，请参阅 Siebel SupportWeb 上的 *Siebel Strong Encryption Pack Installation Guide*（适用于您的支持平台）。
- 5 运行 keydbupgrade 实用程序。
- 6 使用 srvrmgr 程序，更新 Enterprise Server 的数据库口令。
`change ent param password=keyfile_password`
- 7 重新启动服务器。

配置业务组件加密

本节介绍了如何使用 Siebel Tools 启用和禁用业务组件字段的加密。

有关执行本节中介绍的一些任务的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

Siebel Systems 提供了 AES 加密器和 RC2 加密器，让您可以对数据字段进行加密。这些加密器可用于 Siebel Strong Encryption Pack。

有关使用 AES 加密器或 RC2 加密器在 keyfile 中添加加密密钥以及更改 keyfile 口令的详细信息，请参阅第 57 页的“配置数据加密”。

设置加密用户属性

应用程序开发人员可以通过设置此处介绍的加密用户属性，对业务组件中的字段进行加密。如果开启加密，则对写入到字段的数据进行加密，并对从字段读取的数据进行解密。

要为业务组件字段开启加密

- 1 启动 Siebel Tools。
- 2 选择包含要加密字段的业务组件。
- 3 选择要加密的字段。
例如，在“报价”业务组件中，“信用卡号”字段具有用于加密的字段用户属性。

4 在字段用户属性中，设置以下加密值：

字段用户属性	值	说明
加密	Y	<ul style="list-style-type: none"> ■ Y 表示字段已加密。 ■ N 表示字段未加密。
加密服务名称	AES 加密器 RC2 加密器	设置要用于字段的加密类型。
加密密钥字段	<i>KeyIndexField</i>	<p>指定业务组件中存储加密密钥索引的字段。</p> <p>对于“报价”业务组件中的“信用卡号”字段，该用户属性设置为“信用卡号密钥索引”。</p>
加密只读字段	<i>CalculatedField</i>	<p>指定计算的字段，该字段确定加密字段中的数据是否为只读数据。</p> <p>将数据存储在只读表单中，以便允许其他人员在以后恢复数据。</p> <p>例如，对于“报价”业务组件中的“信用卡号”字段，该用户属性被设置为计算的字段“信用卡号 - 只读”。</p> <ul style="list-style-type: none"> ■ 如果加密或解密失败，“信用卡号 - 只读”的计算值是 Y (TRUE) — 该字段数据为只读。 ■ 如果加密或解密成功，计算的值是 N (FALSE) — 该字段数据可以编辑。 <p>如果您需要为另一个业务组件创建等效字段，请将其设置为计算的字段，并且不指定字段值。</p>

第 63 页的表 3 显示了业务组件的密钥索引字段的一些示例。

表 3. 加密密钥索引字段

业务组件	字段	密钥索引字段
FS 发票	信用卡号	信用卡号密钥索引
订单录入 - 订单	信用卡号	信用卡号密钥索引
个人付款资料	帐号	帐号密钥索引
报价	信用卡号	信用卡号密钥索引
配置收藏夹报价项目	信用卡号	(创建新字段)
获取用户数据	PayAcctNum	(创建新字段)

Unicode 支持的安全注意事项

Siebel eBusiness Applications 支持 Unicode。要全面遵循 Unicode 标准，请注意以下加密和验证问题。

在 Unicode 环境中使用非 ASCII 字符

- 对于数据库验证，用户 ID 和口令必须使用 Siebel 数据库支持的字符。
- 如果您登录到 Unicode Siebel 站点，然后使用 Web 单一登录访问不支持 Unicode 的第三方 Web 页，则可能会出现登录问题。确保可以通过 Web SSO 访问的所有应用程序都符合 Unicode 标准。

登录到 Siebel 应用程序

- 如果您为 Siebel 应用程序使用表单登录机制，请确保登录表单中使用的字符获得 Siebel 数据库的支持。
- 如果您为 Siebel 应用程序使用 URL 登录机制，登录表单中使用的字符则必须采用 ASCII。

加密的数据

Siebel 应用程序提供了 AES 和 RC2 加密，以便对敏感信息的字段数据（例如，信用卡号）进行加密。如果使用 Unicode 加密，您必须使用 AES 或 RC2 加密，而不是标准加密器（不再支持这种加密器）。

有关详细信息，请参阅第 57 页的“配置数据加密”。另请参阅适用于您正在使用的操作系统的 *升级指南*。

6

安全适配器验证

本章介绍如何为 Siebel 应用程序设置安全适配器验证。它包括以下主题：

- 第 65 页的“关于用户验证”
- 第 66 页的“验证策略的比较”
- 第 67 页的“关于 Siebel 安全适配器”
- 第 68 页的“配置数据库验证”
- 第 69 页的“关于 LDAP/ADSI 安全适配器验证”
- 第 72 页的“安装 LDAP Client 软件”
- 第 90 页的“实施 LDAP/ADSI 安全适配器验证”
- 第 91 页的“使用 LDAP/ADSI 配置实用程序”
- 第 97 页的“设置安全适配器验证：方案”
- 第 109 页的“配置口令散列处理”
- 第 113 页的“安全适配器部署选项”
- 第 120 页的“安全适配器和 Siebel 专用 Web 客户机”
- 第 122 页的“移动 Web 客户机同步的验证”

关于用户验证

验证是指证实用户身份的流程。Siebel Systems 支持多种验证用户的方法。您可以为 Siebel 应用程序用户选择安全适配器验证或 Web SSO 验证：

- **安全适配器验证。** Siebel 应用程序提供了一种安全适配器结构，支持多个不同的用户验证方案：
 - **数据库验证。** Siebel 应用程序支持根据基本数据库进行验证。在此体系结构中，安全适配器根据 Siebel 数据库对用户进行验证。Siebel Systems 提供了数据库安全适配器（被配置为缺省安全适配器）。
 - **LDAP/ADSI 验证。** Siebel 应用程序支持根据符合 LDAP 要求的目录或 Microsoft Active Directory Server (ADS) 进行验证。在此体系结构中，安全适配器根据目录对用户进行验证。Siebel Systems 提供了适用于 LDAP 的安全适配器和适用于 ADSI 的安全适配器。
 - **定制。** 您可以使用提供的定制适配器并配置 Siebel 应用程序使用该适配器。有关详细信息，请参阅第 19 页的“安全适配器 SDK”。
- **Web 单一登录 (Web SSO)。** 此方法使用外部验证服务，在用户访问 Siebel 应用程序之前对用户进行验证。在此体系结构中，安全适配器不对用户进行验证。安全适配器只是根据从外部验证服务接受的身份密钥，从目录中查找并检索用户的 Siebel 用户 ID 和数据库帐户。有关详细信息，请参阅第 7 章“Web 单一登录验证”。

您可以根据特定的应用程序要求，为您的环境中的每个应用程序单独选择用户验证方法。然而，如果跨所有 Siebel 应用程序使用统一的验证方法可以带来管理利润，因为采用统一方法可以降低部署的总体复杂性。Siebel 移动 Web 客户机只能使用数据库验证。

以下主题中的参考信息和过程信息与所有主要验证策略相关。这些主题中的许多特定信息适用于多个验证策略。有些信息同时适用于验证和用户管理。

- **与验证有关的配置参数。**配置参数值确定了验证体系结构组件的交互方式。有关配置参数的用途和设置其值过程的信息，请参阅附录 B “与验证有关的配置参数”。
- **Seed 数据。**在安装 Siebel eBusiness Applications 时，将为您提供与验证、用户注册和用户访问 Siebel 应用程序有关的 seed 数据。要了解有关所提供 seed 数据及查看和编辑 seed 数据过程的详细信息，请参阅附录 C “Seed 数据”。

验证策略的比较

第 66 页的表 4 重点介绍了每种验证方法的功能，以帮助指导您做出决策。每个基本策略都有多个选择可用。X 表示 Siebel Systems 支持此功能（与适用的第三方组件配合）。(X) 表示 Siebel Systems 不直接支持该功能，但是第三方组件可能支持。

注释：比较不适用于 Siebel 移动 Web 客户机，因为对于 Siebel 移动 Web 客户机，只有数据库验证适用。

表 4. 验证方法的比较

所需的部署或功能	数据库安全适配器	LDAP/ADSI 安全适配器	Web SSO	注释
不需要其它的基础设施组件。	X			
集中存储用户证书和角色。		X	X	
限制应用程序数据库中的数据库帐户数。		X	X	
支持动态用户注册。通过自行注册或管理视图实时创建用户。		X	(X)	如果是 Web SSO，用户注册则是第三方验证体系结构的职责。它不是由 Siebel 体系结构进行逻辑处理。
支持帐户策略。您可以设置口令过期、口令语法和帐户锁定等策略。	X	X	(X)	在 Siebel 数据库支持的 RDBMS 供应商中，只有采用支持的 IBM DB2 Universal Database 平台的供应商才会获得对帐户策略（仅限于口令过期）的支持。 如果是 Web SSO，则由第三方基础设施处理帐户策略的强制执行。
支持 Web 单一登录，即登录一次即可访问 Web 站点或门户中所有应用程序的功能。			X	

关于 Siebel 安全适配器

在安装 Siebel eBusiness Applications 时，将为用户验证提供这些安全适配器：

- 数据库安全适配器
- ADSI（活动目录服务接口）安全适配器
- LDAP（轻型目录访问协议）安全适配器

安全适配器是验证管理器的插件。安全适配器使用户输入（或由验证服务提供）的证书验证用户，并且在需要时允许用户访问 Siebel 应用程序。

LDAP 或 ADSI 目录存储了允许用户连接至 Siebel 数据库所需的信息，例如，数据库帐户、Siebel 用户 ID 或角色，此目录在 Siebel 数据库外部维护，并且由安全适配器进行检索。

通常，安全适配器验证流程包括以下主要阶段：

- 用户提供标识证书。
- 验证用户的身份。
- 用户的 Siebel 用户 ID 和数据库帐户从目录、Siebel 数据库或另一个外部来源（适用于 Web 单一登录）中检索。
- 用户被授予对 Siebel 应用程序和 Siebel 数据库的访问权限。

有关 Siebel 提供的安全适配器支持的第三方目录服务器的特定信息，请参阅 Siebel 应用程序在 Siebel SupportWeb 上的 [系统要求和支持的平台](#)。

您可以实施不是由 Siebel Systems 提供的其它安全适配器。要支持本节介绍的 Siebel 适配器的功能，您实施的适配器必须支持 Siebel 安全适配器软件开发套件。有关详细信息，请参阅第 19 页的“安全适配器 SDK”。

安全适配器可能采用以下与验证相关的模式之一操作，具体视您如何配置验证体系结构而定：

- **通过验证（LDAP 或 ADSI 安全适配器验证模式）。**安全适配器使用户输入的证书，验证用户是否存在于目录中。如果目录中存在用户，适配器将检索用户的 Siebel 用户 ID、数据库帐户，并根据需要检索一组角色，然后将这些信息传送到应用程序对象管理器 (AOM)，以便为用户授予访问 Siebel 应用程序和数据库的权限。此适配器功能通常用于实施安全适配器验证的情况。
- **不通过验证（Web SSO 模式）。**安全适配器将由独立的验证服务提供的身份密钥传送到目录。在使用身份密钥来识别目录中的用户之后，适配器将检索用户的 Siebel 用户 ID、数据库帐户，并根据需要检索一组角色，然后将这些信息传送到 AOM，以便为用户授予访问 Siebel 应用程序和数据库的权限。此适配器功能通常用于实施 Web SSO 的情况。

注释：安全适配器不为 Web SSO 提供验证。Web SSO 是指在您的 Web 站点上对用户进行验证，从而可以在此 Web 站点上访问其它应用程序（包括 Siebel 应用程序）的功能。但是，如果实施 Web SSO，则还必须部署安全适配器。

有关详细信息，请参阅第 7 章“Web 单一登录验证”。

在使用外部安全适配器验证（例如 LDAP 或 ADSI）的环境中，如果用户是在 Siebel 数据库中创建的，此安全适配器则可以在目录中创建记录。

配置数据库验证

如果您未使用 LDAP/ADSI 验证，则必须为每位用户创建唯一的数据库帐户。在管理员将新用户添加到数据库中时，“用户 ID”字段必须与数据库帐户的用户名相匹配。在用户登录到 Siebel 应用程序时，必须输入此数据库用户名和口令。

数据库验证流程

数据库验证流程分为以下阶段：

- 1 用户在 Siebel 应用程序登录表单中输入数据库帐户的用户名和口令。
- 2 Siebel Web Server Extension (SWSE) 将用户证书传送到 AOM，AOM 再将其传送到验证管理器。
- 3 如果为数据库安全适配器指定的数据源的 DBHashUserPwd 是 TRUE，验证管理器则对口令进行散列处理，并且将用户证书传送到数据库安全适配器。
- 4 如果用户证书与数据库帐户匹配，用户则登录到数据库中，并且通过其用户 ID 与该数据库帐户用户名相同的用户记录进行标识。

也就是说，数据库安全适配器通过尝试与 Siebel 数据库连接来验证每位用户的证书。

不可用于数据库验证的功能

其它验证策略提供的某些功能不可用于数据库验证，其中包括：

- 单一用户验证方法，此方法适用于 Siebel 应用程序和其它应用程序
- 用户自行注册（通常与客户应用程序配合使用）
- 外部授权的用户管理（通常与合作者应用程序配合使用）
- 从 Siebel 应用程序的“管理 - 用户”屏幕中创建用户

实施数据库验证

如果您实施数据库验证，它通常适用于 Siebel 雇员应用程序，例如 Siebel Call Center 或 Siebel Sales。

数据库验证被配置为缺省值，而且是本书中介绍的最容易实施的一种验证方法。

虽然可能不需要进行配置，但是可以使用 Siebel Server Manager 配置数据库安全适配器的参数。要配置参数，您应当为指定子系统（企业资料）确定参数值。如果是专用 Web 客户机，参数通过编辑应用程序配置文件进行配置。

数据库安全适配器是通过安全适配器模式 (SecAdptMode) 和安全适配器名称 (SecAdptName) 参数指定：

- 安全适配器模式必须设置为 DB（缺省值）。
- 安全适配器名称必须设置为 DBSecAdpt（缺省值）或设置为具有其它名称的安全适配器（企业资料或指定子系统）。

您可以为 Siebel Enterprise Server、某个特定的 Siebel 服务器、单个 AOM 组件或同步管理器组件（适用于 Siebel Remote）设置安全适配器模式和安全适配器名称参数。

警告：如果要配置服务器组件或 Siebel 服务器，以便使用其它数据库验证设置，该设置不同于在较高级别（即为 Siebel Enterprise 或 Siebel 服务器配置）配置的数据库验证设置，则应该创建新的数据库安全适配器。否则，您所做的设置将重新配置现有的安全适配器，不管此安全适配器是否正在使用。

有关数据库安全适配器参数的详细信息，请参阅附录 B “与验证有关的配置参数”。

管理员必须执行以下任务，以便向新用户提在数据库验证环境中访问 Siebel 应用程序和 Siebel 数据库的权限：

- 为用户创建数据库帐户。使用数据库管理功能，为每位用户创建数据库帐户。
- 在 Siebel 数据库中创建 Siebel 用户记录，记录的用户 ID 与数据库帐户的用户名相匹配。通过 Siebel Call Center 等雇员应用程序添加用户。

有关添加用户的信息，请参阅第 166 页的“用户的内部管理”。

如果实施数据库验证，则以下选项可用：

- **用户口令散列处理。**将未公开且已进行散列处理的口令保留到数据库帐户，而提供未进行散列处理的口令以供用户登录使用。如果启用用户口令散列处理，则在将用户口令与数据库中存储的已进行散列处理的口令相比较之前，先对用户的口令应用散列算法。有关详细信息，请参阅第 109 页的“配置口令散列处理”。

关于 LDAP/ADSI 安全适配器验证

Siebel eBusiness Applications 包括基于 LDAP 和 ADSI 标准的安全适配器，以允许客户使用 LDAP 目录产品或 Microsoft Active Directory Server (ADS) 执行用户验证。

在使用 LDAP 或 ADSI 验证的实施过程中，Siebel 提供的安全适配器（或符合 Siebel 要求的其它适配器）根据目录验证用户的证书，并从目录中检索登录证书。在此体系结构中安全适配器用作验证服务。

安全适配器验证为用户提供了对配置了安全适配器的 Siebel 应用程序的访问权限。您可能配置不同的 Siebel 应用程序以使用不同的安全适配器。

LDAP/ADSI 验证的优点

LDAP/ADSI 安全适配器验证可以提供以下好处：

- 在数据库外部执行用户验证
- 使用内部管理员、授权的管理员或自行注册的用户通过 Siebel 应用程序用户界面输入的新的或已修改的用户信息自动更新目录
- 用户自行注册
- 授权的管理员通过 Web 站点注册用户

LDAP/ADSI 验证流程

LDAP/ADSI 安全适配器验证流程中的步骤如下：

- 1 用户在 Siebel 应用程序登录表单中输入证书。
这些用户证书（用户名和口令）可能随配置安全适配器的方式而有所不同。例如，用户名可能是 Siebel 用户 ID 或标识符，例如帐户或电话号码。用户证书被传送到 Siebel Web Server Extension (SWSE)，然后传送到 AOM，AOM 又将用户证书传到验证管理器。
- 2 验证管理器确定如何处理用户证书并调用安全适配器根据目录对证书进行验证。
- 3 安全适配器将分配给该用户的 Siebel 用户 ID 和数据库证书返回给验证管理器。（如果使用了角色，则也会将角色返回给验证管理器。）
- 4 AOM（或请求验证服务的其它模块）使用返回的证书，将用户连接到数据库并标识用户。

LDAP/ADS 目录的要求

如果您在使用 LDAP 或 ADSI 验证，则必须提供自己的目录产品，它可以是 Siebel 提供的安全适配器支持的某个目录服务器，也可以是您选择的其它目录。有关 Siebel eBusiness Applications 支持的第三方产品的特定信息，请参阅 Siebel 应用程序在 Siebel SupportWeb 上的 [系统要求和支持的平台](#)。

- 如果您提供了某个 Siebel 支持的目录服务器（即支持的 LDAP 目录或 Microsoft ADS），则可以使用 Siebel 提供的安全适配器，也可以创建自己的符合 Siebel 要求的安全适配器。
- 如果提供的目录不是 Siebel 提供的安全适配器支持的那些目录，您则要负责实施支持该目录的安全适配器。

目录的数据要求

您的 LDAP/ADS 目录至少必须为每位用户存储下列数据：每个数据块都包含在该目录的一个属性中。

- **Siebel 用户 ID**。该属性值必须与 Siebel 数据库中用户人员记录的“用户 ID 字段”的值相匹配。它用于标识用户的数据库记录，以便于进行控制访问。
- **数据库帐户**。该属性值必须采用 `username=U password=P` 的形式，其中 `U` 和 `P` 是数据库帐户的证书。在两个密钥值对之间可以有任意空白，但是在每个密钥值对内部不能有空白。关键字 `username` 和 `password` 必须是小写。
- **用户名**。该属性值是传送给目录的用于标识用户的关键字。在简单实施中，它可能是 Siebel 用户 ID，并且可以不必是一个单独属性。
- **口令**。LDAP 服务器和 ADS 存储用户登录口令的方式不相同。
 - **LDAP**。口令是否存储在目录中取决于是否在使用 Web SSO。
 - 如果使用 LDAP 安全适配器通过 LDAP 目录进行用户验证，则必须将登录口令存储在某个属性中。
 - 如果通过验证服务进行用户验证（例如在 Web SSO 实施中），则不需要提供口令属性。
 - **ADS**。ADS 不会将口令作为属性存储。您可以在目录级别输入口令作为客户机的功能，ADSI 安全适配器也可以使用 ADS 方法来创建或修改口令。
 - 如果使用 ADSI 安全适配器通过 ADS 目录进行用户验证，则必须提供登录口令。
 - 如果通过验证服务验证用户（例如在 Web SSO 实施中），则不需要提供口令。

您可以使用其它用户属性存储所需的任何数据，（例如名字和姓氏）。您选择的验证选项可能需要您提交附加属性。

系统支持附加的数据类型（角色），但是不要求提供。角色是一种将 Siebel 职责与用户关联的备用方式。职责通常与 Siebel 数据库中的用户关联，但是他们可以存储在目录中。将角色值留为空白，以便从 Siebel 应用程序中管理职责。有关详细信息，请参阅第 119 页的“配置在目录中定义的角色”。

目录的用户权限

根据您的验证、注册策略以及在策略中使用的选项，您必须在目录中定义可读取目录中的用户信息、而且可以写入用户信息的用户。可在目录中读取或写入数据的用户具有对目录执行搜索和写操作的适当权限，这一点很重要。

注释：对于 ADSI 验证，建议使用“授权控制向导”，为 ADS 目录中的用户定义权限。

您必须创建以下用户：

- **应用程序用户。**您必须实施应用程序用户，只有这些用户才必须可以在目录中搜索和写入记录。有关详细信息，请参阅第 114 页的“配置应用程序用户”。

LDAP 安全适配器的要求

如果您将 LDAP 验证与任何支持的 LDAP 目录产品结合使用，则必须确认已安装 Siebel Systems 提供的 IBM LDAP Client 软件。如果尚未安装此 LDAP Client 软件，则必须手动进行安装。

- LDAP Client 软件必须安装在 LDAP 安全适配器工作的 Siebel 服务器机器上。
- 另外，如果您需要使用 Siebel 专用 Web 客户机的 LDAP 安全适配器功能，则必须在每台此类客户机机器上安装 LDAP Client 软件。

有关 IBM LDAP Client 的安装说明，请参阅第 72 页的“安装 LDAP Client 软件”。

ADSI 安全适配器的要求

如果您在支持的 Microsoft Windows 平台上运行 Siebel 服务器并且在使用 ADSI 验证，则必须符合此处介绍的要求。有关其中某些问题的详细信息，请参阅 Microsoft Active Directory 文档。

- 要允许用户设置或更改口令，ADSI 客户机软件必须可以建立与 Active Directory Server 的安全连接。您可以采用以下多种方式满足该要求：
 - 将所有系统作为单一 Microsoft Windows 域林的一部分包括在内
 - 配置信任关系
 - 配置安全套接层 (SSL)

同时还建议将所有的 Siebel 服务器和 Active Directory Server 置于同一个域林中。

注释：要通过 Siebel 客户机在 ADS 目录中执行用户管理，强烈建议您在服务器级别为 Active Directory 客户机与服务器之间的 SSL 通讯配置 ADS。这一通讯不同于安全适配器与目录之间的 SSL 通讯，它是通过 Siebel 应用程序进行配置，在第 116 页的“配置安全适配器的安全通讯”中有介绍。

- 必须通过 ADS 的 DNS 录入值正确配置网络上的 DNS 服务器。必须将使用 ADSI 安全适配器的客户机机器配置为可以从适当的 DNS 服务器中检索这些录入值。
- 如果您需要使用用于 Siebel 专用 Web 客户机部署的 ADSI 安全适配器功能，则必须在适用时，在每台此类客户机机器上安装 ADSI 客户机软件。此要求并非在所有支持的 Microsoft Windows 平台上都适用。

注释：有关 ADSI 客户机问题的详细信息，请在 Microsoft 的 Web 站点上搜索有关 Active Directory Client Extensions 的信息。

要确认成功安装 Siebel 支持的 ADSI 客户机

- 1 导航至 Microsoft Windows 操作系统安装位置中的 system32 子目录（例如 C:\WINDOWS\system32）。
- 2 验证 ADSI 客户机所需的每个 DLL 的正确版本已位于此子目录中。有关详细信息，请参阅供应商文档。
- 3 对于每个 DLL，请右键单击此文件并选择“属性”。
- 4 单击“版本”选项卡以查看版本号。

安装 LDAP Client 软件

本节提供了有关安装 IBM LDAP Client 和 IBM GSKit 的说明。

- IBM LDAP Client 在与 LDAP 安全适配器配合使用时，为 Siebel 应用程序提供了根据支持的 LDAP 目录服务器进行验证的能力。
- 您可以根据需要随 IBM LDAP Client 一起安装 IBM GSKit，它使 Siebel 应用程序可以通过 SSL 与支持的 LDAP 目录服务器进行通讯。

注释：您运行的 IBM 安装程序是指 IBM Directory Server、IBM Directory Server Client 或 Client SDK。在本文中，适用的客户机模块称为 IBM LDAP Client。Siebel eBusiness Applications 将 IBM LDAP Client 和 GSKit 软件与所有支持的 LDAP 目录产品结合使用，而不只是与 IBM Directory Server 结合使用。

在 Siebel 环境中安装 IBM LDAP Client 时，请考虑以下要求：

- IBM LDAP Client *必须* 安装在要使用 LDAP 安全适配器支持 LDAP 验证的每台 Siebel 服务器机器上。如果要支持 SSL，则还必须安装 IBM GSKit。IBM LDAP Client 软件可以在安装 Siebel 服务器之前或之后安装。
- 对于支持 LDAP 验证的 Siebel 专用 Web 客户机部署，IBM LDAP Client *必须* 安装在每本地客户机机器上。如果要支持 SSL，则还必须安装 IBM GSKit。IBM LDAP Client 软件可以在安装 Siebel 专用 Web 客户机之前或之后安装。

并且通常从 Siebel Systems 提供的 DVD 上执行安装。有关安装 Siebel 服务器、Siebel 专用 Web 客户机和其它模块的信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

本节还提供了安装 IBM GSK iKeyMan 的说明，IBM GSK iKeyMan 是一个用于生成认证数据库文件（CMS 文件）的实用程序。在 Siebel 应用程序通过 SSL 与 LDAP 目录服务器通讯时需要使用认证数据库文件。IBM GSK iKeyMan 可以安装在使用支持平台的任何一台机器上。如果您需要该模块，则只需在每次部署时安装一次该模块即可。

注释：本节中的叙述假定您安装了正确版本的 IBM 软件。有关第三方软件的详细信息，包括这些 IBM 模块的支持的版本号，请参阅 Siebel SupportWeb 上的 *系统要求和支持的平台*。另请参阅供应商文档。

使用 SSL 的安全 LDAP 的考虑事项

如果必须支持 SSL，IBM LDAP Client 要求必须安装 IBM GSKit。随 LDAP Client 提供的 LDAP 库和实用程序使用 SSL 库（如果存在）。SSL 库随 IBM GSKit 提供。

- 如果已经安装 IBM GSKit，LDAP 库将动态加载 SSL 库，并在配置 SSL 时使用这些库启用对 SSL 的支持。
- 如果尚未安装 IBM GSKit 并且 SSL 库不可用，除不支持 SSL 之外，LDAP 库的其它所有功能都一切正常。

如果将 SSL 与服务器验证配合使用，LDAP 应用程序可以通过安全加密的通讯连接，使用简单的 LDAP 验证（用户 ID 和口令）。SSL 的提供是为了在 LDAP 客户机应用程序与 LDAP 服务器之间建立安全的连接。另外，SSL 通过由 SSL 保护的连接提供数据保密性（加密）。服务器到客户机验证通过 X.509 认证完成。

注释：该安装指南假设 Siebel LDAP 验证现在或以后需要使用 SSL 功能。因此，LDAP Client 安装流程将 GSKit 安装作为其必备的组成部分包括在内。如果您有绝对把握相信绝对不会为 Siebel LDAP 验证开启 SSL，则不需要安装 GSKit。

根据以下小节，在不同操作系统平台上安装 IBM LDAP Client。

在 Windows 上安装 IBM LDAP Client 和 GSKit

本节介绍了在 Microsoft Windows 平台上安装 IBM LDAP Client 和 GSKit 的不同方法。

在 Windows 上使用 InstallShield GUI 安装

请按照以下过程，使用 InstallShield GUI 在 Windows 平台上安装 IBM LDAP Client 和 GSKit。

在以下过程中，如果在执行第 74 页的步骤 6 之后，安装程序退出但未显示语言窗口，则可能由以下原因之一导致：

- 视频驱动程序的级别太低。请更新视频驱动程序，以解决该问题。
- 在 TEMP 环境变量指定的目录中没有足够空间。确保该目录中至少有 100 MB 的可用空间。

注释：如果您使用 InstallShield GUI 来安装程序，则还必须使用 InstallShield GUI 来卸载程序。

要在 Windows 上安装 IBM LDAP Client 和 GSKit — InstallShield GUI

- 1 在您要安装 IBM LDAP Client 的计算机上，停止正在运行的任何程序并关闭所有窗口。
- 2 放入 DVD *Siebel eBusiness Applications, Base Applications for Windows*。然后，使用 Windows 资源管理器，从 DVD 根目录导航到文件夹 Windows\Server_Ancillary\ibmlldap51。
- 3 将目录中存储的文件解压缩，例如运行以下命令：


```
unzip ids510fp2refresh-windows-client-us.zip
```
- 4 导航到解压缩的目录，例如：


```
C:\Documents and Settings\Administrator\Local Settings\Temp\ids510fp2refresh-windows-client
```
- 5 导航到 ids_ismp 子目录。

6 运行 setup.exe。

此时将显示语言窗口。

7 选择在安装 IBM LDAP Client 期间要使用的语言。单击“确定”。

这是安装程序使用的语言，不是 IBM LDAP Client 程序本身使用的语言。您可以在第 74 页的步骤 13 中选择 IBM LDAP Client 使用的语言。

8 在“欢迎”窗口中，单击“下一步”。

如果您在系统中安装了旧版的 IBM LDAP Client，则会询问您是否要继续安装。

9 单击“是”，覆盖旧版本进行安装；或者单击“否”，退出安装程序。**10** 阅读软件许可协议之后，单击“我接受许可协议中的条款”选项，然后单击“下一步”。**11** 此时将显示预安装的组件和对应的版本级别。单击“下一步”。**12** 要安装到缺省目录，请单击“下一步”。要指定其它的安装位置，请单击“浏览”。

注释：请勿在安装目录名称中使用特殊字符，例如连字符 (-) 和句点 (.)。如果未使用缺省位置，请使用 ldap 或 ldapdir 等名称。请勿使用 ldap-dir 或 ldap.dir 等名称。

13 选择 IBM LDAP Client 软件要使用的语言。单击“下一步”。**14** 单击“定制”，并单击“下一步”。

此时将显示可用组件列表。

15 同时选择两个显示的选项：Client SDK (LDAP Client) 和 GSKit。单击“下一步”。

注释：如果您确信将永远不会为 LDAP Client 启用 SSL，则可以在此处撤消选择 GSKit。

此时将显示一个窗口，其中汇总了为安装和配置选择的组件。

16 如果要更改选择，请单击“上一步”。要开始安装，请单击“下一步”。**17** 安装文件之后，将打开 Client 自述文件。单击“下一步”。**18** 指定是现在还是以后重新启动计算机。单击“完成”。

您已经完成安装 IBM LDAP Client 和 IBM GSKit。

在 Windows 上使用 InstallShield 控制台安装

请按照以下过程，使用 InstallShield 控制台在 Windows 平台上安装 IBM LDAP Client 和 GSKit。使用 InstallShield 控制台的安装步骤与使用 InstallShield GUI 的安装步骤相似。

要在 Windows 上安装 IBM LDAP Client 和 GSKit — InstallShield 控制台

1 执行第 73 页的步骤 1 至第 73 页的步骤 5。**2** 在 ids_ismp 目录中，运行以下命令：

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

3 通过控制台而不是 GUI 执行其余的用户交互。

在 Windows 上使用 InstallShield 自动安装模式安装

请按照以下过程，使用 InstallShield 自动安装模式在 Windows 平台上安装 IBM LDAP Client 和 GSKit。下面分别提供了安装 IBM LDAP Client 和 IBM GSKit 的过程。

要在 Windows 上安装 IBM LDAP Client — InstallShield 自动安装模式

- 1 执行第 73 页的步骤 1 至第 73 页的步骤 5。

- 2 在 ids_ismp 目录中，运行以下命令：

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

该命令将 IBM LDAP Client 安装到 C:\Program Files\IBM\LDAP 目录中。

- 3 要更改安装位置，请修改文件 .\optionsFiles\InstallClient.txt。

例如，要将 LDAP Client 安装在 D:\Program Files\IBM\LDAP 目录下面，请编辑该文件以包括下列语句：

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

要在 Windows 上安装 IBM GSKit — InstallShield 自动安装模式

- 1 执行第 73 页的步骤 1 至第 73 页的步骤 4。

- 2 导航到 gskit 子目录。

- 3 运行以下命令：

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

该命令将 IBM GSKit 安装到 C:\Program Files\IBM\GSK6 目录中。

- 4 要更改安装位置，请修改 setup.iss 文件。

例如，要将 GSKit 安装在 D:\Program Files\IBM\GSK6 下面，请编辑该文件以包括下列语句：

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

要在 Windows 上卸载 IBM GSKit — InstallShield 自动安装模式

- 要卸载以前通过自动安装模式安装的 IBM GSKit，请在命令行处运行以下命令：

```
gsk6BUI LDAP
```

在 Windows 上验证安装

请按照以下过程验证已成功安装 IBM LDAP Client 和 GSKit。

要在 Windows 上验证安装

- 1 选择“开始”>“设置”>“控制面板”>“添加或删除程序”。
- 2 验证列出了 IBM LDAP Client 和 IBM GSKit 录入值。
- 3 验证安装了相应的库：
 - a 验证 ldap.dll 位于 *installation_location\LDAP\bin* 目录中。
 - b 验证 gsk6ssl.dll 位于 *installation_location\GSK6\lib* 目录中。

在 Windows 上使用 InstallShield 卸载程序

如果您使用了 InstallShield 安装 IBM LDAP Client 和 GSKit，则还必须使用它来卸载这些组件。

要使用 InstallShield 卸载 IBM LDAP Client 和 GSKit

- 1 选择“开始”>“设置”>“控制面板”>“添加或删除程序”。
- 2 选择 IBM Directory Server 5.1（或者您安装的对版本）。

在 Solaris 上安装 IBM LDAP Client 和 GSKit

本节介绍了在 Solaris 平台上安装 IBM LDAP Client 和 GSKit 的不同方法。

在系统上存在非 IBM LDAP 文件时执行安装

在 Solaris 机器上安装 IBM LDAP Client 期间，您可能遇到以下消息：

```
A non-IBM version of LDAP has been located on your system.
```

```
In order to use the command-line version of the IBM-supplied files, the existing files (ldapadd, ldapdelete, ldaplist, ldapmodify, ldapmodrdn, ldapsearch) must be relocated.
```

要在安装期间重新安置遇到的非 IBM LDAP 文件

- 1 指定要移入非 IBM LDAP 文件的新目录:

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

- 2 按 Enter 键接受缺省目录 (/usr/bin/ldapsparc)，或者键入新路径名称并按 Enter 键，又或者键入 q 并按 Enter 键以退出。

重新安置文件之后，您可能会看到以下附加消息：

```
## Processing system information.
```

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

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

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

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

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

```
## Verifying package dependencies.
```

```
## Verifying disk space requirements.
```

```
## Checking for conflicts with packages already installed.
```

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

```
/usr/bin/ldapadd
```

```
/usr/bin/ldapdelete
```

```
/usr/bin/ldapmodify
```

```
/usr/bin/ldapmodrtn
```

```
/usr/bin/ldapsearch
```

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

- 3 键入 y 并按 Enter 键继续安装。现有文件被移到以前指定的目录中，而 IBM LDAP Client 文件则安装在 /usr/bin 目录中。

在 Solaris 上使用控制台模式（交互）安装

请按照以下过程，使用交互控制台模式在 Solaris 平台上安装 IBM LDAP Client 和 GSKit。

下面分别提供了安装 IBM LDAP Client 和 IBM GSKit 的过程。

要在 Solaris 上安装 IBM LDAP Client — 控制台模式

- 1 以 root 身份登录。
- 2 放入 DVD *Siebel eBusiness Applications, Base Applications for Solaris*。然后，从 DVD 根目录导航到文件夹 Solaris\Server_Ancillary\ibmldap51。
- 3 将 ids510fp2refresh-solaris-client-us.tar 文件复制到至少有 50 MB 可用空间的空白目录中。
- 4 输入以下命令：

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

 将在当前位置创建 ids510fp2refresh-solaris-client 目录。
- 5 导航到 ids510fp2refresh-solaris-client 目录。
- 6 输入以下命令：

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

 此时将显示一个可用软件列表，例如：

```
application IBMldapc
IBM Directory Client
```
- 7 输入以下命令开始安装：

```
pkgadd -d 'pwd'/ldap.client_rted.pkg
```
- 8 根据需要对其提示符作出响应。
 在完成安装时，将出现一则与以下项类似的消息：

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

要在 Solaris 上安装 IBM GSKit — 控制台模式

- 1 执行第 78 页的步骤 1 至第 78 页的步骤 5。
- 2 输入以下命令：
 解压缩 gsk6bas.tar.Z
- 3 输入以下命令：

```
tar -xvf gsk6bas.tar
```
- 4 输入以下命令：

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

 此时将显示一个可用软件列表，例如：

```
application gsk6bas
Certificate and SSL Base Runtime (gsk6bas)
```
- 5 输入以下命令开始安装：

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

在 Solaris 上使用自动安装模式（非交互）安装

请按照以下过程，使用自动安装模式在 Solaris 平台上安装 IBM LDAP Client 和 GSKit。

要在 Solaris 上安装 IBM LDAP Client 和 GSKit — 自动安装模式

- 1 执行第 78 页的步骤 1 至第 78 页的步骤 5。
- 2 要添加 IBM LDAP Client，请输入以下命令：

```
pkgadd -d 'pwd' /ldap.client_rtd.pkg -r IBMldapc_response -a 'pwd'/adminfile -n IBMldapc
```
- 3 要添加 GSKit，请输入以下命令：

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

IBMldapc_response、gsk6bas_response 和 adminfile 文件位于 ids510fp2refresh-solaris-client 目录中。

在 Solaris 上验证安装

请按照以下过程验证已成功安装 IBM LDAP Client 和 GSKit。

要在 Solaris 上验证安装

- 1 使用 pkginfo 查看机器上是否安装了软件。输入以下命令：

```
pkginfo|grep IBMldapc
```

```
pkginfo|grep gsk6bas
```
- 2 验证存在 /opt/IBMldapc 和 /opt/ibm/gsk6 目录。
- 3 验证 libibmldap.so 文件位于 /opt/IBMldapc/lib 目录下。
- 4 验证 libgsk6ssl.so 文件位于 /opt/ibm/gsk6/lib 目录下。
- 5 验证 libibmldap.so 和 libgsk6ssl.so 的符号链接位于 /usr/lib 目录下。

在 Solaris 上卸载程序

如果您已经安装 IBM LDAP Client 和 GSKit，请使用以下过程卸载这些组件。

要在 Solaris 上卸载 IBM LDAP Client 和 GSKit

- 1 以 root 身份登录。
- 2 输入以下命令：

```
pkgrm IBMldapc
```

```
pkgrm gsk6bas
```

在 AIX 上安装 IBM LDAP Client 和 GSKit

本节介绍了在 AIX 平台上安装 IBM LDAP Client 和 GSKit 的不同方法。

在 AIX 上使用控制台模式（交互）安装

请按照以下过程，使用交互控制台模式在 AIX 平台上安装 IBM LDAP Client 和 GSKit。下面分别提供了安装 IBM LDAP Client 和 IBM GSKit 的过程。

要在 AIX 上安装 IBM LDAP Client — 控制台模式

- 1 以 root 身份登录。
- 2 放入 DVD *Siebel eBusiness Applications, Base Applications for AIX*。然后，从 DVD 根目录导航到文件夹 AIX\Server_Ancillary\ibmldap51。
- 3 将 ids510fp2refresh-aix-client-us.tar 文件复制到至少有 50 MB 可用空间的空白目录中。
- 4 输入以下命令：

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

将在当前位置创建 ids510fp2refresh-aix-client 目录。

- 5 导航到 ids510fp2refresh-aix-client 目录。

- 6 输入以下命令：

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

此时将显示一个可用软件列表，例如：

ldap.client.adt	5.1.0.0	I N usr
ldap.client.rte	5.1.0.0	I N usr,root
ldap.max_crypto_client.adt	5.1.0.0	I N usr
ldap.max_crypto_client.rte	5.1.0.0	I N usr

- 7 安装所需的软件包。输入以下命令：

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

其中

- -a 代表应用
- -c 代表提交
- -g 在有必要时安装必备文件
- -X 在需要时增加文件系统空间
- -d 代表设备

在完成安装时，系统将生成安装概要。

- 8 验证“结果”列显示成功加载所有文件。您也可以通过在命令提示符位置键入以下命令，验证已成功安装 IBM Directory Server:

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

显示的输出结果列出了以 ldap 开头的所有文件集，其中包括客户机、html 和消息文件集。例如:

```
ldap.client.adt          5.1.0.0  C  F   IBM Directory SDK
ldap.client.rte          5.1.0.0  C  F   IBM Directory Client Runtime
ldap.max_crypto_client.adt
ldap.max_crypto_client.rte
```

要在 AIX 上安装 IBM GSKit — 控制台模式

- 1 执行第 80 页的步骤 1 至第 80 页的步骤 5。

- 2 输入以下命令:

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

此时将显示一个所有可安装的 IBM GSK 软件包组成的列表。

```
gskak.rte                6.0.5.34                I N usr
#   AIX Certificate and SSL Base Runtime ACME Toolkit
```

- 3 在命令提示符位置，使用以下命令安装所需的软件包:

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

其中

-a 代表应用

-c 代表提交

-g 在有必要时安装必备文件

-X 在需要时增加文件系统空间

-d 代表设备

- 4 在完成安装时，系统将生成安装概要。验证“结果”列显示成功加载所有文件。您也可以通过在命令提示符位置键入以下命令，验证已成功安装 IBM LDAP Client:

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

输出结果列出了以 gsk 开头的所有文件集。例如:

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

在 AIX 上使用自动安装模式（非交互）安装

请按照以下过程，使用自动安装模式在 AIX 平台上安装 IBM LDAP Client 和 GSKit。

要在 AIX 上安装 IBM LDAP Client 和 GSKit — 自动安装模式

- 1 执行第 80 页的步骤 1 至第 80 页的步骤 5。
- 2 输入以下命令：

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

此命令将同时安装 IBM LDAP Client 和 GSKit（因为 GSKit 是 LDAP Client 的先决条件）。

在 AIX 上验证安装

请按照以下过程验证已成功安装 IBM LDAP Client 和 GSKit。

要在 AIX 上验证安装

- 1 使用 lspp 查看机器上是否安装了软件。输入以下命令：

```
lspp -L|grep ldap
```

```
lspp -L|grep gsk
```
- 2 验证存在 /usr/ldap 和 /usr/opt/ibm/gskak 目录。
- 3 验证 libibmldap.a 文件位于 /usr/ldap/lib 目录下面。
- 4 验证 libgsk6ssl.so 文件位于 /usr/opt/ibm/gskak/lib 下面。
- 5 验证 libibmldap.a 和 libgsk6ssl.so 的符号链接位于 /usr/lib 目录下面。

在 AIX 上卸载程序

如果您已经安装 IBM LDAP Client 和 GSKit，请使用以下过程卸载这些组件。

要在 AIX 上卸载 IBM LDAP Client 和 GSKit

- 1 以 root 身份登录。
- 2 输入以下命令：

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

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

AIX 上 IBM LDAP Client 安装的疑难解答

在 AIX 上安装 IBM LDAP Client 时，可能出现以下错误消息：

```
mkdir: 0653-358 Cannot create /home/ldap.
/home/ldap: The file system has read permission only.
chgrp: /home/ldap: A file or directory in the path name does not exist.
chown: /home/ldap: A file or directory in the path name does not exist.
cp: /home/ldap/.profile: A file or directory in the path name does not exist.
chmod: /home/ldap/.profile: A file or directory in the path name does not exist.
chgrp: /home/ldap/.profile: A file or directory in the path name does not exist.
chown: /home/ldap/.profile: A file or directory in the path name does not exist.
3004-721 Could not create user.
3004-703 Check "/usr/lib/security/mkuser.sys" file.
instal: Failed while executing the ldap.client.rte.pre_i script.
```

解决方案：如果不存在名为 ldap 的用户，则在安装期间自动创建该用户。有时安装可能失败，原因是无法成功创建 ldap 用户。在这种情况下，请首先手动创建 ldap 用户，然后安装 IBM LDAP Client。

在 HP-UX 上安装 IBM LDAP Client 和 GSKit

本节介绍了在 HP-UX 平台上安装 IBM LDAP Client 和 GSKit 的不同方法。

在 HP-UX 上使用 GUI 模式安装

请按照以下过程，使用 GUI 模式在 HP-UX 平台上安装 IBM LDAP Client 和 GSKit。

要在 HP-UX 上安装 IBM LDAP Client — GUI 模式

- 1 以 root 身份登录。
- 2 如果您已经远程登录到 HP-UX 机器，请为您的会话相应地设置 DISPLAY 环境变量，以便 SD 安装 GUI 显示在您的本地桌面上。
- 3 放入 DVD *Siebel eBusiness Applications, Base Applications for HP-UX*。然后，从 DVD 根目录导航到文件夹 HP-UX\Server_Ancillary\ibmlldap51。
- 4 将 ids510fp2refresh-hpux-client-us.tar 文件复制到至少有 50 MB 可用空间的空白目录中。
- 5 输入以下命令：
tar -xvf ids510fp2refresh-hpux-client-us.tar
- 6 导航到 ids510fp2refresh-hpux-client 目录。

7 输入以下命令：

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

此时将显示 .depot 文件中的可用软件列表，与以下项类似：

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

8 输入以下命令：

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

此时将显示 SD 安装 GUI。

9 选择 LDAPClient。**10** 选择 Actions -> Mark For Install。**11** 选择 Actions -> Install...。

在状态字段显示 Ready 时，表示已完成分析。

12 单击“确定”。**13** 单击“是”，开始安装。

在状态字段显示 Completed 时，表示已完成安装。

14 单击“完成”。**15** 退出 SD 安装 GUI。**16** 创建 LDAP Client 库的符号链接。

注释：HP-UX 上的 IBM LDAP Client 安装程序不会在 /usr/lib 目录中设置 LDAP Client 库的符号链接。如果未设置这些符号链接，则无法加载 Siebel LDAP 安全适配器。

要在 /usr/lib 中设置 LDAP Client 库的符号链接，请运行 ids510fp2refresh-hpux-client 目录中的 setlinkforibmldaplib.csh 脚本。由于该脚本采用 C shell 编写，请确保 /bin/csh 存在。请首先使用 chmod +x setlinkforibmldaplib.csh 命令将脚本更改为可执行文件，然后运行该文件。

要在 HP-UX 上安装 IBM GSKit — GUI 模式**1** 执行第 83 页的步骤 1 至第 83 页的步骤 6。**2** 输入以下命令：

```
解压缩 gsk6bas.tar.z
```

3 输入以下命令：

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

4 导航到 gsk6bas 目录。

5 输入以下命令：

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

此时将显示一个可用软件列表，与以下项类似：

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

6 输入以下命令：

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

显示 SD 安装 GUI。

7 选择 gsk6bas。**8** 选择 Actions -> Mark For Install。**9** 选择 Actions -> Install...。

在状态字段显示 Ready 时，表示已完成分析。

10 单击“确定”。**11** 单击“是”，开始安装。

在状态字段显示 Completed 时，表示已完成安装。

12 单击“完成”。**13** 退出 SD 安装 GUI。**14** 在 /usr/lib 目录中为 /usr/IBMldap/lib 中的每个库手动创建符号链接。

在 HP-UX 上使用自动安装模式（非交互）安装

请按照以下过程，使用自动安装模式在 HP-UX 平台上安装 IBM LDAP Client 和 GSKit。下面分别提供了安装 IBM LDAP Client 和 IBM GSKit 的过程。

要在 HP-UX 上安装 IBM LDAP Client — 自动安装模式

1 执行第 83 页的步骤 1 至第 83 页的步骤 6。**2** 输入以下命令：

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

3 创建 LDAP Client 库的符号链接。

注释：HP-UX 上的 IBM LDAP Client 安装程序不会在 /usr/lib 目录中设置 LDAP Client 库的符号链接。如果未设置这些符号链接，则无法加载 Siebel LDAP 安全适配器。

要在 /usr/lib 中设置 LDAP Client 库的符号链接，请运行 ids510fp2refresh-hpux-client 目录中的 setlinkforibmldaplib.csh 脚本。由于该脚本采用 C shell 编写，请确保 /bin/csh 存在。请首先使用 chmod +x setlinkforibmldaplib.csh 命令将脚本更改为可执行文件，然后运行该文件。

要在 HP-UX 上安装 IBM GSKit — 自动安装模式

- 1 执行第 83 页的步骤 1 至第 83 页的步骤 6。
- 2 输入以下命令：

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

在 HP-UX 上验证安装

请按照以下过程验证已成功安装 IBM LDAP Client 和 GSKit。

要在 HP-UX 上验证安装

- 1 使用 swlist 查看机器上是否安装了软件。输入以下命令：

```
swlist | grep LDAPClient
```



```
swlist | grep gsk6bas
```
- 2 验证存在 /usr/IBMldap 和 /opt/ibm/gsk6 目录。
- 3 验证 libibmldap.sl 文件位于 /usr/IBMldap 目录下面。
- 4 验证 libgsk6ssl.sl 文件位于 /opt/ibm/gsk6/lib 目录下面。
- 5 验证 libibmldap.sl 和 libgsk6ssl.sl 的符号链接位于 /usr/lib 目录下。

在 HP-UX 上卸载程序

如果您已经安装 IBM LDAP Client 和 GSKit，请使用以下过程卸载这些组件。

要在 HP-UX 上卸载程序

- 1 以 root 身份登录。
- 2 如果您已经远程登录到 HP-UX 机器，请为您的会话相应地设置 DISPLAY 环境变量，以便 SD Remove 窗口显示在您的本地桌面上。
- 3 输入以下命令：

```
swremove
```


此时将显示 SD Remove 窗口。
- 4 选择要删除的 LDAPClient 和 gsk6bas。
- 5 选择 Remove...

要在 HP-UX 上卸载程序 — 自动安装模式

- 1 执行第 86 页的步骤 1 至第 86 页的步骤 2。
- 2 要删除 LDAPClient，请输入以下命令：
swremove LDAPClient
- 3 要删除 GSKit，请输入以下命令：
swremove gsk6bas

安装和配置 IBM GSK iKeyMan

本节提供了有关安装和配置 IBM GSK iKeyMan 的信息。该模块只需在每次部署时安装一次。

运行 IBM GSK iKeyMan 的先决条件

- 需要安装 Java 1.3 或 1.3.1 版才能使 GSK iKeyMan 正常工作。（IBM GSK iKeyMan 不与 Java 1.4 配合使用。）

安装 IBM GSK iKeyMan

请按照适用于您的平台的 IBM GSKit 安装说明操作。

- 第 73 页的“在 Windows 上安装 IBM LDAP Client 和 GSKit”
- 第 76 页的“在 Solaris 上安装 IBM LDAP Client 和 GSKit”
- 第 80 页的“在 AIX 上安装 IBM LDAP Client 和 GSKit”
- 第 83 页的“在 HP-UX 上安装 IBM LDAP Client 和 GSKit”

为 IBM GSK iKeyMan 启用 CMS 功能

在您启动 GSK iKeyMan GUI 之前，请执行以下过程。

要设置 GSK iKeyMan 以支持 CMS 密钥数据库

- 1 安装 IBM 或等效的 JDK 1.3 或 1.3.1 版。
- 2 设置 JAVA_HOME，以指向安装 JDK 1.3 的目录。例如：
 - 在 Windows 上，设置 JAVA_HOME=C:\Program Files\IBM\Java13。
 - 在 UNIX 上，导出 JAVA_HOME=/usr/opt/IBMJava13。

注释：Microsoft Windows 平台上 Siebel 高交互客户机的 Java 要求与以上设置不兼容。如果需要在同一台机器上同时运行 Siebel 客户机软件和 IBM GSK iKeyMan，则可能需要在每次使用 IBM GSK iKeyMan 后重置 Java 的设置。有关 Siebel 高交互客户机的 Java 要求的详细信息，请参阅 *Siebel System Administration Guide* 中的浏览器配置信息。

3 从 `${JAVA_HOME}/jre/lib/ext` 目录中删除 `gskikm.jar` 和 `ibmjcaprovider.jar` 文件。

4 确保 `${JAVA_HOME}/jre/lib/ext` 目录中具有以下 jar 文件：

```
ibmjceprovider.jar
ibmpkcs.jar
ibmjcefw.jar
local_policy.jar
US_export_policy.jar
ibmjlog.jar
```

注释： IBM GSKit 将上述 jar 文件和 `ibmjsse.jar` 文件包括在 GSKit 安装路径中。这些文件位于 `GSK_installation_directory\classes\jre\lib\ext` 目录中。请将 GSKit jar 文件复制到 `${JAVA_HOME}/jre/lib/ext` 目录中。

5 注册 IBM JCE 和 IBM CMS 服务提供商：

更新 `${JAVA_HOME}/jre/lib/security/java.security` 文件，以便在 Sun 提供商之后添加 IBMJCE 提供商和 IBMCMS 提供商。例如：

```
"security.provider.1=sun.security.provider.Sun
"security.provider.2=com.ibm.spi.IBMCMSProvider
"security.provider.3=com.ibm.crypto.provider.IBMJCE
```

`GSK_installation_directory\classes\gsk_java.security` 中可以找到 GSKit 用户的 `java.security` 示例文件。

使用 IBM GSK iKeyMan 生成 CMS 文件

通过为 Siebel LDAP 安全适配器启用 SSL，在 Siebel 应用程序与其 LDAP 服务器之间将建立安全连接。

本手册未介绍如何为 LDAP 服务器启用 SSL。如果需要了解此信息，请参阅第三方 LDAP 服务器管理文档。本节假设 LDAP 服务器已启用 SSL — 也就是说，它接受 SSL 连接。

要为 Siebel LDAP 安全适配器启用 SSL，在运行 AOM 或其它组件的 Siebel 服务器机器上必须安装认证数据库文件，而且 AOM 或其它组件必须支持通过 LDAP 安全适配器进行 LDAP 验证。LDAP 安全适配器必须使用接受 SSL 连接的端口连接至 LDAP 服务器。

Siebel LDAP 安全适配器被建立在 IBM LDAP Client 顶层。IBM LDAP Client 要求认证数据库文件使用 CMS 文件格式。您可以使用 IBM GSK iKeyMan 生成 CMS 文件。

本节的其它部分提供了生成 CMS 文件以及为 Siebel LDAP 安全适配器启用 SSL 的详细说明。在完成时，您应该可以通过 LDAP 验证调用 Siebel 应用程序，并且可以预计 Siebel 应用程序与 LDAP 服务器之间的通讯将安全可靠。

关于生成 CMS 文件

CMS 文件应该包含那些认证机构的 CA 认证，这些机构已经向 LDAP 服务器发行服务器认证。

例如，假设将 Siebel 服务器配置为根据 LDAP 服务器 evlabnet9:392 进行验证。此 LDAP 服务器的服务器认证由认证服务器 evlab1 发行。因此，CMS 文件只需包含 evlab1 的 CA 认证，而不必包含 evlabnet9 的服务器认证。如果将 Siebel 服务器配置为根据从 evlab1 获取其服务器认证的另一个 LDAP 服务器进行验证，您则不必更新 CMS 文件。

生成 CMS 文件

请使用以下过程配置 IBM GSK iKeyMan，以支持 CMS 密钥数据库并生成 CMS 文件。

在执行此操作之前，请按照第 72 页的“安装 LDAP Client 软件”总主题下特定于平台的前面小节中的说明，安装 IBM LDAP Client 和 GSKit 软件。

要配置 GSK iKeyMan 以支持 CMS 密钥数据库

- 1 在您的机器上安装 IBM GSK iKeyMan。有关详细信息，请参阅第 87 页的“安装和配置 IBM GSK iKeyMan”。
- 2 确定哪一个 CA 为您的 LDAP 服务器发行了服务器认证并获得此 CA 认证。
- 3 将 CA 认证复制到已安装 GSK iKeyMan 的机器上。
- 4 使用 iKeyMan 创建新的 CMS 文件。
 - a 导航到 *GSK_installation_directory/bin*，其中 *GSK_installation_directory* 是同时安装了 IBM GSKit 和 GSK iKeyMan 的目录。
 - b 输入以下命令：


```
gsk6ikm
```
 - c 要创建新的 CMS 文件，请从密钥数据库的“文件”菜单中选择“新建”。
 - d 在对话框中，将密钥数据库类型指定为 CMS，并且指定文件名（使用文件扩展名 .kdb）以及要存储 CMS 文件的位置。单击“确定”。
 - e 在“口令提示”对话框中，输入并确认口令，然后选择“对文件隐藏口令”选项。单击“确定”。

隐藏口令选项将创建一个与 CMS 文件同名的文件，但是其扩展名为 .sth。该文件的创建位置与 CMS 文件相同。例如，CMS 文件的名称为 ldapkey.kdb，则将创建 ldapkey.sth 文件。
 - f 如果您要使用隐藏口令选项，请单击“确定”，以确认创建 .sth 文件。

新建的 CMS 文件将在 iKeyMan 主窗口中打开。

5 将一个或多个 CA 认证添加到在上一步创建的 CMS 文件中。

- a** 在“签署人认证”提示符位置单击“添加”。
- b** 在名为“从文件添加 CA 的认证”对话框中，指定数据类型，并指定认证文件名称以及要存储该文件的位置。如有必要，请使用“浏览”按钮，指定 CA 认证文件的位置。单击“确定”。
 - ☐ 如果采用 Base64 格式保存认证，请将数据类型指定为 Base-64 编码的 ASCII 数据。
 - ☐ 如果采用 DER 二进制格式保存认证，请将数据类型指定为 DER 二进制数据。
- c** 为要添加到 CMS 文件中的每个 CA 认证重复前面的子步骤。确保您选择了正确的数据类型。

注释：对于从新的 CA 获得其服务器认证的 LDAP 服务器，您只需将 CA 认证添加到 CMS 文件中，而不必为每个 LDAP 服务器创建新的 CMS 文件。

为 Siebel LDAP 安全适配器启用 SSL

请使用以下过程为 Siebel LDAP 安全适配器配置 SSL。有关 LDAP 安全适配器配置的详细信息，请参阅本章中的以下小节：

- 第 69 页的“关于 LDAP/ADSI 安全适配器验证”
- 第 90 页的“实施 LDAP/ADSI 安全适配器验证”（包括第 91 页的“使用 LDAP/ADSI 配置实用程序”）

要为 Siebel LDAP 安全适配器启用 SSL

1 将您刚刚在上一过程中创建的 ldapkey.kdb（CMS 文件）和 ldapkey.sth 文件复制到要运行 AOM 组件的 Siebel 服务器机器上，这些 AOM 组件将支持 LDAP 验证。

例如，您可能将这些文件复制到 \ssldb 目录中。

2 修改 LDAP 安全适配器配置。配置以下参数：

- port = 636
可以为 LDAP 服务器配置 SSL 端口。验证 LDAP 服务器用于 SSL 的实际端口号。
- sslatabase = CMS_file_path
指定 CMS 文件的绝对路径，例如 d:\ssldb\ldapkey.kdb。

3 重新启动 Siebel 服务器（如果您在 Siebel 服务器上配置 LDAP）。

实施 LDAP/ADSI 安全适配器验证

本节提供了实施 LDAP/ADSI 安全适配器验证的说明。

要为用户提供对实施 LDAP/ADSI 安全适配器或 Web SSO 验证的 Siebel 应用程序的访问权限，Siebel 应用程序必须可以检索以下信息：

- 用于访问数据库的证书
- 用户的 Siebel 用户 ID

任务概述

您必须执行以下任务，以设置典型的 LDAP/ADSI 安全适配器验证体系结构：

- 设置可从中为每个用户检索数据库帐户和 Siebel 用户 ID 的目录。
- 配置安全适配器的参数。您可以通过运行 LDAP/ADSI 配置实用程序，或直接使用 Server Manager 设置名称服务器的参数来执行此操作。
- 配置参数，以指定要使用哪一个安全适配器。您可以通过运行 LDAP/ADSI 配置实用程序，或直接使用 Server Manager 设置名称服务器参数来执行此操作。
- 仅限于专用 Web 客户机：配置应用程序配置文件中与安全有关的参数。
- 仅限于专用 Web 客户机：设置与安全有关的系统首选项。
- 在 SWSE 上的 eapps.cfg 文件中配置与安全有关的参数。
- 重新启动 Siebel 服务器和 Web 服务器。

LDAP/ADSI 配置实用程序可以修改名称服务器上的参数值。您还可以使用 Siebel Server Manager 修改名称服务器的参数。

对于专用 Web 客户机部署，LDAP/ADSI 配置实用程序可以修改应用程序配置文件中的参数值，例如 Siebel Call Center 的 uagent.cfg 文件。您还可以通过手动编辑配置文件的方式修改配置文件。

有关使用 LDAP/ADSI 配置实用程序的详细信息，请参阅第 91 页的“使用 LDAP/ADSI 配置实用程序”。

有关与安全有关的配置参数的详细信息，请参阅附录 B “与验证有关的配置参数”。

专用 Web 客户机和移动 Web 客户机的问题

在使用 Siebel 专用 Web 客户机或移动 Web 客户机部署时，验证可能遇到一些特殊的问题：

- 对于特定 Siebel 应用程序，用户在从 Siebel 专用 Web 客户机连接至服务器数据库时，采用的验证机制必须与 Siebel Web 客户机用户使用的验证机制相同。该机制可能是数据库验证，也可能是支持的外部验证策略，例如 LDAP 或 ADSI。
- 在从移动 Web 客户机连接至本地数据库时，移动用户必须使用数据库验证。有关本地数据库同步的验证选项的信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

使用 LDAP/ADSI 配置实用程序

Siebel Systems 提供了 LDAP/ADSI 配置实用程序，帮助您将 Siebel 应用程序配置为根据外部 LDAP 或 ADS 目录执行验证。

该实用程序提供了一个图形用户界面 (GUI) 用于更新配置参数，这些参数可能存储在 Siebel 网关名称服务器中，也可能存储在 Siebel 应用程序配置文件中（在配置 Siebel 专用 Web 客户机时）。

该实用程序随 Siebel 服务器一起安装。在安装和配置 Siebel Enterprise 时，您可以将该实用程序作为一个独立程序运行。

- 在 Windows 平台上，该实用程序以控制台模式运行。
- 在 UNIX 平台上，该实用程序以命令行模式运行。

LDAP/ADSI 配置实用程序包括用于多个 Siebel 模块的配置可执行程序（包括用于配置 Siebel Enterprise 和 SWSE 的主要 Siebel 软件配置实用程序）以及提供特定 LDAP/ADSI 配置功能的模型文件。

- 可执行程序位于 Siebel 服务器安装目录的 bin 子目录中，在 Microsoft Windows 平台上被命名为 ssincfgw.exe，在 UNIX 平台上被命名为 icfg。

- 模型文件位于 Siebel 服务器安装目录的 admin 子目录中，文件名是 secadpt.scm。

有关使用主要 Siebel 软件配置实用程序的信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

LDAP/ADSI 配置实用程序的全称是 Siebel 软件配置实用程序 - LDAP/ADSI 安全适配器配置。该名称出现在此实用程序的标题栏中（以控制台模式）。

在您配置 Siebel 网关名称服务器参数时，名称服务器必须正在运行。除此之外，没有其它运行该实用程序的特殊设置要求。

注释：如果该实用程序在本地而不是通过网络运行，其运行效果达到最佳。因此，建议您从 Siebel 服务器机器上运行该实用程序。

第 92 页的图 6 显示一个示例屏幕（适用于 Windows 平台）。

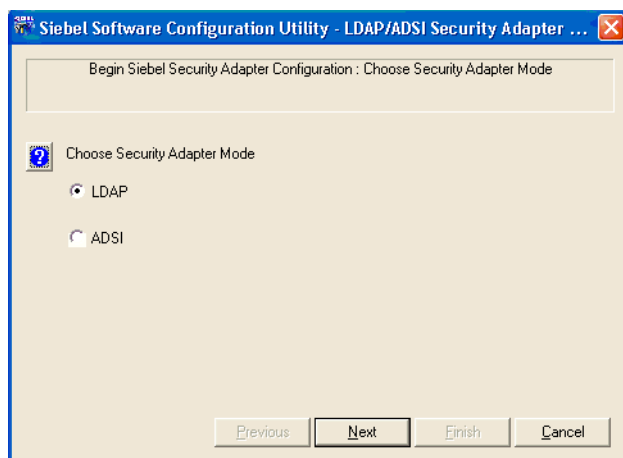


图 6. LDAP/ADSI 配置实用程序（Windows 版本）

如果指定 LDAP 或 ADSI 安全适配器模式，您所做的设置将为安全适配器模式 (SecAdptMode) 参数提供值（LDAP 或 ADSI）。

您还可以为 LDAP 或 ADSI 安全适配器指定名称。该设置为安全适配器名称 (SecAdptName) 参数提供值。您可以使用缺省名称或指定其它名称。如果尚不存在具有所指定名称的企业资料（指定子系统），该实用程序将使用此名称创建新的企业资料。

- 如果是 LDAP，缺省的安全适配器名称是 LDAPSecAdpt。

- 如果是 ADSI，缺省的安全适配器名称是 ADSISecAdpt。

您可以为 Siebel Enterprise Server、某个特定的 Siebel 服务器、单个 AOM 组件或同步管理器组件（适用于 Siebel Remote）设置安全适配器模式和安全适配器名称参数。

警告：如果要配置服务器组件或 Siebel 服务器，以便使用其它 LDAP 或 ADSI 验证设置，该设置不同于在较高级别（即为 Siebel Enterprise 或 Siebel 服务器配置）配置的验证设置，则应该创建新的 LDAP 或 ADSI 安全适配器。否则，您所做的设置将重新配置现有的安全适配器，不管此安全适配器是否正在使用。

您可以为特定 LDAP 或 ADSI 安全适配器（也就是为 LDAPSecAdpt 或 ADSISecAdpt 企业资料或使用非缺省名称的类似资料）定义附加的配置参数。一个为安全适配器定义参数示例就是，在您按安全适配器模式指定 LDAP 或 ADSI 时，安全适配器 DLL 名称 (SecAdptDllName) 参数将自动被设置。

注释：该实用程序为 Siebel 应用程序设置与验证有关的配置参数，但是不更改 LDAP/ADS 目录。确保您输入的配置信息与目录服务器兼容。

关于专用 Web 客户机的配置

在您配置 Siebel 专用 Web 客户机时（请参阅第 94 页的步骤 5），参数值被写入到您指定的配置文件中，例如 Siebel Call Center 的 uagent.cfg 文件。SecAdptMode 和 SecAdptName 在 [InfraSecMgr] 部分中定义。附加的 LDAP 或 ADSI 参数在 [LDAPSecAdpt]、[ADSIAdpt] 部分或使用非缺省名称的部分中定义。

警告：LDAP/ADSI 配置实用程序将改写，而不是附加配置文件中已存在的相关部分，例如 [LDAPSecAdpt] 或 [ADSIAdpt]。为防止丢失重要的配置信息，请在开始之前先备份文件。LDAP/ADSI 配置实用程序使用 filename.cfg_bak 的形式保存一份已修改的配置文件的完全副本，例如 uagent.cfg_bak。请勿使用此类名称手动创建备份文件，否则这些文件将被配置实用程序改写。

您可以通过添加使用非缺省名称的新部分，为安全适配器指定该名称。例如，您将 LDAPSecAdpt1 指定为安全适配器名称，这将是 SecAdptName 参数的值，并且将在配置文件中创建名为 [LDAPSecAdpt1] 的部分。在此情况下，名为 [LDAPSecAdpt] 的现有部分将不会被修改。

在配置一个文件之后，您可以将相关的参数部分复制到要使用相同设置的其它配置文件中。

有关详细信息，请参阅第 120 页的“安全适配器和 Siebel 专用 Web 客户机”，其中还包含配置文件中的示例部分。

配置 LDAP/ADSI 安全适配器的过程

下面介绍了使用 LDAP/ADSI 配置实用程序配置 LDAP 或 ADSI 安全适配器的过程。

在启动此实用程序之后，将显示一系列屏幕或提示。显示哪些项目以及如何显示这些项目，取决于您如何运行该实用程序以及进行了哪些选择。在输入信息后，请选择“下一步”，进入下一个屏幕。选择“上一步”，则返回到上一个屏幕。

要在运行 LDAP/ADSI 配置实用程序时创建详细的日志文件，请使用 -logevents all 标志运行该实用程序。日志文件名为 sw_cfg_util.log。例如，在 Windows 上运行以下命令：

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

注释：此过程中提到的配置参数都是为您要配置的适用的安全适配器而定义，但不包括安全适配器模式 (SecAdptMode) 和安全适配器名称 (SecAdptName) 参数。

要运行 LDAP/ADSI 配置实用程序

- 1** 在 Siebel 服务器机器上，更改为 `SIEBSRVR_ROOT\bin` 目录，其中 `SIEBSRVR_ROOT` 是 Siebel 服务器的安装目录。
 - 2** 请根据您的 Siebel 服务器平台执行以下操作之一：
 - 在 Microsoft Windows 实施中，选择“开始”>“运行”，然后键入：
`ssincfgw -l enu -f ../admin/secadpt.scm`
 - 在 UNIX 实施中，从命令行运行实用程序。键入：
`icfg -l enu -f ../admin/secadpt.scm`
 - 3 选择安全适配器模式。**选择安全适配器模式：LDAP 或 ADSI。您所做的设置将为安全适配器模式参数提供值。
 - 如果是 LDAP，安全适配器模式设置为 LDAP。
 - 如果是 ADSI，安全适配器模式设置为 ADSI。
 - 4 安全适配器名称。**指定安全适配器的名称。您可以接受缺省名称，也可以指定非缺省名称。您所做的设置将为安全适配器名称参数提供值。
 - 如果是 LDAP，缺省的安全适配器名称是 LDAPSecAdpt。
 - 如果是 ADSI，缺省的安全适配器名称是 ADSISecAdpt。
 - 5 是否配置专用 Web 客户机？**指定是否为专用 Web 客户机进行配置。
 - 如果选择“是”，实用程序将相关部分附加到指定的配置文件（例如 Siebel Call Center 的 `uagent.cfg` 文件）中或替换现有部分。请转到第 94 页的步骤 6。
 - 如果未选择“是”，实用程序在名称服务器中定义（适用于 Siebel Web 客户机部署）配置参数。您必须指定如何应用配置设置，并指定服务器连接信息。请转到第 94 页的步骤 7。

有关详细信息，请参阅第 93 页的“关于专用 Web 客户机的配置”和第 120 页的“安全适配器和 Siebel 专用 Web 客户机”。
 - 6 选择配置文件。**如果要为专用 Web 客户机配置，请指定要修改以包括指定设置的配置文件的名称。请转到第 95 页的步骤 11。
- 警告：**在指定现有的配置文件之前，请确保您已首先备份了该配置文件。有关详细信息，请参阅第 93 页的“关于专用 Web 客户机的配置”。
- 7 指定在哪一个级别启用 LDAP/ADSI 验证。**指定应该在哪个级别应用 LDAP/ADSI 安全适配器配置：
 - **Enterprise。**为 Siebel Enterprise Server 配置 LDAP/ADSI 安全适配器。
 - **Siebel 服务器。**为 Siebel 服务器配置 LDAP/ADSI 安全适配器。
 - **Siebel 服务器上的组件。**为单个 AOM 组件或同步管理器组件配置 LDAP/ADSI 安全适配器。
 - 8 输入服务器的连接信息：**
 - **网关名称服务器主机名。**Siebel 网关名称服务器机器的名称。如果网关名称服务器使用的端口不是缺省端口 (2320)，则还应该以 **机器名称: 端口号** 的形式包括此端口号（跟在冒号后面）。
注释：请勿使用端口号 2321 作为网关名称服务器的备用端口，因为此端口已用于 SCBroker 组件。
 - **Enterprise 名称。**Siebel Enterprise Server 的名称。

- 如果您已指定配置 Siebel Enterprise, 请转到第 95 页的步骤 11。
- 如果您已指定配置 Siebel 服务器或配置 Siebel 服务器上的组件, 请转到第 95 页的步骤 9。

9 Siebel 服务器名称。选择要应用安全适配器配置设置的 Siebel 服务器。

- 如果您已指定配置 Siebel 服务器, 请转到第 95 页的步骤 11。
- 如果您已指定配置 Siebel 服务器上的组件, 请转到第 95 页的步骤 10。

10 选择组件。选择要应用安全适配器配置设置的单个 AOM 组件或同步管理器。

11 输入与目录有关的配置信息:

- **目录服务器。**对应于 `ServerName` 参数。
 - 如果是 LDAP, 这是目录服务器的名称 (例如 `ldap.siebel.com`)。建议指定完全符合要求的服务器名称, 包括域名。
 - 如果是 ADSI, 这是目录服务器的名称 (例如 `adsi.siebel.com`) 或者只是域名。建议指定完全符合要求的服务器名称, 包括域名。(如果域包含多个目录服务器, 指定域名对于保持各个服务器间的负载平衡非常有用。)
- **端口号。**LDAP 目录服务器使用的端口号 (仅限于 LDAP)。标准传输使用端口 389 (缺省值), 安全传输使用端口 636。(ADS 端口作为目录安装的一部分, 而不是作为一个配置参数进行设置) 对应于 `Port` 参数。

12 输入与属性映射有关的配置信息:

- **用户名属性。**目录使用的 Siebel 用户 ID 属性。对于 LDAP 目录, 该属性的一个示例录入为 `uid`。对于 ADSI, 该属性的一个示例录入为 `sAMAccountName` (最长为 20 个字符)。如果您的目录为 Siebel 用户 ID 使用其它属性, 请改为输入该属性。对应于 `UsernameAttributeType` 参数。
- **口令属性。**目录使用的 Siebel 用户 ID 属性的口令 (仅限于 LDAP)。对应于 `PasswordAttributeType` 参数。

13 输入与属性映射有关的附加配置信息:

- **数据库帐户属性。**目录使用的数据库证书属性类型。对于 LDAP 和 ADSI, 该属性的一个示例录入为 `dbaccount`。如果您的目录为数据库帐户使用其它属性, 请改为输入该属性。对应于 `CredentialsAttributeType` 参数。要配置第 96 页的步骤 15 中指定的共享数据库帐户, 您必须已经定义该数据库帐户属性。

LDAP 和 ADSI 环境处理共享数据库帐户的方式各不相同。有关详细信息, 请参阅第 116 页的“配置共享数据库帐户”。

- **角色属性。**存储在目录中的角色的属性类型。只有在您使用目录中的角色时, 才需要提供该设置。对应于 `RolesAttributeType` 参数。

有关详细信息, 请参阅第 119 页的“配置在目录中定义的角色”。

14 配置应用程序用户:

- **应用程序用户的识别名 (DN)。**存储在目录中的应用程序用户的完整 DN (识别名)。在您指定应用程序用户时, 请加上引号。对应于 `ApplicationUser` 参数。

除了在此处定义应用程序用户之外, 您还必须在 LDAP/ADS 目录中创建应用程序用户。有关详细信息, 请参阅第 114 页的“配置应用程序用户”。

- **应用程序口令。**存储在目录中的应用程序用户的口令。对应于 `ApplicationPassword` 参数。确认口令。

15 共享数据库帐户的识别名 (DN)。为存储在目录中的共享数据库帐户指定完整 DN。在指定共享数据库帐户时，请加上引号。对应于 `SharedCredentialsDN` 参数。

配置共享数据库帐户时还会使用您在第 95 页的步骤 13 中定义的数据库帐户属性。有关详细信息，请参阅第 116 页的“配置共享数据库帐户”。

16 启用 Web 单一登录。指定是否要配置 Web 单一登录 (Web SSO)。对应于 `SingleSignOn` 参数。

- 如果选择“是”，则必须指定共享密钥。请转到第 96 页的步骤 17。

- 如果未选择“是”，请转到第 96 页的步骤 18。

有关配置 Web SSO 的详细信息，请参阅第 7 章“Web 单一登录验证”。

17 共享密钥。指定用于 Web SSO 的信任标记。对应于 `TrustToken` 参数。该值还对应于 SWSE 上 `eapps.cfg` 文件中的 `TrustToken` 参数，您必须手动将其添加到文件中。

18 传播更改。指定是否需要配置从 Siebel 专用 Web 客户机传播对 LDAP/ADS 目录所做更改的功能。对应于 `PropagateChange` 参数。

注释：如果指定该选项，则还必须将 `SecThickClientExtAuthent` 系统首选项设置为 `TRUE`。

有关详细信息，请参阅第 120 页的“安全适配器和 Siebel 专用 Web 客户机”。

19 Checksum。指定安全适配器 DLL 文件是否要使用 checksum 验证。对应于 `CRC` 参数。

有关详细信息，请参阅第 115 页的“配置 Checksum 验证”。

20 SSL 数据库。指定您要使用的 SSL 数据库的名称（*仅限于 LDAP*）。对应于 `SslDatabase` 参数。

有关详细信息，请参阅第 116 页的“配置安全适配器的安全通讯”。

21 散列数据库口令。指定是否要对数据库证书口令使用口令散列处理。对应于 `HashDBPwd` 参数。

有关详细信息，请参阅第 109 页的“配置口令散列处理”。

22 散列用户口令。指定是否要对用户口令使用口令散列处理。对应于 `HashUserPwd` 参数。

- 如果您为“散列用户口令”或“散列数据库口令”中的任何一个选项选择了“是”，则必须指定散列算法。请转到第 96 页的步骤 23。

- 如果您没有为“散列用户口令”或“散列数据库口令”中的任何一个选项选择“是”，请转到第 96 页的步骤 24。

23 散列算法。为数据库证书口令或用户口令指定要使用的散列算法。对应于 `HashAlgorithm` 参数。

- 指定 RSASHA1 (RSA SHA-1) 或 SIEBELHASH。（必须为新客户提供 RSA SHA-1。）

24 实施适配器定义的用户名。指定是否要实施适配器定义的用户名。对应于 `UseAdapterUserName` 参数。有关详细信息，请参阅第 117 页的“配置适配器定义的用户名”。

- 如果选择“是”，则必须指定 Siebel 用户 ID 属性。请转到第 96 页的步骤 25。

- 如果未选择“是”，请转到第 96 页的步骤 26。

25 Siebel 用户 ID 属性。为适配器定义的用户名指定 Siebel 用户 ID 属性。对应于 `SiebelUsernameAttributeType` 参数。

26 基本识别名 (DN)。指定在其中存储用户的基本识别名 (DN)。对应于 `BaseDN` 参数。

27 复审设置，然后单击“完成”以应用设置。

设置安全适配器验证：方案

本节在此以单一 Siebel 应用程序为例，提供了实施安全适配器验证的说明。此实施通过 Siebel SupportWeb 上的系统要求和支持的平台中介绍的所支持的目录之一使用 LDAP 安全适配器或 ADSI 安全适配器。

您的实施可能包括多个 Siebel 应用程序，而且您可能实施未在此处包括的组件和选项。

提供这些说明的目的是允许您确认已经成功地通过目录实施安全适配器。您应该首先在开发环境中实施验证体系结构，然后在生产环境中部署该体系结构。您可以重复执行此处的适用说明，以便为附加的 Siebel 应用程序提供安全适配器验证。

这些说明用于实施以下基本配置：

- 目录是 Siebel 支持的 LDAP 服务器或 Microsoft ADS。
- 使用 LDAP 安全适配器或 ADSI 安全适配器在验证管理器和目录之间通讯。
- 按用户的 Siebel 用户 ID 和口令对用户进行验证。

有关配置安全适配器验证的附加详细信息，另请参阅第 113 页的“安全适配器部署选项”。

有关实施用户验证时的特别注意事项的信息，请参阅第 243 页的“用户验证问题”。

如果您使用了不是由 Siebel Systems 提供的安全适配器，它必须支持 Siebel 安全适配器软件开发人员套件，这在第 19 页的“安全适配器 SDK”中有介绍。您必须修改以下实施的适用部分，以适应您的安全适配器需要。

在设置此安全适配器验证环境之前，必须首先完成以下安装：

- 已安装 Web 服务器。
- 已安装 LDAP/ADS 目录。
- 已安装 Siebel 应用程序，包括 Siebel 网关名称服务器和 Siebel 服务器。
- 已安装 LDAP/ADSI 客户机软件。
- URL 或超级链接可用，用户可以通过它访问您要配置的 Siebel 应用程序的登录表单。

注释：这些说明假设您已具备管理目录的经验。也就是说，您可以执行创建和修改用户存储子目录、创建属性、创建用户以及为用户提供权限等任务。

实施 LDAP/ADSI 验证的流程

您必须实施以下任务，以通过 Siebel 提供的安全适配器实施和测试 LDAP/ADS 目录。

- 1 创建数据库登录。请参阅第 98 页的“创建数据库登录”。
- 2 为目录中的用户设置属性。请参阅第 98 页的“设置 LDAP/ADS 目录”。
- 3 在目录中创建以下三个用户：普通用户、匿名用户和应用程序用户。请参阅第 99 页的“在 LDAP/ADS 目录中创建用户”。
- 4 在 Siebel 数据库中添加与目录中的两个用户相对应的记录。请参阅第 100 页的“在 Siebel 数据库中添加用户记录”。
- 5 编辑 eapps.cfg 文件参数。请参阅第 101 页的“编辑 eapps.cfg 文件中的参数”。
- 6 使用 Siebel Server Manager 编辑名称服务器参数。请参阅第 101 页的“使用 Siebel Server Manager 编辑参数”。

- 7 为 Siebel 专用 Web 客户机编辑 Siebel 应用程序的配置文件参数。请参阅第 105 页的“编辑应用程序配置文件中的参数”。
- 8 为 Siebel 专用 Web 客户机设置系统首选项。请参阅第 106 页的“设置专用 Web 客户机的系统首选项”。
- 9 重新启动 Siebel 服务器和 Web 服务器。请参阅第 106 页的“重新启动服务器”。
- 10 测试实施。请参阅第 106 页的“测试 LDAP/ADSI 验证系统”。

创建数据库登录

必须存在一个针对所有外部验证用户的数据库登录。该登录不能分配给任何真实人员。为实现这一点，在您安装 Siebel eBusiness Applications 时提供了一个 seed 数据库登录，这在第 261 页的“Seed 数据”中有介绍。它的登录名为 LDAPUSER，其缺省口令为 LDAPUSER，这些值都应该由管理员更改。如果该登录名不存在，请创建一个。

设置 LDAP/ADS 目录

要测试安全适配器，此测试实施可以：

- 通过目录验证用户。
- 允许自行注册。
- 将 Siebel 用户 ID 用作用户名。

注释：有关设置目录的详细信息，请复审第 70 页的“LDAP/ADS 目录的要求”。

确定基本识别名，它是目录中用于存储用户的子目录。有关详细信息，请参阅第 251 页的“Siebel 网关名称服务器参数”中的 BaseDN 参数说明。

您不能将单一 Siebel 应用程序的用户分布到多个基本 DN 中。然而，您可以将多个 Siebel 应用程序的用户存储在一个基本 DN 或用于 LDAP 的子结构（例如组织单位 (OU)）中。

在该示例中，用户存储在 LDAP 示例目录中域级下面的“人员”基本 DN 中，或者存储在 ADS 示例目录中域级下面的“用户”基本 DN 中。

定义要用于以下用户数据的属性。如果您不想使用现有属性，请创建新属性。在该示例中，提供了建议的属性。其中一些建议的属性是一个或多个支持目录中的缺省属性。

- **Siebel 用户 ID。**建议的属性：uid（适用于 LDAP）或 sAMAccountName（适用于 ADS）。
- **数据库帐户。**建议的属性：dbaccount。
- **口令。**建议的属性（仅适用于 LDAP）：userPassword。ADS 不使用属性来存储用户的口令。

您可以根据需要使用其它属性来表示名字、姓氏或其它用户数据。

在 LDAP/ADS 目录中创建用户

请在 LDAP/ADS 目录中创建在第 99 页的表 5 中介绍的三个用户。请根据此处的建议指定属性名称，例如，为 LDAP 目录指定 uid 和 userPassword。您输入的内容可能随您在第 98 页的“设置 LDAP/ADS 目录”中分配属性的方式而变化。

表 5. LDAP/ADS 目录中的记录

用户的类型	Siebel 用户 ID 属性 (适用于 LDAP 的 uid 或适用于 ADS 的 sAMAccountName)	口令 (适用于 LDAP 的 userPassword 属性 或适用于 ADS 的 ADS 口令)	数据库帐户属性 (dbaccount)
匿名用户	<p>为要实施的 Siebel 应用程序输入匿名用户记录的用户 ID。</p> <ul style="list-style-type: none"> 您可以为 Siebel 客户或合作者应用程序使用 seed 数据匿名用户记录。例如，您要实施 Siebel eService，请输入 GUESTCST。 您可以为 Siebel 雇员应用程序创建一个新用户记录或修改 seed 匿名用户记录。 即使应用程序不允许未注册的用户访问，您仍然需要提供匿名用户。 <p>有关详细信息，请参阅第 118 页的“配置匿名用户”。</p>	GUESTPW 或您选择的口令	username = LDAPUSER password=P
应用程序用户	APPUSER 或您选择的名称	APPUSERPW 或您选择的口令	数据库帐户不用于应用程序用户。
测试用户	TESTUSER 或您选择的名称	TESTPW 或您选择的口令	不需要为任何用户记录提供数据库帐户，但匿名用户除外。

注释：只建议特定的用户和口令录入值。您可以更改那些录入值。

该示例实施共享证书。适用于所有用户的数据库帐户存储在目录的一个对象中。在该示例中，共享数据库帐户存储在匿名用户记录中。数据库帐户必须与您为在第 98 页的“创建数据库登录”中介绍的外部验证用户保留的数据库帐户相匹配。P 符号表示该数据库帐户中的口令。

注释：在生产环境中，请勿将匿名用户用作包含共享证书的目录对象。

有关数据库帐户属性录入值的格式化要求的信息，请参阅第 70 页的“LDAP/ADS 目录的要求”。

警告：确保匿名用户和应用程序用户具有对目录的写权限。匿名用户必须具有写权限，因为这是自行注册的一个组件。应用程序用户还必须具有搜索所有用户记录的权限。

您可以根据需要为每位用户填写其它属性要目。

在 Siebel 数据库中添加用户记录

您必须在 Siebel 数据库中创建与您在第 99 页的“在 LDAP/ADS 目录中创建用户”中创建的测试用户对应的记录。

您必须确认第 262 页的“Seed 用户”中介绍的用于 Siebel 客户或合作者应用程序的匿名用户的 seed 数据记录存在。该记录还必须与您在第 99 页的“在 LDAP/ADS 目录中创建用户”中创建的匿名用户相匹配。

您可以为 Siebel 雇员应用程序修改 seed 数据匿名用户或创建新的匿名用户。要修改 Siebel 雇员应用程序的 seed 匿名用户，请在匿名用户的职责中添加雇员应用程序所需的任意视图，例如嵌入登录表单的主页视图。

要确认与数据库的连通性，您可以使用以下过程，为任何 Siebel 应用程序添加测试用户。然而，如果您要配置 Siebel 雇员或合作者应用程序，并且希望用户是雇员或合作者用户，请填写职位、部门和组织，请参阅第 166 页的“用户的内部管理”中有关添加此类用户的说明。

要在数据库中添加用户记录

- 1 以管理员身份登录 Siebel 雇员应用程序，例如 Siebel Call Center。
- 2 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 用户”>“用户”。
- 3 在“用户”列表中，创建新记录。
- 4 为测试用户填写以下字段，然后保存记录。使用所示的准则，所建议的录入值适用于本示例。您可以填写其它字段，但是这一操作不是必需的。

字段	示例录入值	准则
姓氏		必需。输入任何名称。
名字		必需。输入任何名称。
用户 ID	TESTUSER	必需。此录入值必须与目录中测试用户的 uid (LDAP) 或 sAMAccountName (ADS) 属性值相匹配。如果使用了其它属性，则必须与其它属性的值相匹配。
职责		必需。输入为所实施 Siebel 应用程序的注册用户提供的 seed 数据职责。例如，为 eService 输入 Web 注册用户。如果相应的 seed 职责不存在（例如 Siebel 雇员应用程序），请分配一个您创建的相应职责。
新职责		可选。输入为所实施 Siebel 应用程序的注册用户提供的 seed 数据职责。例如，为 eService 输入 Web 注册用户。该职责自动被分配给为此测试用户创建的新用户。

- 5 验证所实施 Siebel 应用程序的匿名用户的 seed 数据用户记录存在，这在第 262 页的“Seed 用户”中有介绍。
例如，您在实施 Siebel eService，请验证存在用户 ID 为 GUESTCST 的 seed 数据用户记录。如果记录不存在，请使用第 262 页的“Seed 用户”中的字段值创建该记录。您可以填写其它字段，但是这一操作不是必需的。

编辑 eapps.cfg 文件中的参数

按照第 101 页的表 6 中准则的指示，在 eapps.cfg 文件中提供参数值。

有关编辑 eapps.cfg 参数以及参数意图的详细信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。

表 6. eapps.cfg 文件中的参数值

部分	参数	准则
[缺省值]	SingleSignOn TrustToken UserSpec UserSpecSource	如果存在这些参数，请在每行开头加上分号，以标注每个参数。 如果这些参数出现在其它任何部分中，请执行相同操作。
特定于应用程序的部分，例如以下部分之一： [/eservice] [/callcenter]	AnonUserName	输入为所实施应用程序提供的 seed 数据用户记录的用户 ID，或者输入为匿名用户创建的用户记录的用户 ID。 此录入值还与目录中匿名用户记录的 uid (LDAP) 或 sAMAccountName (ADS) 录入值相匹配。例如，为 Siebel eService 输入 GUESTCST。
	AnonPassword	输入在目录中为匿名用户创建的口令。 注释： 通常对 eapps.cfg 文件应用口令加密。在此情况下，除非您通过 LDAP/ADSI 配置实用程序提供口令，否则您必须指定加密口令。请参阅第 33 页的“管理 eapps.cfg 文件中的加密口令”。
	ProtectedVirtualDirectory	如果存在该参数，请在每行开头加上分号，以标注该参数。

使用 Siebel Server Manager 编辑参数

您用于配置 LDAP 或 ADSI 安全适配器的多个与安全有关的配置参数都是在 Siebel 网关名称服务器中定义。您可以使用 Siebel Server Manager 配置这些参数。

请遵循提供的准则，按照列出参数的子部分中的说明设置每个参数。

有关这些参数的详细信息，请参阅第 251 页的“Siebel 网关名称服务器参数”。

Enterprise、Siebel 服务器或组件的参数

第 102 页的表 7 列出您可以在 Enterprise 级别、Siebel 服务器级别或组件级别设置的参数。您可以为其设置这些参数的适用组件包括所有 AOM 组件和同步管理器组件（适用于 Siebel Remote）。

在此方案中，请为适用的 AOM 组件设置参数，例如，为 Siebel Call Center 或 Siebel eService。

注释：您可以使用 Siebel Server Manager 修改这些配置参数，也可以使用 LDAP/ADSI 配置实用程序修改这些参数。有关详细信息，请参阅第 91 页的“使用 LDAP/ADSI 配置实用程序”。

表 7. Siebel 网关名称服务器参数（适用于 Enterprise、服务器或组件）

子系统	参数	准则
安全管理器	安全适配器模式 (SecAdptMode)	安全适配器模式的操作环境： <ul style="list-style-type: none"> ■ 如果是 LDAP，请指定 LDAP。 ■ 如果是 ADSI，请指定 ADSI。
	安全适配器名称 (SecAdptName)	安全适配器的名称。 <ul style="list-style-type: none"> ■ 如果是 LDAP，请指定 LDAPSecAdpt 或者您选择的其它名称。 ■ 如果是 ADSI，请指定 ADSISecAdpt 或者您选择的其它名称。 名称代表所指定安全适配器的企业资料（指定子系统）的别名。

AOM 组件的参数

第 102 页的表 8 列出了在 AOM 中设置的参数。

表 8. Siebel 网关名称服务器参数（适用于 AOM）

子系统	参数	准则
对象管理器	OM - 代理雇员	输入 PROXYE。
	OM - 用户名 BC 字段	在此方案中，请将该参数留为空白。

安全适配器的参数（资料/指定子系统）

第 103 页的表 9 列出了为要配置的特定安全适配器的企业资料（指定子系统）设置的参数。

对于此方案，您为以下某个适配器（定义为企业资料或指定子系统）配置参数：

■ **LDAP 安全适配器。**通常，该适配器的别名是 LDAPSecAdpt。

■ **ADSI 安全适配器。**通常，该适配器的别名是 ADSISecAdpt。

注释：您可以使用 Siebel Server Manager 修改这些配置参数，也可以使用 LDAP/ADSI 配置实用程序修改这些参数。有关详细信息，请参阅第 91 页的“使用 LDAP/ADSI 配置实用程序”。

表 9. Siebel 网关名称服务器参数（适用于企业资料/指定子系统）

参数	准则
安全适配器 DLL 名称 (SecAdptDllName)	<p>如果是 LDAP，请输入 <code>sscfldap</code>。</p> <p>如果是 ADSI，请输入 <code>sscfadsi</code>。</p> <ul style="list-style-type: none"> ■ 请勿包括文件扩展名（例如，不要为 LDAP 指定 <code>sscfldap.dll</code>）。 ■ 所指定值在内部被转换为适用于您的操作系统的实际文件名。
服务器名称 (ServerName)	如果是 LDAP 和 ADSI，请输入运行 LDAP 或 ADS 服务器的机器名称。
端口 (Port)	<ul style="list-style-type: none"> ■ 如果是 LDAP，示例录入值为 389。通常标准传输使用端口 389，安全传输使用端口 636。 ■ 如果是 ADSI，请在 ADS 目录级别设置端口号，而不是作为配置参数设置。
基本 DN (BaseDN)	<p>基本识别名是树中存储用户的根目录。在该目录下面可以直接或间接地添加用户。</p> <p>您不能将单一 Siebel 应用程序的用户分布到多个基本 DN 中。但是，您可以将用户分布到用于 LDAP 的多个子目录中，例如，组织单位 (OU)。</p> <p>LDAP 示例录入值（包括引号）：</p> <p><code>"ou=People, o=domainname"</code></p> <p>在该示例中，“o”表示“组织”，并且是该服务器的域名系统 (DNS) 名称，例如 <code>machine.company.com</code>。“ou”表示“组织单位”，它是存储用户的子目录的名称。</p> <p>ADSI 示例录入值（包括引号）：</p> <p><code>"CN=Users, DC=machinename, DC=domainname, DC=com"</code></p> <p>域控制器 (DC) 录入值是确定该服务器位置的嵌入域。公共名称 (CN) 录入值是目录中用户对象的特定路径。因此，请调整 DC 和 CN 录入值数量以代表您的体系结构。</p>

表 9. Siebel 网关名称服务器参数（适用于企业资料/指定子系统）

参数	准则
用户名属性类型 (UsernameAttributeType)	LDAP 示例录入值为 uid ADSI 示例录入值为 sAMAccountName 如果您在目录中为 Siebel 用户 ID 使用其它属性，请输入该属性名称。
口令属性类型 (PasswordAttributeType)	LDAP 录入值必须是 userPassword。如果指定了其它值，LDAP 安全适配器将不能正常工作。 ADS 不在属性中存储口令，因此该参数不用于 ADSI 安全适配器。
证书属性类型 (CredentialsAttributeType)	LDAP 示例录入值为 mail ADSI 示例录入值为 physicalDeliveryOfficeName 如果您在目录中为数据库帐户使用了其它属性，请输入该属性名称。
应用程序用户 (ApplicationUser)	LDAP 示例录入值（包括引号）： "uid=APPUSER, ou=People, o=domainname" ADSI 示例录入值（包括引号）： "CN=APPUSER, CN=Users, DC=machinename, DC=domainname, DC=com" 如果您在实施中为用户名使用了其它属性、为应用程序用户名使用了其它用户名或使用了其它的基本 DN，请调整录入值。
应用程序口令 (ApplicationPassword)	如果是 LDAP 和 ADSI，请输入分配给应用程序用户的 APPUSERPW 或口令。
共享证书 DN (SharedCredentialsDN)	■ LDAP 示例录入值（包括引号）： "uid=anonymous user User ID, ou=People, o=domainname" 例如： "uid=GUESTCST, ou=People, o=siebel.com" ■ ADSI 示例录入值（包括引号）： "CN=anonymous user User ID, CN=Users, DC=machinename, DC=domainname, DC=com" 例如： "CN=GUESTCST, CN=Users, DC=qa1, DC=siebel, DC=com"

编辑应用程序配置文件中的参数

请按照第 105 页的表 10 中准则的指示，在所实施 Siebel 应用程序的配置文件中提供参数值。

对于 Siebel 服务器上的配置文件，有些参数还适用于 AOM，因此也适用于 Siebel Web 客户机：[SWE] 部分中定义的参数。

在此上下文中，直接与安全适配器有关的小节中的参数仅适用于 Siebel 专用 Web 客户机。这些参数对应于第 102 页的表 7 和第 103 页的表 9 中列出的名称服务器参数。

注释：您可以使用文本编辑器更改应用程序配置文件，或者使用 LDAP/ADSI 配置实用程序进行更改。有关详细信息，请参阅第 91 页的“使用 LDAP/ADSI 配置实用程序”。

有关编辑应用程序的配置文件以及参数意图的详细信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。有关 Siebel 应用程序配置文件的列表，请参阅 *Siebel System Administration Guide*。

表 10. Siebel 应用程序配置文件参数

部分	参数	适用于 Siebel LDAP 和 ADSI 安全适配器的准则
[SWE]	AllowAnonUsers	如果是 LDAP 或 ADSI，请输入 TRUE。
	SecureLogin	输入 TRUE 或 FALSE。如果是 TRUE，则使用 HTTPS 传输从登录表单发出的登录请求 (HTTP POST)。 有关安全登录的其它要求的信息，请参阅第 140 页的“登录功能”中的安全登录主题。
[InfraSecMgr]	SecAdptMode	■ 如果是 LDAP，请指定 LDAP。 ■ 如果是 ADSI，请指定 ADSI。
	SecAdptName	■ 如果是 LDAP，请指定 LDAPSecAdpt 或者您选择的其它名称。 ■ 如果是 ADSI，请指定 ADSISecAdpt 或者您选择的其它名称。
[LDAPSecAdpt]	如果是参数，请参阅第 101 页的“使用 Siebel Server Manager 编辑参数”或附录 B “与验证有关的配置参数”	
[ADSIAdpt]	如果是参数，请参阅第 101 页的“使用 Siebel Server Manager 编辑参数”或附录 B “与验证有关的配置参数”	

设置专用 Web 客户机的系统首选项

如果您要为 Siebel 专用 Web 客户机配置 LDAP 或 ADSI 验证，则还要设置第 106 页的表 11 中所示的系统首选项。

有关设置系统首选项的详细信息，请参阅第 260 页的“系统首选项”。

表 11. 系统首选项

系统首选项	示例录入值	准则
SecThickClientExtAuthent	FALSE	将该系统首选项设置为 TRUE，以允许专用 Web 客户机使用安全适配器。

重新启动服务器

您必须在 Web 服务器机器上停止并重新启动以下 Windows 服务，以激活您对配置参数所做的更改。

- **IIS 管理服务和万维网发布服务。**停止 IIS 管理服务，然后重新启动万维网发布服务。由于万维网发布服务是 IIS 管理服务的子服务，因此还会启动 IIS 管理服务。
- **Siebel 服务器系统服务。**停止并重新启动 Siebel 服务器。有关详细信息，请参阅 *Siebel System Administration Guide*。

测试 LDAP/ADSI 验证系统

以下测试确认 Siebel 提供的安全适配器、您的 LDAP 或 ADS 目录以及您实施的 Siebel 应用程序是否相互配合以便：

- 提供用户可以登录的 Web 页。
- 允许已验证的用户登录。
- 允许用户匿名浏览（如果适合于 Siebel 应用程序）。
- 允许用户自行注册（如果适合于 Siebel 应用程序）。

第 107 页的图 7 显示包含嵌入的登录表单的 Siebel eService 主页。

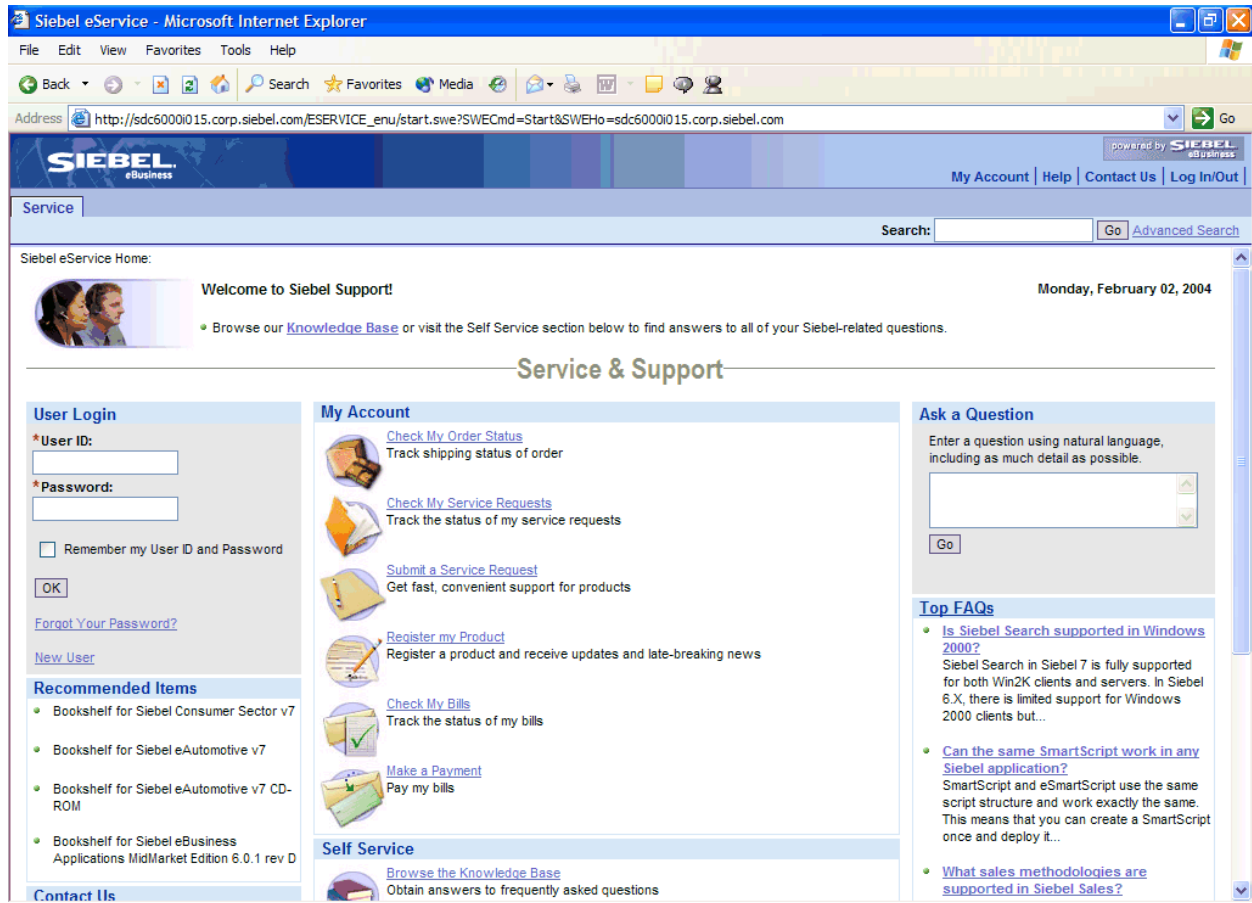


图 7. Siebel eService 主页中嵌入的登录表单

要测试 LDAP/ADSI 验证系统

- 1 在 Web 浏览器中，输入 Siebel 应用程序的 URL，例如：

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

此时应该出现一个包含登录表单的 Web 页，用于确认该匿名用户可以成功访问此登录页。

第 107 页的图 7 中的 Siebel eService 登录表单包括用户 ID 和口令字段。

- 2 各链接提供了匿名浏览视图的访问权限。其它一些链接需要您首先登录。

注释：雇员应用程序（例如，Siebel Call Center）通常不允许匿名浏览，而客户应用程序（例如，Siebel eService）允许这样做。

- 3** 导航回到包含登录文本框的 Web 页，然后使用您为测试用户创建的用户 ID 和口令登录。输入 TESTUSER 或您创建的用户 ID，并输入 TESTPW 或您创建的口令。

此时可能出现更多屏幕选项卡和其它应用程序功能，表明测试用户已经成功通过验证。数据库中的用户记录通过该注册用户的扩展职责提供视图。

- 4** 单击“注销”链接。
- 5** 重复第 107 页的步骤 1 以访问登录页。如果出现“新建用户”按钮，请单击该按钮。

注释：如果未出现“新建用户”按钮，并且没有进行附加配置，您的 Siebel 应用程序则不允许用户自行注册。

- 6** 在“个人信息”表单中，按以下所示填写必需字段，然后提交表单。您可以填写其它字段，但是这一操作不是必需的。

字段	说明
姓氏	必需。输入任何名称。
名字	必需。输入任何名称。
用户 ID	必需。输入简单且连续的用户 ID，每个用户的用户 ID 必须唯一。通常，由用户提供该用户 ID 以便登录。 根据您配置验证的方式，用户使用该标识符可能可以，也可能无法登录。
口令	可选（对于某些验证实施是必需项）。 输入简单且连续的登录口令。口令必须符合验证系统的语法要求，但是在该表中不会检查口令是否符合要求。 如果是 LDAP/ADSI 安全适配器验证，口令将传播至用户目录。如果是数据库验证，口令将传播至数据库。 有关用户验证体系结构的信息，请参阅第 6 章“安全适配器验证”。
验证口令	在需要提供口令时必需。
口令提示问题	必需。输入具有答案的问题短语。如果您以后单击“忘记口令？”，将会显示该短语，您必须输入正确的答案，才能收到新的口令。
口令提示问题答案	必需。输入被视为提示问题正确答案的单词或短语。

- 7** 导航到包含登录文本字段的页面。
- 8** 使用您在第 108 页的步骤 6 中创建的用户 ID 和口令登录。
- 您应该可以成功登录，并且可以在为注册用户提供的屏幕中导航。

配置口令散列处理

为了提高安全性，可以对用户口令或数据库证书口令进行散列处理。

与涉及到双向算法（加密和解密）的加密不同，散列处理使用单向算法。纯文本版本的口令使用 Siebel 实用程序进行散列处理，然后存储在数据库或外部目录中，例如 LDAP/ADS。在登录时，请提供纯文本版本的口令（例如由用户提供），系统会对口令进行散列处理并将其与存储的已进行散列处理的口令进行比较。

口令散列处理用于以下上下文中：

- **用户口令散列处理。**如果您在使用安全适配器验证（包括数据库、LDAP/ADSI 或定制的安全适配器），则可以对用户口令进行散列处理。

系统为每位用户维护未公开且已进行散列处理的口令，而用户使用未进行散列处理（纯文本）版本的口令登录。此口令将在登录时进行散列处理。

- **数据库证书口令散列处理。**如果您在使用安全适配器验证而不是数据库验证（包括 LDAP/ADSI 或定制的安全适配器），或者使用 Web SSO 验证，则可以对数据库证书口令进行散列处理。

系统为数据库帐户维护未公开且已进行散列处理的口令，而将未进行散列处理（纯文本）版本的口令存储在外部目录中，例如 LDAP 或 ADS。此口令将在登录时进行散列处理。

口令散列处理是一个至关重要的工具，用于防止未授权的用户绕过 Siebel 应用程序并使用 RDBMS 工具（例如，SQL*Plus）直接登录到 Siebel 数据库中。它还会防止使用通过网络截取的口令访问应用程序，因为在尝试登录时所截取的已进行散列处理的口令本身还会进行散列处理，从而导致登录失败。

证书口令散列处理可以防止用户使用通过擅自访问外部目录获取的口令，直接登录到 Siebel 数据库，因为未进行散列处理的口令与数据库中存储的已进行散列处理的版本不匹配。

有关配置每种口令散列处理的详细信息，请参阅第 111 页的“配置用户口令和证书口令散列处理”。

Siebel Systems 提供了称为 hashpwd.exe 的口令散列处理实用程序。缺省的散列算法是 RSA SHA-1。例如，使用 hashpwd.exe 实用程序的缺省选项 rsasha1，则将 siebel 散列处理为 6sxr7MWJDyNiMfw2f0cyo+g0Vcs=。有关运行 hashpwd.exe 的信息，请参阅第 112 页的“运行口令散列处理实用程序”。

注释：要求新客户使用 RSA-SHA1，强烈建议现有客户立即转移到 RSA-SHA1。

适用于所有 Siebel 提供的安全适配器以及您所实施的定制安全适配器的配置参数，指定了有效的口令散列处理设置。对于每个安全适配器，参数指定是否应该对用户口令和（或）证书口令使用口令散列处理，如果使用，应该使用哪一种散列算法。

如果是数据库验证，则为从数据库安全适配器引用的数据来源（而不是安全适配器的指定目录）指定相关参数。

如果是现有客户，Siebel 独有的散列算法（即杂乱算法，以前通过 encrypt.exe 实用程序可用）仍作为 hashpwd.exe 实用程序的一个选项提供。该选项也称为 siebelhash，它还可以被指定为适用的配置参数的值。这些参数包括适用于 LDAP/ADSI 安全适配器的 HashAlgorithm 和适用于数据来源的 DSHashAlgorithm（用于数据库验证）。

有关口令散列处理参数的详细信息，请参阅附录 B “与验证有关的配置参数”。

有关升级 Siebel 应用程序的详细信息，请参阅适用于您正在使用的操作系统的升级指南。

注释：有关在 eapps.cfg 文件中管理加密口令的信息，请参阅第 33 页的“管理 eapps.cfg 文件中的加密口令”。该处介绍的口令加密机制与本节中介绍的口令散列机制无关。

口令散列处理的登录方案

用户通过以下流程登录到 Siebel 应用程序：

- 1 用户使用包含未进行散列处理口令的用户证书登录。
- 2 AOM 接收用户证书，然后将其传送到验证管理器。
- 3 验证管理器根据安全适配器的配置，对口令进行散列处理。
- 4 在数据库验证环境中：
 - a 验证管理器将用户证书（用户 ID 和散列的口令）传送给数据库安全适配器。
 - b 数据库安全适配器验证散列的口令与数据库中存储的用户散列口令相匹配。它通过尝试连接至数据库服务器来对证书进行验证。安全适配器通过验证管理器向 AOM 确认证书有效。
- 5 在 LDAP/ADSI 验证环境中：
 - a 验证管理器将用户证书（包括已进行散列处理的口令）传送到 LDAP/ADSI 安全适配器。
 - b LDAP/ADSI 安全适配器验证已进行散列处理的口令与目录中为该用户存储的已进行散列处理的口令相匹配，然后通过验证管理器将数据库帐户和 Siebel 用户 ID 返回到 AOM。
- 6 AOM 为此用户启动 Siebel 应用程序会话。

口令散列处理的使用准则

为 Siebel 应用程序使用口令散列处理的准则包括以下项：

- 口令散列实用程序 hashpwd.exe 不会自动将已进行散列处理的口令存储在 Siebel 数据库或 LDAP/ADS 目录中。管理员负责定义和存储已进行散列处理的口令。已进行散列处理的口令存储在以下位置之一：
 - 在数据库验证环境中，它被设置为数据库帐户的有效口令。
 - 在 LDAP/ADSI 验证环境中，它存储在为用户口令指定的属性中。
- 为用户提供未进行散列处理的口令版本以便在登录时使用。
- 所存储的口令首先必须采用适用于验证流程中的口令的相同散列算法（通常是 RSA SHA-1）进行散列处理。
- 但是，存储在 Siebel 数据库以外的数据库证书口令应该以未进行散列处理的形式存储，因为此类口令将在验证流程中进行散列处理。
- 在数据库验证中，登录到数据库的 Siebel 服务器组件必须使用 Siebel 数据库中存储的已进行散列处理的口令值。否则，组件登录将失败。

例如，在您运行“生成触发器” (GenTrig) 组件时，为 PrivUserPass 参数（与 PrivUser 参数一起使用）提供的值必须是已进行散列处理的口令值。
- 必须为将配合使用的所有 Siebel Enterprise 组件统一指定口令散列处理。例如，受 AOM 负载平衡支配的所有 Siebel 服务器必须使用相同的安全适配器设置，其中包括那些口令散列处理的设置，否则组件登录将失败。

- 如果是 Siebel 移动 Web 客户机，对本地数据库口令应用的口令散列处理具有以下要求：
 - 在提取用户的本地数据库时，必须将服务器组件“数据库提取”（别名为 DbXtract）的参数加密客户机数据库口令（别名为 EncryptLocalDbPwd）设置为 TRUE。有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。
 - 数据库安全适配器必须对移动 Web 客户机有效，而且必须为安全适配器指定的数据来源相应地设置 DSHashUserPwd 和 DSHashAlgorithm 参数。有关详细信息，请参阅第 68 页的“配置数据库验证”和第 256 页的“Siebel 应用程序配置文件参数”。

配置用户口令和证书口令散列处理

请使用以下过程，对用户口令或数据库证书实施口令散列处理。

根据您所使用的验证方法，用户口令和数据库证书帐户口令可能存储在第 110 页的“口令散列处理的使用准则”中介绍的位置。

注释：以下过程中的某些步骤（例如，使用 Siebel Server Manager 设置配置参数值的步骤）也可以通过 LDAP/ADSI 配置实用程序来完成。有关详细信息，请参阅第 91 页的“使用 LDAP/ADSI 配置实用程序”。

配置用户口令散列处理

请使用以下过程配置用户口令散列处理。

要实施用户口令散列处理

- 1 为每位用户创建并记录用户名和口令。
- 2 要对一个或多个口令进行散列处理，请在命令提示符位置运行 hashpwd.exe 实用程序。有关命令语法的选项，请参阅第 112 页的“运行口令散列处理实用程序”。
- 3 请为每位用户执行以下操作：
 - 在数据库验证环境中，将数据库帐户的证书设置为用户名和已进行散列处理的口令。
有关设置数据库帐户证书的信息，请参阅 RDBMS 文档。
 - 在 LDAP/ADSI 验证环境中，将目录属性中的用户名和口令值设置为该用户名和已进行散列处理的口令。
- 4 使用 Siebel Server Manager 为用户口令散列处理配置安全适配器。
 - 对于数据库安全适配器（通常为 DBSecAdpt）：
 - 将 DataSourceName 参数设置为适用的数据来源的名称（例如，ServerDataSrc）。
 - 对于适用的数据来源，将 DSHashUserPwd 参数设置为 TRUE。
 - 对于适用的数据来源，将 DSHashAlgorithm 参数设置为 RSASHA1（这是缺省值）或 SIEBELHASH（Siebel 独有的算法）。
 - 对于 LDAP 或 ADSI 安全适配器（通常为 LDAPSecAdpt 或 ADSISecAdpt）：
 - 将 HashUserPwd 参数设置为 TRUE。
 - 将 HashAlgorithm 参数设置为 RSASHA1（这是缺省值）或 SIEBELHASH（Siebel 独有的算法）。
- 5 向每位用户提供用于登录的用户名和纯文本口令。

配置数据库证书口令散列处理

请使用以下过程配置数据库证书口令散列处理。

要实施数据库证书口令散列处理

- 1 为每个适用的数据库帐户创建并记录登录名和口令。
- 2 要对一个或多个口令进行散列处理，请在命令提示符位置运行 `hashpwd.exe` 实用程序。有关命令语法的选项，请参阅第 112 页的“运行口令散列处理实用程序”。
- 3 为每个数据库帐户，将已进行散列处理的口令分配给其对应的数据库帐户。
有关设置数据库帐户证书的信息，请参阅 RDBMS 文档。
- 4 在 LDAP/ADS 目录中，为包含数据库帐户的属性指定未进行散列处理的口令版本。
有关目录中所需属性的信息，请参阅第 70 页的“LDAP/ADS 目录的要求”。
- 5 使用 Siebel Server Manager 为证书口令散列处理配置安全适配器。
 - 对于 LDAP 或 ADSI 安全适配器：
 - 将 `HashDBPwd` 参数设置为 `TRUE`。
 - 散列算法将基于您以前在配置用户口令散列处理时指定的 `HashAlgorithm` 参数设置。

运行口令散列处理实用程序

要对口令进行散列处理，请运行 `hashpwd.exe` 实用程序，该实用程序位于 `SIEBSRVR_ROOT\admin` 或 `SIEBEL_CLIENT_ROOT/bin` 目录中，这两个目录代表 Siebel 服务器或 Siebel 移动/专用 Web 客户机的安装目录。

然后，已进行散列处理的口令可存储在此目录或数据库中，以便在登录时对口令进行散列处理并且与存储的已进行散列处理的版本比较时使用。

注释：有关下面提到的口令散列处理选项的重要信息，请参阅第 109 页的“配置口令散列处理”。

使用 RSA SHA-1 算法对口令进行散列处理

缺省的口令散列处理算法为 RSA SHA-1。如果使用该算法，请使用以下语法之一运行此实用程序：

```
hashpwd password1 password2 ...
```

```
hashpwd -a rsasha1 password1 password2 ...
```

要使用批处理文件对多个口令进行散列处理，请将口令输入到批处理文件中（例如，文件可能是指定的 `passwords.txt`），然后使用以下语法指定文件名：

```
hashpwd @password_file_name
```


使用 siebelhash 算法对口令进行散列处理

Siebel 独有的口令散列算法（以前通过 encrypt.exe 实用程序可用）也可用。如果使用该算法，请使用以下语法运行此实用程序：

```
hashpwd -a siebelhash password1 password2 ...
```

要使用批处理文件对多个口令进行散列处理，请将口令输入到批处理文件中（例如，文件可能是指定的 passwords.txt），然后使用以下语法指定文件名：

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

安全适配器部署选项

本节介绍了可在安全适配器验证环境或 Web SSO 环境中实施的安全适配器选项。除非另有说明，否则 Siebel LDAP 和 ADSI 安全适配器以及符合 *Siebel 安全适配器软件开发人员套件第 7 版* 的适配器都支持这些选项。

- **应用程序用户。**此目录中的指定录入值是唯一对目录具有搜索和写权限的用户。您可以在目录中为应用程序用户维护未公开的口令，而在验证流程的其它阶段使用加密版本的口令。在应用程序用户口令被发送到数据库之前，将对其应用加密算法，而且还必须使用该口令的加密版本设置应用程序用户登录。

有关详细信息，请参阅第 114 页的“配置应用程序用户”。

- **Checksum 验证。**证实该验证管理器加载的是正确版本的安全适配器。强烈建议您使用 Checksum 验证，确保由适当的安全适配器将请求访问的所有用户的用户证书提供给验证管理器。

有关详细信息，请参阅第 115 页的“配置 Checksum 验证”。

- **安全适配器的安全通讯。**您可以使用安全套接层 (SSL)，在 Siebel 提供的安全适配器与 LDAP/ADS 目录之间传输数据。

有关详细信息，请参阅第 116 页的“配置安全适配器的安全通讯”。

- **共享数据库帐户。**目录中的指定条目包含由其它用户共享的数据库帐户。

有关详细信息，请参阅第 116 页的“配置共享数据库帐户”。

- **适配器定义的用户名。**您可以配置 Siebel 应用程序，以使用户提供的用户名是 Siebel 用户 ID 之外的值，例如社会保障号。安全适配器将目录中验证用户的 Siebel 用户 ID 和数据库帐户返回给验证管理器。

有关详细信息，请参阅第 117 页的“配置适配器定义的用户名”。

- **在目录中定义的角色。**您可以选择将用户的 Siebel 职责作为角色存储在目录属性中，而不是存储在 Siebel 数据库中。

有关详细信息，请参阅第 119 页的“配置在目录中定义的角色”。

配置应用程序用户

应用程序用户必须用于实施 Siebel 安全适配器的以下验证策略中：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

通过将应用程序用户设置为唯一具有对目录进行搜索、读取和更新操作权限的用户，您可以尽量减少所有其他用户对目录的访问级别，并尽可能减少提供此类访问所需的管理工作。

应用程序用户是指您在目录定义的具有以下特点的用户：

- 用户在请求登录页时提供了 LDAP 或 Active Directory Server 与 AOM 的初始绑定。否则，绑定缺省为匿名用户。
- 该用户具有足够权限读取目录中任何用户的信息并执行任何必要的管理工作。应用程序用户对目录执行通过安全适配器请求的所有搜索和写操作。
- 应用程序用户的权限应该在组织级别（例如，适用于 LDAP 的 OU）定义。

注释：应用程序用户不是登录到应用程序的实际用户，而是处理对目录的访问的特殊用户。您必须实施应用程序用户。

要配置应用程序用户

1 在目录中，定义使用与其他用户相同属性的用户。在适当的属性中分配包含以下信息的值：

- **用户名。**分配您选择的名称。如果您实施适配器定义的用户名，请使用该属性。否则，请使用存储 Siebel 用户 ID 的属性，即使该应用程序用户没有 Siebel 用户 ID。
- **口令。**分配您选择的口令。口令必须以未加密的形式输入。如果您实施 ADS 目录，则使用 ADS 用户管理工具指定口令，而不是作为一个属性指定。

注释：在 Siebel 安全适配器实施中，应用程序用户必须对目录中的所有用户记录执行搜索和写操作的权限。在 Web SSO 实施中，应用程序用户至少必须具有搜索权限。

2 如果是 Siebel 安全适配器，请为 Siebel 网关名称服务器中安全适配器的企业资料（例如 LDAPSecAdpt 或 ADSISecAdpt）定义以下参数值。

- ApplicationUser = 目录中应用程序用户的完整识别名 (DN)

例如，ApplicationUser 可以按以下示例设置：

```
ApplicationUser = "uid=APPUSER, ou=people, o=siebel.com"
```

- ApplicationPassword = 应用程序用户口令（未加密）

如果是专用 Web 客户机，请在应用程序配置文件的相应部分中定义这些参数，例如，Siebel Call Center 的 uagent.cfg 文件。

有关设置 Siebel 配置参数的信息，请参阅附录 B “与验证有关的配置参数”。

应用程序用户和口令过期策略

通常，LDAP 或 ADS 服务器中的用户管理通过应用程序用户来执行。此外，为整个目录设置的用户策略适用于应用程序用户以及其他所有用户。

如果您在目录中实施口令过期策略，请将应用程序用户排除在策略范围之外，以便应用程序用户的口令不过期。为此，请在应用程序用户为整个目录设置口令策略之后，明确地设置应用程序用户的口令策略。

有关帐户策略和口令过期的详细信息，请参阅第 140 页的“登录功能”。

配置 Checksum 验证

安全适配器的 Checksum 验证可以在以下验证策略中实施：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

Checksum 验证将核对每位尝试获得对 Siebel 数据库访问权限的用户是否通过正确的安全适配器获得了访问权限。

您可以使用 Siebel checksum 实用程序实施 checksum 验证，该实用程序在您安装 Siebel 应用程序时将同时安装。

Checksum 验证支持以下原则：

- 安全适配器库文件（例如 Windows 中的 DLL 文件）的 CRC（循环冗余检查）checksum 值作为安全适配器的配置参数值存储。
- 在安全适配器向 AOM 提供用户身份和数据库帐户时，为该安全适配器计算 checksum 值。
- 如果两个 checksum 值相等，则为用户授予访问权限。

要配置 checksum 验证

- 1 在命令提示符位置输入并运行以下命令，并且将所需的安全适配器库文件名（例如，Windows 中的 DLL 文件）用作参数：

```
checksum -f filename
```

该实用程序返回 checksum 值。例如，以下命令：

```
checksum -f sscfldap.dll
```

将返回以下类似的结果：

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

- 2 对于您要使用的安全适配器，将 CRC 配置参数设置为第 115 页的步骤 1 中计算的 checksum 值。

注释：该过程中的 checksum 只是一个示例。您必须根据说明运行 checksum 实用程序，以便为您的实施生成有效值。另外，无论何时您要升级 Siebel 应用程序，都必须重新计算 CRC checksum 值并更新 CRC 参数值。

（如果是以前版本，则是使用安全适配器 CRC 系统首选项设置 CRC checksum 值，而不是使用配置参数设置。）

有关设置 Siebel 配置参数的信息，请参阅附录 B “与验证有关的配置参数”。

配置安全适配器的安全通讯

Siebel 安全适配器的安全通讯可以在以下验证签略中实施：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

您可以使用 SSL 对 Siebel LDAP 或 ADSI 安全适配器与目录之间的通讯加密。您必须要执行的设置工作随您实施的是 LDAP 还是 ADSI 安全适配器而有所不同。

要为 LDAP 安全适配器配置 SSL

- 将安全适配器 (LDAPSecAdpt) 的 SslDatabase 参数值设置为 ldapkey.kdb 文件的绝对路径。该文件由 IBM GSK iKeyMan 生成，它包含 LDAP 服务器使用的认证机构发行的认证。

有关为 LDAP 验证环境生成 SSL 数据库文件的信息，请参阅第 88 页的“使用 IBM GSK iKeyMan 生成 CMS 文件”。

要为 ADSI 安全适配器配置 SSL

- 1 在域中设置企业认证机构。
- 2 设置公共密钥策略，以便 Active Directory Server 自动向认证机构要求发行认证。

有关设置 Siebel 应用程序配置文件参数的信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。

配置共享数据库帐户

共享数据库帐户选项可以在以下验证策略中实施：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

您可以配置验证系统，以便指定的目录条目包含由多位用户共享的数据库帐户。

缺省情况下，不实施共享数据库帐户选项，而且每位用户的数据库帐户位于目录中的该用户记录的属性中。由于所有已在外部验证的用户共享一个或多个数据库帐户，因此，相同的证书被多次复制。如果必须更改这些证书，则必须为每位用户进行编辑。通过实施共享的证书，您可以减少目录管理工作。

LDAP 和 ADSI 以不同的方式使用共享数据库帐户选项：

- 对于 LDAP，如果指定了共享数据库帐户，则始终从该帐户中检索数据库证书。
- 对于 ADSI，如果指定了共享数据库帐户，并且可以提取数据库证书，则从用户处检索数据库证书。如果不能从用户检索数据库证书，则从共享数据库帐户中进行检索。

要配置共享数据库帐户

- 1 创建一个数据库帐户，让登录到指定 Siebel 应用程序的所有用户都可以共享该帐户。
- 2 在目录中创建指定条目，并在该条目的某个属性（例如 dbaccount 属性）中输入公共数据库帐户的用户名和口令参数。您可能需要创建该属性。

有关格式化包含数据库帐户的目录属性的信息，请参阅第 70 页的“LDAP/ADS 目录的要求”。

- 3 为每个实施此共享数据库帐户的安全适配器（例如 LDAPSecAdpt）定义以下参数值：
 - CredentialsAttributeType = 目录中存储数据库帐户的属性，例如 dbaccount
 - SharedCredentialsDN = 指定条目的识别名（包括引号），例如 "uid=SHAREDENTRY, ou=People, o=companyname.com"

有关设置 Siebel 应用程序配置文件参数的信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。

配置适配器定义的用户名

适配器定义的用户名选项可以在以下验证策略中实施：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

您可以配置验证系统，以使传送给目录用于检索用户数据库帐户的用户名不是 Siebel 用户 ID。例如，您可能希望用户输入适配器定义的用户名，例如，他们的社会保障号、电话号码、电子邮件地址或帐号。

在用户使用适配器定义的用户名登录时，仍然必须向 AOM 提供用户的 Siebel 用户 ID。

适配器定义的用户名必须存储在目录的一个属性中，而 Siebel 用户 ID 存储在另一个属性中。例如，您可能让用户输入电话号码并存储在 telephonenumber 属性中，而将他们的 Siebel 用户 ID 存储在 uid 属性中。

UsernameAttributeType 配置参数定义用于存储用户名的目录属性，用户名被传送给目录以识别用户身份，它可以是 Siebel 用户 ID 或适配器定义的用户名。AOM 的 OM - 用户名 BC 字段（别名为 UsernameBCField）参数定义用户业务组件的字段，它是 UsernameAttributeType 指定的属性的基础。

即使符合通过 Siebel 客户机管理目录中用户属性的其它要求，您也必须为该安全适配器设置 UsernameAttributeType 参数，并设置 OM - 用户名 BC 字段参数。如果您未相应地定义这些参数，请通过 Siebel 客户机对基本字段所做的更改不会传播到目录中。

例如，对于使用其办公电话号码登录的用户，您必须将 UsernameAttributeType 指定为存储电话号码的目录属性（例如 telephonenumber），并且必须将 OM - 用户名 BC 字段定义为电话号码，即用户业务组件中用于该办公电话号码的字段。

要配置适配器定义的用户名

1 为实施适配器定义的用户名的每个安全适配器（例如 LDAPSecAdpt）定义以下参数值：

- UseAdapterUsername = TRUE
- SiebelUserNameAttributeType = 存储 Siebel 用户 ID 的属性，例如 uid (LDAP) 或 sAMAccountName (ADSI)。
- UsernameAttributeType = 存储适配器定义的用户名的属性，例如 telephonenumber。

2 确定用户业务组件中的字段，该字段用于填入目录中包含适配器定义的用户名的属性。

要填写的 AOM 参数是 OM - 用户名 BC 字段。

有关处理 Siebel 业务组件的信息，请参阅 *Configuring Siebel eBusiness Applications*。有关处理配置参数的信息，请参阅 *Siebel System Administration Guide*。

3 使用 Siebel Server Manager，指定用户业务组件字段名作为 OM - 用户名 BC 字段参数的值。您可以在 Enterprise、Siebel 服务器或组件级别提供该值。如果该参数未出现在参数列表中，请添加该参数。

注释：如果您未在 OM - 用户名 BC 字段参数中指定字段，Siebel 安全适配器则假定用户业务组件的“登录名”字段（Siebel 用户 ID）是 UsernameAttributeType 参数定义的属性的基础。

有关设置 Siebel 配置参数的信息，请参阅附录 B “与验证有关的配置参数”。

配置匿名用户

匿名用户是一个访问权限非常有限的 Siebel 用户。匿名用户（在 Siebel 数据库中定义）允许用户访问登录页或包含登录表单的页面。对于 LDAP/ADSI 验证，匿名用户必须在用户目录中具有对应的记录。

您必须为实施 LDAP/ADSI 验证的任何 Siebel 应用程序定义匿名用户。

即使应用程序不允许未注册的用户进行访问，仍然需要提供匿名用户。在初次启动 AOM 线程时，它首先使用匿名用户帐户连接至数据库并检索信息（例如，许可证密钥），然后显示登录页。

在 eapps.cfg 文件中，您可以指定是将匿名用户用于单一应用程序，还是用作所部署的所有 Siebel 应用程序的缺省用户。即使将匿名用户指定为缺省用户，任何单一应用程序都可以覆盖缺省用户。

如果您在大多数或所有应用程序中使用一个匿名用户，则可能需要在缺省级别定义匿名用户，执行这一操作所需的管理工作更少。要设置参数的缺省值（例如 AnonUserName 和 AnonPassword），请在 eapps.cfg 文件的 [defaults] 部分中包括该缺省值。

要使参数覆盖单个应用程序的缺省值，请将其列在应用程序的部分中，例如 [/eservice] 部分。

匿名浏览和匿名用户

如果您实施安全适配器验证或数据库验证，则可以允许或禁止未注册的用户浏览应用程序视图的一组子视图。如果您允许匿名浏览，用户则可以浏览未标记为显式登录的视图。

如果您禁止匿名浏览，未注册的用户则无权访问应用程序的任何视图。

注释：即使您禁止匿名浏览，未注册的用户仍然有权访问应用程序的登录页。

有关处理 Siebel 应用程序视图的信息，请参阅 *Configuring Siebel eBusiness Applications*。

如果您允许匿名浏览，请在应用程序的配置文件中（例如，在 `eservice.cfg` 文件中）设置以下参数：

```
[SWE]
AllowAnonUsers = TRUE
```

如果该参数值为 `FALSE`，则不允许未注册的用户访问该 Siebel 应用程序。

注释：由于匿名用户会话将高速缓存信息；因此在用户登录或重新启动匿名用户会话之前，对目录等数据所做的任何更改将不会被更新。

除 `AllowAnonUsers` 参数之外，您还可以设置 `LoginView` 参数。该参数确定显示什么样的登录视图（相对于缺省的 Web 登录页）。`AllowAnonUsers` 参数必须为 `TRUE`，才能识别 `LoginView` 参数。

缺省情况下，`LoginView` 参数不会出现在应用程序配置文件的 `[SWE]` 部分中，必须添加该参数。

有关设置 Siebel 配置参数的信息，请参阅附录 B “与验证有关的配置参数”。

配置在目录中定义的角色

角色是一种将 Siebel 职责与用户关联的备用方式。此选项可在以下验证策略中实施：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

在 Siebel 应用程序中分配给每位用户的职责向用户提供了访问特定视图的权限。职责在 Siebel 应用程序中创建，并且存储在 Siebel 数据库中。一个或多个职责通常与“管理 - 应用程序”屏幕中的每位用户关联。

LDAP/ADS 目录中的角色是将 Siebel 职责与用户关联的另一种方式。如果要管理大量职责，角色将非常有用。只要职责直接或间接地与用户关联，用户就有权访问与所有这些职责关联的所有视图。

警告：建议您在数据库或目录中分配职责，但不要同时在两个地点分配职责。如果您为角色定义了目录属性，但是不使用它来将职责与用户关联，请将该属性留空。

如果您使用角色管理用户职责，请遵循以下准则：

- 在 Siebel 应用程序中创建职责，但是不要通过 Siebel 应用程序界面向用户分配任何职责。
- 要允许为任何用户分配多个职责，您必须将角色的目录属性定义为多值属性。Siebel 支持的安全适配器不能从单一值属性中读取多个职责。
- 角色的目录属性应该包含您希望用户拥有的 Siebel 职责的名称。在多值字段的每个元素中输入一个职责名称，例如 Web 注册用户。角色名称区分大小写。

您可以配置 Siebel 提供的安全适配器，以便从目录中检索用户的角色。对于使用角色的每个 Siebel 应用程序，请为 LDAP 或 ADSI 安全适配器设置以下参数值。

例如，对于 LDAP 安全适配器，定义以下参数：

```
RolesAttributeType= attribute_in_which_roles_are_stored
```

有关设置 Siebel 配置参数的信息，请参阅附录 B “与验证有关的配置参数”。

安全适配器和 Siebel 专用 Web 客户机

Siebel 专用 Web 客户机会重新查找从 Siebel 服务器到客户机的业务逻辑。专用 Web 客户机的验证体系结构与标准 Web 客户机的验证体系结构不同，因为它在客户机而不是 Siebel 服务器上查找以下组件：

- AOM（通过 siebel.exe 程序）
- 应用程序配置文件
- 验证管理器和安全适配器

在您为 Siebel 专用 Web 客户机实施安全适配器验证时，请遵循以下原则：

- 建议使用远程配置选项，它帮助您确保所有的客户机使用相同的配置设置。本小节稍后将介绍该选项。
- 对于存储在客户机的应用程序配置文件或者远程配置文件中与验证有关的配置参数，它们包含的值通常应该与名称服务器（适用于 Siebel Web 客户机用户）中对应的参数值相同。请将适当的配置文件分布到所有 Siebel 专用 Web 客户机用户中。

有关在 Siebel 专用 Web 客户机上设置 Siebel 应用程序配置文件中参数的信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。

- 建议您使用 Checksum 验证，确保由适当的安全适配器将请求访问的所有用户的用户证书提供给验证管理器。有关 checksum 验证的信息，请参阅第 115 页的“配置 Checksum 验证”。
- 在安全适配器验证实施中，您必须将安全适配器配置参数 PropagateChange 设置为 TRUE，并且将 Siebel 系统首选项 SecThickClientExtAuthent 设置为 TRUE，条件是您要实施：
 - Siebel 专用 Web 客户机用户的安全适配器验证。
 - 将对用户管理所做的更改从 Siebel 专用 Web 客户机传播至外部目录，例如 LDAP 或 ADS。（例如，用户在专用 Web 客户机中更改了他或她的口令，所更改的口令将被填入到该目录。）

有关详细信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”和第 260 页的“系统首选项”。

- 在某些环境中，您可能要依靠数据服务器本身来确定是否允许 Siebel 专用 Web 客户机用户访问 Siebel 数据库和运行应用程序。在本地客户机的应用程序配置文件中，您可以根据需要定义服务器数据来源的参数 IntegratedSecurity（通常位于配置文件的 [ServerDataSrc] 部分中）。

该参数可以设置为 TRUE 或 FALSE。缺省值为 FALSE。如果设置为 TRUE，则防止 Siebel 客户机在用户登录时提示用户输入用户名和口令。现有数据服务器基础设施中提供的设施确定了是否应该允许用户登录到数据库。

您可以将 IntegratedSecurity = TRUE 用于数据库安全适配器。另请参阅第 68 页的“配置数据库验证”。

注释：只有 Oracle 和 Microsoft SQL Server 数据库支持 IntegratedSecurity。有关附加信息，请参阅第三方文档。对于 Oracle，请参阅 OPS\$ 和 REMOTE_OS_AUTHENT 功能。对于 Microsoft SQL Server，请参阅“集成安全性”。

有关 Siebel 专用 Web 客户机的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南* 和 *Siebel System Administration Guide*。

配置文件中 LDAP 部分的示例

以下是您在为专用 Web 客户机配置 LDAP 安全适配器时 LDAP/ADSI 配置实用程序生成的 LDAP 配置信息示例。有关详细信息，请参阅第 91 页的“使用 LDAP/ADSI 配置实用程序”。

有关设置 Siebel 配置参数的信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。

```
[LDAPSecAdpt]
SecAdptDllName = sscfldap
ServerName = ldapserver.siebel.com
Port = 636
BaseDN = "ou=people, o=xyz.com"
SharedCredentialsDN = "uid=HKIM, ou=people, o=Siebel.com"
UsernameAttributeType = uid
PasswordAttributeType = userPassword
CredentialsAttributeType = mail
RolesAttributeType = roles
SslDatabase = /suitespot/https-myhost/ldapkey.kdb
ApplicationUser = "uid=APPUSER, ou=people, o=xyz.com"
ApplicationPassword = APPUSERPW
HashDBPwd = TRUE
PropagateChange = TRUE
CRC =
SingleSignOn = TRUE
TrustToken = mydog
UseAdapterUsername = TRUE
SiebelUsernameAttributeType = PHONE
HashUserPwd = TRUE
HashAlgorithm = RSASHA1
```

专用 Web 客户机的远程配置选项

仅限于 Siebel 专用 Web 客户机，远程配置选项可以在以下验证策略中实施：

- 安全适配器验证：LDAP、ADSI 或定制（不是数据库验证）
- Web SSO 验证

通过此方法，您创建一个单独的文本文件，用于定义配置安全适配器的任何参数值。您在远程文件而不是应用程序配置文件中配置所有的安全适配器参数，例如，类似于 [LDAPSecAdpt] 或 [ADSIAdpt] 部分中的那些参数。

将配置参数存储在一个集中位置可以帮助您降低管理费用。所有专用 Web 客户机都可以读取在某个集中的远程位置上同一个文件中存储的与验证有关的参数。

以下示例显示如何使用远程配置文件以便为在 Web SSO 环境中为由 Siebel eService 实施的安全适配器提供参数。以下示例来自 Siebel Call Center 的配置文件 uagent.cfg：

```
[InfraSecMgr]
SecAdptMode = LDAP
SecAdptName = LDAPSecAdpt
UseRemoteConfig = \\it_3\vol_1\private\ldap_remote.cfg
```

在此情况下，配置文件 `ldap_remote.cfg` 将包含一个 `[LDAPSecAdpt]` 部分。它可以类似于本节前面的示例进行定义，并且不包含其它任何内容。应用程序配置文件将包含上面定义的 `[InfraSecMgr]` 部分。它不包含 `[LDAPSecAdpt]` 部分 — 即使包含该部分，该部分也会被忽略。

要为 Siebel 专用 Web 客户机实施远程安全配置，请遵循以下准则：

- Siebel 配置文件中的 `[InfraSecMgr]` 部分必须包括 `UseRemoteConfig` 参数，该参数提供了远程配置文件的路径。路径以通用命名惯例格式指定 - 例如，`\\server\vol\path\ldap_remote.cfg`。
- 远程安全配置文件只包含用于配置安全适配器的一个部分，例如，`[LDAPSecAdpt]` 部分。
- 每位专用 Web 客户机用户必须具有读取远程配置文件及该文件所在磁盘目录的权限。

移动 Web 客户机同步的验证

本节介绍了在同步期间为验证远程用户而执行的一些处理。有关同步流程的详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

请注意有关 Siebel Remote 和远程用户的以下详情：

- 远程用户不连接至 Web 服务器。在远程用户同步时，他们直接从 Siebel 移动 Web 客户机连接至 Siebel Remote 服务器（专用于支持与远程用户同步的 Siebel 服务器）。
- 访问本地数据库时只能使用一个用户 ID 和口令。本地数据库不能属于多个用户。
- 单一用户可以具有多个移动 Web 客户机，例如，两台独立计算机上的两个客户机。

要同步本地数据库

- 1 Siebel Remote 用户连接至其客户机上的本地数据库，并执行交易修改。为此，请执行此操作：
 - a 启动客户机上的 Siebel 图标，然后输入用户 ID 和口令。
 - b 在“连接至”参数中，选择“本地”。

用户 ID 和口令由客户机上的本地数据库进行验证。

此时将在 Web 浏览器中出现 Siebel 应用程序，用户可以通过应用程序导航。
 - c 根据需要修改数据（插入、更新或删除操作）。
- 2 以后，用户决定同步本地数据库更改，并且从 Siebel Remote 服务器下载更新。为此，请执行此操作：
 - a 使用拨号调制解调器、LAN、WAN 或 VPN 连接至 Siebel Remote 服务器。
 - b 启动客户机上的 Siebel 图标，然后输入用户 ID 和口令。
 - c 在“连接至”参数中，选择“本地”。

用户 ID 和口令由客户机上的本地数据库进行验证。
- 3 在 Web 浏览器中出现 Siebel 应用程序时，用户请选择“文件” > “同步数据库”。

现在用户正在访问 Siebel Remote 服务器以执行同步，并且需要通过验证。
- 4 一旦远程用户通过验证，则开始执行同步。

同步管理器的验证选项

Siebel Remote 的同步管理器服务器组件将验证每个传入的移动 Web 客户机请求。同步管理器根据服务器数据库中有效的移动 Web 客户机列表验证移动用户的用户 ID，并验证有效结束日期是有效还是为 NULL。

同步管理器还验证移动 Web 客户机已经连接至正确的 Siebel Remote 服务器。如果移动 Web 客户机连接至错误的 Siebel Remote 服务器，同步管理器将移动 Web 客户机重新连接至另一个 Siebel Remote 服务器，并更新客户机的本地配置信息。

同步管理器使用由验证方法配置参数（别名是 Authentication）指定的方法验证移动 Web 客户机的口令。请使用 Siebel Server Manager 为同步管理器设置该参数。有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

验证方法可以设置为以下值之一：

- **无**。不验证移动 Web 客户机的口令。这是缺省设置。
- **数据库**。使用移动 Web 客户机的用户名和口令连接至服务器数据库。使用数据库安全适配器（通常是 DBSecAdpt）完成该任务。
- **安全适配器**。使用由安全适配器模式和安全适配器名称参数指定的安全适配器对用户进行验证。用户验证可能基于数据库或 LDAP/ADS 目录，具体取决于哪个安全适配器有效。口令散列处理取决于该安全适配器的配置。
注释：安全适配器模式和安全适配器名称参数可以在 Enterprise 或 Siebel 服务器级别设置，或者为同步管理器组件设置。数据库验证是缺省的安全适配器。您可以在整个 Siebel Enterprise 中使用同一个安全适配器，也可以为同步管理器使用其它安全适配器，该适配器不同于为 Enterprise 中的其余组件使用的安全适配器。有关详细信息，请参阅本章前面的第 67 页的“关于 Siebel 安全适配器”以及随后的主题。
- **Siebel**。根据在移动 Web 客户机屏幕存储的口令，验证移动 Web 客户机的口令。（该选项使用杂乱式加密算法，通常不再推荐使用该选项。）
- **AppServer**。验证口令与 Siebel 服务器机器上用户操作系统的口令相同。（通常不再推荐使用该选项。）

7

Web 单一登录验证

本章介绍了如何实施 Web 单一登录 (Web SSO) 以执行用户验证。它包括以下主题：

- 第 125 页的“关于 Web 单一登录”
- 第 126 页的“实施 Web SSO 验证”
- 第 127 页的“设置 Web SSO：方案”
- 第 137 页的“数字认证验证”
- 第 138 页的“用户身份的来源”

关于 Web 单一登录

在 Web SSO 实施中，用户通过第三方在 Web 站点级别进行验证。Siebel 应用程序支持这种验证模式，它提供了一个界面，以允许第三方将用户信息传送到 Siebel 应用程序。一旦通过第三方验证，用户就不必显式登录到 Siebel 应用程序。Web SSO 让您可以在现有 Web 站点或门户站点中部署 Siebel 应用程序。

Web SSO 体系结构适用于只有批准的注册用户才能获得访问敏感数据权限的 Web 站点，例如，您与渠道合作者共享数据的 Web 站点。

注释： Web SSO 验证不适用于 Siebel 移动 Web 客户机。

Web SSO 验证流程

以下所示的是 Web SSO 验证流程的步骤：

- 1** 用户在 Web 站点输入要传送给 Web 服务器的证书。Web 服务器上的第三方验证客户机将用户证书传送给第三方验证服务。第三方验证服务验证用户的证书，并将已验证用户的用户名传送给 Siebel Web Server Extension (SWSE)。
- 2** SWSE 将已验证用户的用户名传送给验证管理器。用户名可以是 Siebel 用户 ID 或其它属性。
- 3** 安全适配器将已验证用户的用户名提供给目录，用户的 Siebel 用户 ID、数据库帐户和角色（可选）再从该目录返回给验证管理器。
- 4** 应用程序对象管理器 (AOM) 使用返回的证书，将用户连接至数据库并标识用户。

Web SSO 限制

由于 Web SSO 部署假设用户验证和用户管理是第三方安全基础设施的职责，因此在 Web SSO 环境中不象 Siebel eBusiness Applications 那样提供以下功能：

- 用户自行注册
- 用户的授权管理
- 登录表单
- 注销链接或应用程序级别菜单“文件”中的“注销”菜单项
- 更改口令功能（在“用户首选项”屏幕的“资料”视图中）

您的 Siebel 应用程序可能需要更改一些配置，以隐藏此类功能。有关详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

注释：由于 Web SSO 环境中 Siebel 应用程序用户不能使用注销功能，因此此类用户必须通过关闭浏览器窗口来结束应用程序会话。在 Microsoft Internet Explorer 中，请选择“文件”>“关闭”或者单击窗口右上角的 X 来结束会话。如果达到用户的会话超时时间，AOM 则终止该会话的任务（线程）。SessionTimeout 参数位于 SWSE 的 eapps.cfg 文件中。有关该参数的详细信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。

Web SSO 实施的注意事项

以下是实施 Web SSO 策略的一些注意事项：

- 用户独立于 Siebel 应用程序进行验证，例如，可以通过第三方验证服务或 Web 服务器进行验证。
- 您必须在 Web 站点级别使验证系统中的用户与 Siebel 数据库中的用户同步。
- 您必须在 Web 站点级别配置用户管理功能，例如，自行注册。
- 授权的管理员可以在 Siebel 数据库中添加用户，但是不能在验证系统中添加。

有关将第三方验证软件与 Siebel eBusiness Applications 集成的详细信息，请参阅 Siebel SupportWeb 或与 Siebel 联盟访问组联系。

实施 Web SSO 验证

要在实施 Web SSO 的 Web 站点上向用户提供 Siebel 应用程序的访问权限，Siebel 应用程序必须可以根据验证系统确定以下信息：

- 确认用户已通过验证的证明
- 可传送给目录的用户证书，从该证书中可以检索用户的 Siebel 用户 ID 和数据库帐户

在 Web SSO 环境中，您还必须提供验证服务以及所需的任何组件，例如验证客户机组件。

注释：对于特定 Siebel 应用程序，用户在从 Siebel 专用 Web 客户机连接至服务器数据库时，采用的验证机制必须与 Siebel Web 客户机用户使用的验证机制相同。该机制可能是数据库验证，也可能是支持的外部验证策略，例如 LDAP 或 ADSI。然而，在使用 Siebel 移动 Web 客户机连接至本地数据库时，移动用户必须使用本地数据库验证。

有关移动用户用于本地数据库同步的验证选项的信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

有关设置 Web SSO 时涉及的任务概述, 请参阅第 127 页的“设置 Web SSO: 方案”。

您可以在使用符合 Siebel 要求的安全适配器的 Web SSO 环境中实施以下选项:

- **用户身份的来源。**您必须指定 Siebel Web 引擎从中得出用户身份密钥的来源: Web 服务器环境变量或 HTTP 请求标题变量。有关详细信息, 请参阅第 138 页的“用户身份的来源”。
- **数字认证验证。**Siebel Systems 支持 Web 服务器执行的 X.509 数字认证验证。有关为 Web SSO 实施数字认证验证的信息, 请参阅第 137 页的“数字认证验证”。
- 此外, 您还可以为 Web SSO 实施第 113 页的“安全适配器部署选项”中指定的许多选项。

有关用户验证疑难解答的信息, 请参阅第 243 页的“用户验证问题”。

设置 Web SSO: 方案

本节介绍了为单一 Siebel 应用程序设置 Web SSO 体系结构的说明。您的实施可能包括多个 Siebel 应用程序, 而且您可能实施未在此处包括的选项。

请确保在生产环境中部署 Web SSO 之前, 首先在开发环境中实施此体系结构。您可以重复执行此处的适用说明, 以便为附加的 Siebel 应用程序提供 Web SSO 访问。

这些说明用于实施以下基本 (示例) 配置:

- 在 Windows 2000 上部署 IIS Web 服务器。IIS Web 服务器用作验证服务。
- Active Directory Server (ADS) 和 Web 服务器安装在不同的机器上。ADS 用作用户的目录以提供以下功能:
 - 验证 Web 服务器用户。
 - 为已验证的 Web 服务器用户提供 Siebel 用户 ID 和数据库帐户。
- ADSI 安全适配器在验证管理器与 ADS 之间通讯。
- Siebel 服务器, 包括代表基于 Web 的 Siebel 应用程序部署的 AOM。

注释: 本节中的说明描述了最低的基准配置。在生产环境中, 建议不要将 Siebel 服务器与 Web 服务器安装在同一台机器上。

如果您使用非 Siebel 安全适配器, 该适配器必须支持第 19 页的“安全适配器 SDK”中介绍的 Siebel 安全适配器软件开发人员套件。您必须修改实施过程的适用部分, 以满足安全适配器的需要。

在设置该 Web SSO 验证环境之前, 您必须先完成以下安装:

- 将 Web 服务器和 ADS 安装在不同的机器上。
- 安装 Siebel 应用程序, 包括 Siebel 网关名称服务器和 Siebel 服务器。在 Web 服务器机器上安装 Siebel 服务器, 包括受影响的 AOM。

这些说明假设您已具备管理 ADS 的经验。您可以执行创建和修改用户存储子目录、创建属性、创建用户以及为用户提供权限等任务。

实施 Web SSO 的流程

您必须执行以下流程中的任务，以便在该环境中实施 Web SSO：

- 1 在 Web 服务器机器上为 Siebel 应用程序创建被保护的虚拟目录。请参阅第 128 页的“创建被保护的虚拟目录”。
- 2 设置第三方 Web SSO 验证。
- 3 设置可以从中检索数据库帐户和用户的 Siebel 用户 ID 的目录。
- 4 为外部验证的用户创建数据库登录。请参阅第 130 页的“创建数据库登录”。
- 5 设置 ADS。请参阅第 130 页的“设置 Active Directory Server”。
- 6 在 ADS 目录中创建以下三个用户：普通用户、匿名用户和应用程序用户。请参阅第 131 页的“在目录中创建用户”。
- 7 在 Siebel 数据库中添加与目录中的普通用户和匿名用户对应的用户记录。请参阅第 132 页的“在 Siebel 数据库中添加用户记录”。
- 8 编辑 eapps.cfg 文件参数。请参阅第 133 页的“编辑 eapps.cfg 文件中的参数”。
- 9 为专用 Web 客户机编辑 Siebel 应用程序的配置文件参数。请参阅第 135 页的“编辑应用程序配置文件中的参数”。
- 10 编辑 Siebel 网关名称服务器参数。请参阅第 134 页的“编辑名称服务器参数”。
- 11 重新启动 Siebel 服务器和 Web 服务器。请参阅第 136 页的“重新启动服务器”。
- 12 测试实施。请参阅第 136 页的“测试 Web SSO 验证”。

创建被保护的虚拟目录

被保护的虚拟目录用于支持匿名浏览的 Siebel 应用程序。通过在两个 Web 服务器虚拟目录下面提供部分应用程序，您可以将第三方验证客户机配置为保护其中一个虚拟目录，而不保护另一个虚拟目录，以供匿名浏览时访问。在用户请求需要显式登录的 Siebel 视图时，该请求被自动重定向到被保护的虚拟目录。

您必须执行以下任务，以便为 Siebel 应用程序指定一个 Web 服务器虚拟目录。对于用户通过 Web 服务器访问的每个 Siebel 应用程序，您必须重复执行该流程的两个阶段。

- 创建虚拟目录。
- 为 Web 服务器指定一个特定的 DLL 文件，以允许 SWSE 与 Web 服务器通讯。

对于每个 Siebel 应用程序，每个虚拟目录和 DLL 文件的实际路径都相同。

注释：您可以根据需要修改现有的虚拟目录，而不是创建新的虚拟目录。

要在 Microsoft Internet Information Server 上创建虚拟目录

- 1 启动“Internet 服务管理器”。选择“程序”>“管理工具”>“Internet 服务管理器”。
- 2 在“Internet 服务管理器”浏览器中，右键单击缺省的 Web 站点，然后选择“新建”>“虚拟目录”。
此时将出现“虚拟目录创建向导”。
- 3 输入 Siebel 应用程序虚拟目录的名称，然后单击“下一步”。例如，输入 p_eservice 作为 Siebel eService 的虚拟目录。
- 4 输入 *SWEAPP_ROOT*\public 目录的完整路径，然后单击“下一步”（其中 *SWEAPP_ROOT* 是 SWSE 的安装目录）。
该子目录包含要发布到站点的内容。
- 5 选择以下复选框，并将其它复选框留空，然后单击“完成”。
 - 允许读取访问
 - 允许脚本访问
 - 允许执行访问
 此时将出现“Internet 服务管理器”浏览器，并且结构中出现该新虚拟目录。

要允许 SWSE 与 Web 服务器通讯

- 1 在“Internet 服务管理器”浏览器中，右键单击您创建的虚拟目录，然后选择“属性”。
此时将出现“属性”对话框。
- 2 单击“配置”。
此时将出现“应用程序配置”对话框。
- 3 单击“添加”。
此时将出现“添加/编辑应用程序扩展名映射”对话框。
- 4 单击“浏览”，导航并选择 *SWEAPP_ROOT*\bin 目录中的 sweiis.dll 文件，然后单击“打开”（其中 *SWEAPP_ROOT* 是 SWSE 的安装目录）。
此时将出现“添加/编辑应用程序扩展名映射”对话框，其中包括 sweiis.dll 文件的路径。
- 5 输入 .swe 作为扩展名，只核选“脚本引擎”复选框，然后单击“确定”。
此时将出现“应用程序配置”对话框。
- 6 单击“应用”，然后单击“确定”。
此时将出现“属性”对话框。
- 7 单击“目录安全性”选项卡。
- 8 在“匿名访问和验证控制”部分中单击“编辑”。
此时将出现“验证方法”对话框。
- 9 核选“基本验证”复选框，并取消核选其它复选框。

10 在“Internet 服务管理器”的警告对话框中单击“是”，然后在返回到“验证方法”对话框时，单击“确定”。

此时将出现“属性”对话框中的“目录安全性”选项卡。

11 单击“应用”，然后单击“确定”。

创建数据库登录

必须存在一个针对所有外部验证用户的数据库登录。该登录不能分配给任何真实人员。为实现这一点，在您安装 Siebel eBusiness Applications 时提供了一个 seed 数据库登录，这在第 261 页的“Seed 数据”中有介绍。它的登录名为 LDAPUSER，其缺省口令为 LDAPUSER，这些值都应该由管理员更改。如果该登录名不存在，请创建一个。

设置 Active Directory Server

在此方案中，Active Directory Server (ADS) 执行两项功能，而在其它 Web SSO 实施中，这两项功能可能由两个单独的实体分别进行处理。

- 用户通过 ADS 进行验证，ADS 将其功能作为 IIS Web 服务器目录执行。

- ADS 用作从中检索已验证用户的 Siebel 用户 ID 和数据库帐户的目录。

您必须执行单独的配置任务以达到以下目的：

- 将 ADS 配置为提供已验证用户的用户 ID 和 Siebel 数据库帐户的目录。

- 将 IIS Web 服务器配置为根据 ADS 执行验证。

配置 Active Directory Server

确定在 ADS 目录中用于存储用户的子目录。您不能将单一 Siebel 应用程序的用户分布到多个子目录中。然而，您可以在一个子目录中存储多个 Siebel 应用程序的用户。在本示例中，用户存储在 ADS 域级别目录下面的 Users 子目录中。

定义要用于以下用户数据的属性。如果您不想使用现有属性，请创建新属性。在该示例中，提供了建议的属性。ADS 目录中已经存在一些建议的属性，不需要另外配置。

- **Siebel 用户 ID。** 建议的属性：sAMAccountName。

- **数据库帐户。** 建议的属性：dbaccount。

此外，用户口令通过 ADS 用户管理工具分配给每位用户。用户口令不作为属性存储。

注释：对于其角色是 IIS Web 服务器目录，而且是此配置中的验证服务的 ADS，用户口令是一个必需属性，而对于用作目录的 ADS，用户口令则不是必需属性。在验证服务实际上独立于此目录的其它配置中，不必提供此目录即可将用户口令分配给每位用户。

要执行 IIS Web 服务器验证，请根据需要提供属性以存储用户名、名字、姓氏或其它用户数据。

配置 IIS Web 服务器

您必须将 IIS Web 服务器配置为根据 Active Directory Server 执行验证。

您可以将 IIS Web 服务器配置为使用基本验证。

有关为 IIS Web 服务器设置验证模式的信息，请参阅 IIS Web 服务器文档。

要测试该 Web SSO 的实施情况，请将您的 Web 站点配置为要求用户在 Web 站点入口处登录。

在目录中创建用户

请根据第 131 页的表 12 中的介绍在目录中创建三个用户。本示例中建议创建属性名称 sAMAccountName 和口令。您输入的内容可能随您在第 130 页的“设置 Active Directory Server”中的属性分配方式而有所不同。

表 12. 目录记录

用户	sAMAccountName	口令	数据库帐户
匿名用户	<ul style="list-style-type: none"> ■ 为要实施的 Siebel 应用程序输入匿名用户记录的用户 ID。 您可以为 Siebel 客户或合作者应用程序使用 seed 数据匿名用户记录，这在第 261 页的“Seed 数据”中有介绍。例如，对于 Siebel eService，请输入 GUESTCST。 ■ 您可以为 Siebel 雇员应用程序创建一个新用户记录或修改 seed 匿名用户记录。 	GUESTPW 或您选择的口令	username=LDAPUSER password= <i>P</i>
应用程序用户	APPUSER 或您选择的名称	APPUSERPW 或您选择的口令	数据库帐户不用于应用程序用户。
测试用户	TESTUSER 或您选择的名称	TESTPW 或您选择的口令	username=LDAPUSER password= <i>P</i>

所有三个用户的数据库帐户相同，并且必须与第 130 页的“创建数据库登录”中介绍的为外部验证用户保留的数据库帐户相符。*P* 表示该数据库帐户中的口令。有关数据库帐户属性录入值的格式化要求的信息，请参阅第 70 页的“LDAP/ADS 目录的要求”。

警告：请确保应用程序用户具有对目录中的所有记录执行搜索和写操作的权限。

根据需要为每位用户填写其它属性字段。

在 Siebel 数据库中添加用户记录

您必须在 Siebel 数据库中创建与您在第 131 页的“在目录中创建用户”中创建的测试用户对应的记录。

您必须确认第 262 页的表 25 中介绍的用于 Siebel 客户或合作者应用程序的匿名用户的 seed 数据记录存在。该记录还必须与您在第 131 页的“在目录中创建用户”中创建的匿名用户相匹配。

您可以为 Siebel 雇员应用程序修改 seed 数据匿名用户或创建新的匿名用户。

要确认与数据库的连通性，您可以使用以下过程，为任何 Siebel 应用程序添加测试用户。然而，如果您要配置 Siebel 雇员或合作者应用程序，并且希望用户是雇员或合作者用户，请填写职位、部门和组织，请参阅第 166 页的“用户的内部管理”中有关添加此类用户的说明。

要在数据库中添加用户记录

- 1 以管理员身份登录 Siebel 雇员应用程序，例如 Siebel Call Center。
- 2 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 用户”>“用户”。
- 3 在“用户”列表中，创建新记录。
- 4 为测试用户填写以下字段，然后保存记录。使用所示的准则，所建议的录入值适用于本示例。您可以填写其它字段，但是这一操作不是必需的。

字段	示例录入值	准则
姓氏		必需。输入任何名称。
名字		必需。输入任何名称。
用户 ID	TESTUSER	必需。该录入值必须与目录中测试用户的 sAMAccountName 属性值相匹配。如果您使用了其它属性，而不是 sAMAccountName，它必须与该值相匹配。
职责		必需。输入为所实施 Siebel 应用程序的注册用户提供的 seed 数据职责。例如，为 Siebel eService 输入 Web 注册用户。如果相应的 seed 职责不存在（例如 Siebel 雇员应用程序），请分配一个您创建的相应职责。
新职责		可选。输入为所实施 Siebel 应用程序的注册用户提供的 seed 数据职责。例如，为 Siebel eService 输入 Web 注册用户。该职责自动被分配给为此测试用户创建的新用户。

- 5 验证所实施 Siebel 应用程序的匿名用户的 seed 数据用户记录存在，这在第 262 页的表 25 中有介绍。

例如，您在实施 Siebel eService，请验证存在用户 ID 为 GUESTCST 的 seed 数据用户记录。如果记录不存在，请使用第 262 页的表 25 中的字段值创建该记录。您可以填写其它字段，但是这一操作不是必需的。

编辑 eapps.cfg 文件中的参数

请根据第 133 页的表 13 中准则的指示，在 eapps.cfg 文件中提供参数值。

有关编辑 eapps.cfg 参数以及参数意图的详细信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。

表 13. eapps.cfg 文件中的参数值

部分	参数	示例录入值	准则
[defaults]			<p>此部分中的参数值被您在单个应用程序的部分中设置的参数值覆盖。</p> <p>对于此方案，请在特定于应用程序的部分中设置 Web SSO 和相关的参数。</p>
特定于应用程序的部分，例如以下部分之一： [/eservice] [/callcenter]	AnonUserName		<p>输入为所实施应用程序提供的 seed 数据用户记录的用户 ID，或者输入为匿名用户创建的用户记录的用户 ID。</p> <p>此录入值还与目录中匿名用户记录的 sAMAccountName 录入值相匹配。例如，为 Siebel eService 输入 GUESTCST。</p>
	AnonPassword		<p>输入在目录中为匿名用户创建的口令。</p> <p>注释：通常对 eapps.cfg 文件应用口令加密。在此情况下，您必须指定加密的口令。请参阅第 33 页的“管理 eapps.cfg 文件中的加密口令”。</p>
	SingleSignOn	TRUE	
	TrustToken		<p>输入 HELLO，或者您选择的连续字符串。</p> <p>在与定制的安全适配器配合使用的 Web SSO 模式下，指定的值作为口令参数被传送到定制的安全适配器，但是只有在此值与为定制的安全适配器定义的信任标记参数值相对应时才传送。</p>

表 13. eapps.cfg 文件中的参数值

部分	参数	示例录入值	准则
	UserSpec	REMOTE_USER	REMOTE_USER 是缺省的 Web 服务器变量，该变量的用户身份密钥被替换，供验证管理器检索。
	UserSpecSource	服务器	REMOTE_USER 是一个 Web 服务器变量。
	ProtectedVirtualDirectory		通常，您要输入在第 128 页的“创建被保护的虚拟目录”中创建的被保护的虚拟目录名称。 注释： 建议该参数应该始终用于 Web SSO 实施中。
[swe]	IntegratedDomainAuth	TRUE	如果是 Windows 集成身份验证，请将其设置为 TRUE。 参数的缺省设置为 FALSE。

编辑名称服务器参数

请为与所实施应用程序的对象管理器（例如，Call Center 对象管理器或 eService 对象管理器）对应的组件设置第 134 页的表 14 中列出的每个名称服务器参数。请在组件级别设置参数，并且遵循此表中提供的准则。

有关设置名称服务器参数以及参数意图的信息，请参阅第 251 页的“Siebel 网关名称服务器参数”。

表 14. 名称服务器参数

子系统	参数	准则
对象管理器	OM - 代理雇员	输入 PROXYE。
	OM - 用户名 BC 字段	留空。

表 14. 名称服务器参数

子系统	参数	准则
安全管理器	安全适配器模式	<p>安全适配器的模式。值包括：</p> <ul style="list-style-type: none"> ■ DB ■ LDAP ■ ADSI ■ CUSTOM <p>该参数可能在 Enterprise、Siebel 服务器或组件级别进行设置。有关详细信息，请参阅第 6 章“安全适配器验证”。</p>
	安全适配器名称	<p>安全适配器的名称。缺省提供的安全适配器名称包括：</p> <ul style="list-style-type: none"> ■ DBSecAdpt ■ LDAPSecAdpt ■ ADSISecAdpt <p>该参数可能在 Enterprise、Siebel 服务器或组件级别进行设置。有关详细信息，请参阅第 6 章“安全适配器验证”。</p>
<p>您所使用的安全适配器的企业资料或指定子系统。例如：</p> <ul style="list-style-type: none"> ■ 用于数据库安全适配器的 DBSecAdpt。 ■ 用于 LDAP 安全适配器的 LDAPSecAdpt。 ■ 用于 ADSI 安全适配器的 ADSISecAdpt。 	<p>有关配置每个安全适配器参数的详细信息，请参阅第 6 章“安全适配器验证”。</p> <p>另请参阅附录 B“与验证有关的配置参数”。</p>	

编辑应用程序配置文件中的参数

请根据第 136 页的表 15 中准则的指示，在配置文件中为您实施的 Siebel 应用程序提供参数值。有关 Siebel 应用程序配置文件的列表，请参阅 *Siebel System Administration Guide*。

有关编辑应用程序的配置文件以及参数意图的信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。

表 15. Siebel 应用程序配置文件的参数值

部分	参数	ADSI 安全适配器的准则
[SWE]	AllowAnonUsers	输入 TRUE。 注释： 如果未将该参数设置为 TRUE，则可能出现浏览器循环行为。
	SecureLogin	输入 TRUE 或 FALSE。如果输入 TRUE，用户填写的登录表单将通过安全套接层 (SSL) 传输。有关安全登录的其它要求的信息，请参阅第 140 页的“登录功能”中的安全登录主题。

重新启动服务器

您必须停止并重新启动 Web 服务器上的以下 Windows 服务，以激活对 AOM 配置所做的更改。

- **IIS 管理服务和万维网发布服务。**停止 IIS 管理服务，然后重新启动万维网发布服务。由于万维网发布服务是 IIS 管理服务的子服务，因此还会启动 IIS 管理服务。
- **Siebel 服务器系统服务。**停止并重新启动 Siebel 服务器。有关详细信息，请参阅 *Siebel System Administration Guide*。

测试 Web SSO 验证

以下测试确认 Web SSO 组件可以相互配合，以便：

- 允许用户登录到 Web 站点。
- 允许在 Web 站点级别验证的用户无需提供附加登录即可获得 Siebel 应用程序的访问权限。

要测试 Web SSO 验证

- 1 在 Web 浏览器上，输入您的 Web 站点的 URL，例如 <http://www.mycompany.com>。
此时应该出现包含 Web 站点登录表单的 Web 页。
- 2 使用您创建的测试用户的用户 ID 和口令登录。输入 TESTUSER 或您创建的用户 ID 以及 TESTPW 或您创建的口令。
您应该可以访问 Web 站点。
- 3 在 Web 浏览器上，输入用于连接到您的 Siebel 应用程序的 URL，例如 <http://www.mycompany.com/eservice>。或者，如果您提供了 Web 站点上的链接，请单击该链接。

您应该可以在无需登录的情况下以注册用户身份访问 Siebel 应用程序。

数字认证验证

数字认证是一个数字文档，它包括了受个人、组织或机器限制的公共密钥。认证由认证机构 (CA) 发行，它记录了用于确定所有者身份和分发认证的政策。

X.509 数字认证验证是一个基于标准的安全结构，用于保护私有信息和交易处理的安全。认证采用以下方式交换：即确保认证的提交者拥有与认证中所包含公共密钥相关联的私有密钥的方式。

Siebel Systems 支持 Web 服务器执行的 X.509 数字认证验证。Web 服务器执行数字认证验证，并且 Siebel 应用程序接受采用 Web SSO 形式的验证结果。

对于其现有 PKI（公共密钥基础设施）包含客户机认证的用户，Siebel Systems 支持使用 X.509 认证向应用程序验证用户。这一操作可通过将 SSL 与所支持的 Web 服务器的客户机验证功能配合使用完成认证处理来实现。

要实施 X.509 数字认证验证，您必须按照第 126 页的“实施 Web SSO 验证”中的介绍，遵循以下特定准则执行用于实施 Web SSO 验证的任务：

- 在 eapps.cfg 文件的 [defaults] 部分中输入以下参数：

参数	注释
SingleSignOn = TRUE	
TrustToken = HELLO	
ClientCertificate = TRUE	
UserSpec = CERT_SUBJECT 或 REMOTE_USER	对于 Windows 和 AIX 上的客户机验证，请使用 CERT_SUBJECT。对于其它 UNIX 平台，请使用 REMOTE_USER。
SubUserSpec = CN	该参数值告诉应用程序从认证名称中提取用户名。对于 Sun ONE Web Server，该设置将被忽略。
UserSpecSource = Server	

- 在每个受影响的应用程序的配置文件中（例如 eservice.cfg），在指定部分输入以下参数：

```
[SWE]
SecureBrowse = FALSE
```

- 对于用于支持基于认证验证的每个安全适配器（例如 LDAPSecAdpt），请定义以下参数值：

```
SingleSignOn = TRUE
TrustToken = HELLO
```

有关数字认证实施的附加信息，请参阅 Siebel SupportWeb 上提供的 *Siebel 7 中基于认证的验证及其应用*。

用户身份的来源

此选项可通过以下验证策略实施：

■ Web SSO 验证

在 Web SSO 实施中，SWSE 从 Web 服务器环境变量或 HTTP 请求标题变量得出用户的用户名。您必须指定一个来源或另一个来源。

警告：如果您的实施使用标题变量传送从第三方验证服务获得的用户的身份密钥，则应该由第三方或定制的验证客户机负责正确设置标题变量。标题变量应该只在验证用户之后才设置，而且应该在适当的时候由验证客户机清除。如果标题变量将身份密钥传送给 Siebel 验证管理器，并且验证了信任标记，则表示已接受用户作为已验证的用户。

要指定用户名的来源

- 在 eapps.cfg 文件中，在 [defaults] 部分或用于各单个应用程序的部分（例如 [/eservice]）中提供以下参数值：
 - UserSpec = 变量的名称。例如：REMOTE_USER（如果 UserSpecSource 设置为 Server。）如果 UserSpecSource 设置为 Header，UserSpec 的值将是传送到 HTTP 标题的变量；变量的名称前面不应该加上 HTTP_。
 - UserSpecSource = Server（如果您使用 Web 服务器环境变量。）
 - UserSpecSource = Header（如果您使用 HTTP 请求标题变量。）

注释：如果您使用标题变量传送从 IIS Web 服务器获得的用户名，请首先配置 IIS Web 服务器，以允许匿名访问。请在 IIS 服务管理器中为缺省的 Web 站点设置此安全性。

有关设置 eapps.cfg 文件中参数的信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。

8

Siebel Web Server Extension 的安全功能

本章介绍了与安全性和 Siebel Web Server Extension (SWSE) 有关的多项选项。它包括以下主题：

- 第 139 页的“配置安全视图”
- 第 140 页的“登录功能”
- 第 143 页的“Cookie 和 Siebel 应用程序”

配置安全视图

您可以要求为 Siebel 应用程序中的特定视图使用 HTTPS 协议的 URL。

注释：只有标准交互的应用程序才能够有选择地指定安全视图，高交互应用程序则不具备这样的能力。

以下因素决定了 Siebel Web 引擎是否验证要求使用 HTTPS 协议访问视图：

- 视图“安全”属性的值（TRUE 或 FALSE）。有关视图“安全”属性的信息，请参阅 *Configuring Siebel eBusiness Applications*。
- SecureBrowse 参数的值（TRUE 或 FALSE），该参数位于应用程序配置文件（例如 siebel.cfg）的 [SWE] 部分中。
 - 如果 SecureBrowse 设置为 TRUE，则整个应用程序中的所有视图都需要使用 HTTPS，而不考虑单个视图的“安全”属性是如何设置的。
 - 如果 SecureBrowse 设置为 FALSE，整个应用程序的所有视图则使用 HTTP，但“安全”属性设置为 TRUE 的视图除外。安全视图需要使用 HTTPS。

如果您计划使用 HTTPS 协议，记住以下几点：

- 您可以在 Siebel 客户应用程序中的安全视图与非安全视图之间切换，但是在雇员应用程序（例如 Siebel Call Center）中则不能。对于雇员应用程序，如果任何视图要成为安全视图，则所有的视图都必须是安全视图。请将 SecureBrowse 的值设置为 TRUE。
- 您必须将 Web 服务器配置为支持 HTTPS。
- Sun ONE Web Server 不支持在 Siebel 应用程序的安全视图与非安全视图之间切换。如果您要使用 Sun ONE Web Server，请将 SecureBrowse 的值设置为 TRUE。

登录功能

本节介绍了与用户登录到 Siebel 应用程序有关的功能和注意事项。

登录页或登录表单嵌入在 Siebel 应用程序页中，它是收集用户证书的方式。第 140 页的图 8 显示嵌入了登录表单的 Siebel eService 主页。

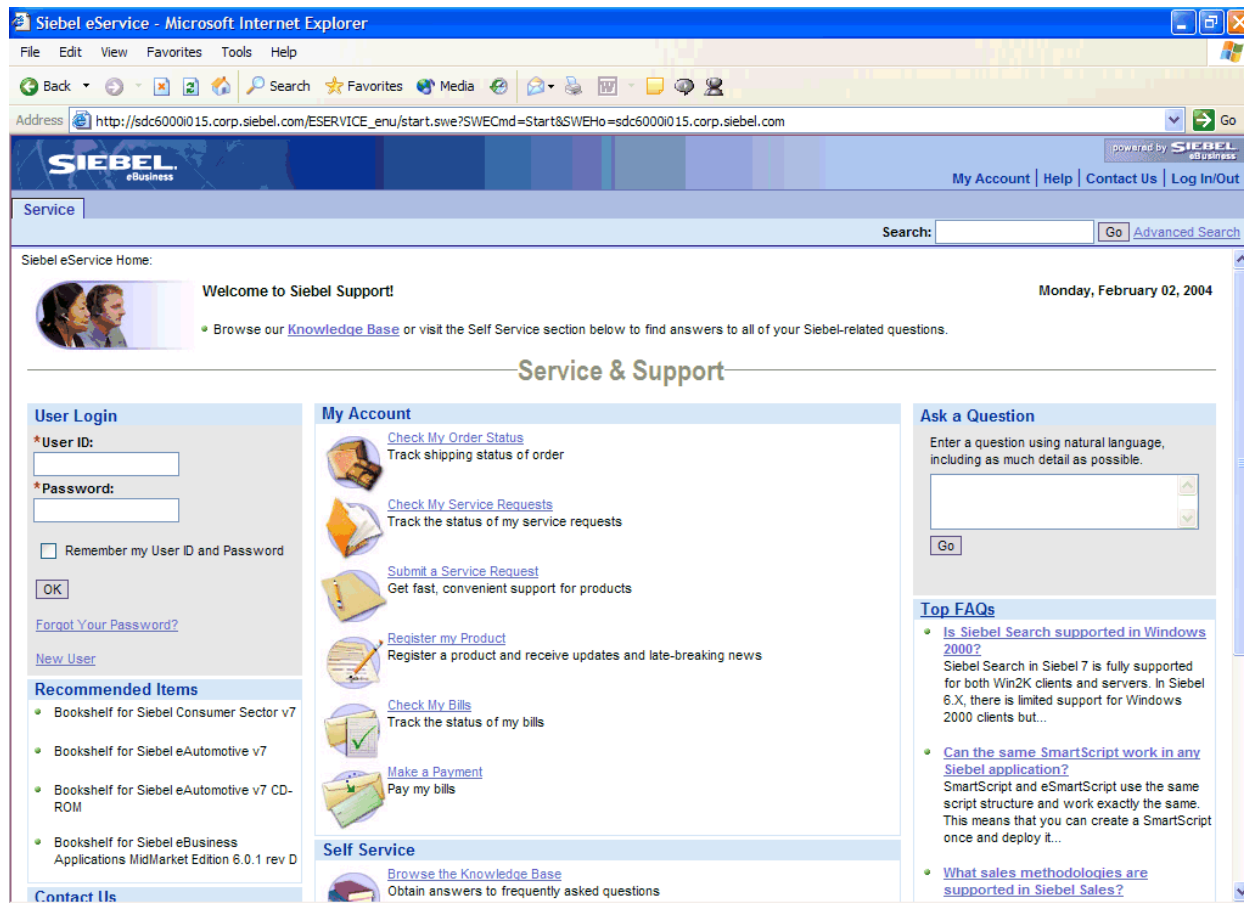


图 8. Siebel eService 主页中嵌入的登录表单

用户必须登录才能将自己标识为注册用户，从而获得访问 Siebel 应用程序中被保护视图的权限。被保护的视图专门用于显式登录。如果 Siebel 应用程序允许匿名浏览，那些不是专门用于显式登录的视图则可以用于匿名浏览。

有关设置视图属性的信息，请参阅 *Configuring Siebel eBusiness Applications*。

有关匿名浏览的信息，请参阅第 118 页的“配置匿名用户”。

除了收集用户证书之外，Siebel 应用程序还在登录表单中提供了其它的功能，例如，记住用户名和口令，并提供忘记口令支持。

或者，您可以将 Siebel 应用程序配置为，通过在访问应用程序的 URL 中提供所需的用户 ID 和口令而绕过登录表单。

安全登录

通过安全登录，您可以指定 Siebel Web 引擎使用安全套接层 (SSL)，也就是通过 HTTPS，将用户在浏览器的登录表单中输入的用户证书传送给 Web 服务器。

安全登录可以在以下验证策略中实施：

- 安全适配器验证：数据库验证
- 安全适配器验证：LDAP、ADSI 或定制
- Web SSO 验证

要实施安全登录

- 对于实施安全登录的每个 Siebel 应用程序，请在应用程序配置文件 [SWE] 部分中设置以下参数值。例如，编辑 Siebel eService 的 eservice.cfg 文件。

```
SecureLogin = TRUE
```

- 要实施安全登录，您还必须在安装 SWSE 的 Web 服务器上具有认证机构发行的认证。

有关设置 Siebel 配置参数的信息，请参阅[附录 B “与验证有关的配置参数”](#)。

记住我的用户 ID 和口令

用户在登录到 Siebel 应用程序时，可以选择“记住我的用户 ID 和口令”复选框。如果选择该复选框，只要用户没有使用“文件”>“注销”命令注销 Siebel 应用程序，就可以访问同一个 Siebel 应用程序，而不必再次登录。

“记住我的用户 ID 和口令”功能在会话启动时，使用 Siebel Web 引擎提供的自动登录证书 cookie。该功能需要启用此 cookie。

有关 cookie 和会话管理以及自动登录证书 cookie 的信息，请参阅[第 143 页的“Cookie 和 Siebel 应用程序”](#)。

忘记口令？

“忘记口令？”功能使忘记登录口令的用户可以获得新的口令。seed 工作流程过程提供了一些交互式问题，用户通过回答这些问题可以表明自己的身份。

有关“忘记口令？”功能的信息，请参阅[第 161 页的“管理“忘记口令””](#)。

帐户策略

为了增强安全性，您可能需要实施以下帐户策略：帐户策略是验证服务的功能。如果要实施帐户策略，您则负责通过验证服务供应商提供的管理功能设置这些策略。

- 口令语法规则，例如口令最小长度。在创建或更改口令时，Siebel 应用程序将强制执行在外部目录中定义的最小长度要求和其它语法规则。
- 尝试登录失败的次数超过指定次数之后，执行帐户封锁。封锁帐户可以防止他人通过猜测口令进行攻击。对于外部目录已禁用的帐户，Siebel 应用程序支持帐户封锁条件。
- 口令在经过指定的时间期后将会过期。您可以将配置外部目录配置为使口令过期，并且警告用户口令快要过期。Siebel 应用程序可以识别外部目录发出的口令过期警告，并且用户会收到更改口令的通知。

口令过期

口令过期由外部 LDAP 目录或 Active Directory 处理，并且取决于第三方目录产品对这种行为的配置。

例如，在口令快要过期时，目录可能向 Siebel 应用程序提供在用户登录时显示的警告消息。此类警告表示用户的口令快要过期，应该更改口令。如果用户对此类警告置之不理并且让口令过期，则他（她）需要首先更改口令，然后才能登录应用程序。或者，口令一旦过期，用户可能无法进入该应用程序。

每个目录供应商的口令过期配置步骤各不相同。有关详细信息，请参阅随目录产品提供的文档。下面提供了有关用于 Active Directory 的口令过期的详细信息。

口令过期可以在以下验证策略中实施：

- 安全适配器验证：LDAP、ADSI 或适用的定制安全适配器；RDBMS 支持的数据库验证

ADS 的口令过期

在 ADS 中，影响口令状态的因素包括以下属性和参数：

- 口令永不到期（用户对象的属性）
- 在下次登录时用户必须更改口令（用户对象的属性）
- 用户上次设置口令的时间（用户对象的属性）
- 最大口令时限（域的属性）
- 口令过期警告天数（ADSI 安全适配器的参数）

您在为 ADSI 配置口令过期时，请在 ADSI 安全适配器中添加参数口令过期警告天数（别名是 PasswordExpirewarnDays）。请将该值设置为在用户的口令过期之前发出警告消息的天数。

注释：属性口令永不到期和在下次登录时用户必须更改口令相互排斥，因此用户不能同时选择这两个参数。

每位用户的口令状态由以下逻辑决定：

- 如果为用户选择了口令永不到期，则不管如何设置其它属性，该用户则从来不会遇到口令过期的错误。
- 反之，如果为用户选择了在下次登录时用户必须更改口令，则不管如何设置其它属性，该用户将会遇到口令过期的错误。
- 如果没有为用户选择上述任何一个属性，则会出现以下状况：
 - 如果域的最大口令时限设置为 0，用户则不会遇到口令过期的错误。域中的口令不会过期。
 - 或者，如果当前时间与用户上次设置口令的时间（该用户的用户上次设置口令的时间属性的值）之间的时差超过了最大口令时限的值，该用户将遇到口令过期的错误。
 - 或者，如果当前时间与用户上次设置口令的时间之间的时差小于口令过期警告天数（为 ADSI 安全适配器设置），该用户将遇到口令过期的警告消息。
 - 或者，如果当前时间与用户上次设置口令的时间之间的时差小于最大口令时限并且超过口令过期警告天数，用户将成功登录并且不会遇到任何错误或警告消息。

注释：请按照第三方文档，确认所有第三方目录产品的行为和配置。

URL 登录

用户可以通过在 URL 中提供作为参数的用户证书，登录到 Siebel 应用程序。用户不必在登录表单中手动输入证书。

警告：在使用 URL 登录时，用户口令可能通过网络以纯文本形式传输。

越简单越不安全。选择 Web SSO 的形式进入 Siebel 应用程序，就是要在应用程序的导航入口处向 Siebel 客户或合作者应用程序提出显式登录的要求。如果 Siebel 应用程序的导航入口数很少，而且您不关心用户是否知道自己的 Siebel 用户名和口令，并且您没有部署完整的 Web SSO 基础设施，那么这种选择最适合您。

以下是显示 URL 语法的示例：

```
http://yourhost/eservice/
start.swe?SWECmd=ExecuteLogin&SWEUserName=HKIM&SWEPassword=HKIM
```

注释：URL 中的参数名称区分大小写。

您可以创建单一 URL，除用户的登录证书之外，该 URL 还包含预定义视图的路径。您必须使用如以下示例所示的 SWE 表达式。以下示例显示在用户登录后到某个服务请求的向下搜索情况。在该示例中，HKIM 的用户名和口令使用转义符表示：%48%4B%49%4D。（请注意，此类字符串不安全。）

```
http://siebel.com/eservice/
start.swe?SWECmd=ExecuteLogin&SWEUserName=%48%4B%49%4D&SWEPassword=%48%4B%49%4D
&SWEAC="SWECmd=InvokeMethod,SWEMethod=Drilldown,SWEView=Service+Request+List+View+
(SCW),SWEApplet=Service+Request+List+Applet+(SCW),SWEField=SR+Number,SWERowIds=SWE
RowId0%3d1-15P"
```

注释：在 SWEAC 表达式中，您必须使用逗号（而不是 & 符号）作为参数间的分隔符。

Cookie 和 Siebel 应用程序

在 Web 浏览器中运行的 Siebel 应用程序为了各种目的可以根据需要使用 cookie。一些可选的 Siebel 应用程序功能要求可以使用 cookie。本节详细介绍了每一种特殊类型的 cookie。

除非另有说明，否则，本节中介绍的所有 cookie 同时适用于高交互和标准交互的应用程序。Siebel 应用程序使用的所有 cookie 都通过 RSA 提供的标准加密算法加密。

有关在 Microsoft Internet Explorer Web 浏览器中启用 cookie 的信息，请参阅第 146 页的“为 Siebel 应用程序启用 Cookie”。

Siebel 应用程序使用以下类型的 cookie：

- **会话 cookie。**管理 Siebel Web 客户机用户的用户会话。有关详细信息，请参阅第 144 页的“会话 Cookie”。
- **自动登录证书 cookie。**存储 Siebel Web 客户机用户的用户证书。有关详细信息，请参阅第 145 页的“自动登录证书 Cookie”。
- **Siebel QuickStart cookie。**在使用 Siebel QuickStart 时移动 Web 客户机使用该 cookie。有关详细信息，请参阅第 145 页的“Siebel QuickStart Cookie”。

会话 Cookie

会话 cookie 由为用户的会话生成的会话 ID 组成。该 cookie 用于管理用户会话的状态。该会话 cookie 只适用于 Siebel Web 客户端。

SWSE 上的 cookie 模式由 eapps.cfg 文件中的 SessionTracking 参数的设置决定。该设置为自动、Cookie 或 URL。

- 如果使用缺省的 SessionTracking 设置自动，SWSE 则在基于 cookie 的模式下运行。然而，如果浏览器不支持 cookie 或者用户的浏览器配置为不允许使用 cookie，SWSE 将在 cookieless 模式下工作，并使用 URL。
- 要强制 SWSE 始终使用基于 cookie 的模式，请将 SessionTracking 设置为 Cookie。
- 要强制 SWSE 始终使用 cookieless 模式，请将 SessionTracking 设置为 URL。

有关设置 eapps.cfg 文件中的参数值的信息，请参阅附录 B “与验证有关的配置参数”

下面是与设置 SessionTracking 参数有关的 Siebel 应用程序的一些要求：

- “快速打印”功能需要将 SessionTracking 设置为自动（缺省值）或 URL。有关使用此打印功能的信息，请参阅基础。有关该功能对浏览器的要求的信息，请参阅 *Siebel System Administration Guide*。
- 对内 EAI HTTP 传输需要使用基于 cookie 的模式。在 eapps.cfg 文件以 eai 开头的部分中，您可以忽略 SessionTracking 参数，或者将其设置为自动（缺省值）或 Cookie。有关对内 EAI HTTP 传输的详细信息，请参阅 *Transports and Interfaces: Siebel eBusiness Application Integration Volume III* 以及其它相关的 Siebel EAI 文档。
- “记住我的用户 ID 和口令”功能需要将 SessionTracking 设置为自动（缺省值）或 Cookie。确定在浏览器中启用了 cookie。另请参阅自动登录证书 cookie 的说明。
- 有关涉及到 cookie 的服务器重定向机制的信息，请参阅 *Siebel Portal Framework Guide*。

基于 Cookie 的模式

本节介绍了基于 cookie 的模式的行为。基于 cookie 的模式适用于 SessionTracking 设置为 Cookie，或者 SessionTracking 设置为自动并且用户的浏览器接受 cookie 时。

在用户成功登录到应用程序之后，将生成唯一的会话 ID。会话 ID 的组件在 Siebel 服务器中生成，并且被发送到 SWSE 中运行的会话管理器。在基于 cookie 的模式下，会话 ID 以非持续 cookie 的形式传送给用户的浏览器。

会话 ID 组件包括适用的服务器 ID、流程 ID 和任务 ID，并且加上时间戳。所有的值都采用十六进制形式，如下所示：

```
server_ID.process_ID.task_ID.timestamp
```

例如，会话 ID 可能类似于：

```
sn=!1.132.6024.3ca46b0a
```

该会话 cookie 是非持续的，并且只存储在内存中。在会话期间，它一直位于浏览器中，在用户注销或超时，则将被删除。

如果将 eapps.cfg 文件中的 EncryptSessionId 参数设置为 TRUE，cookie 中的会话 ID 则被加密。对会话 ID 加密可以防止未授权的攻击者捕获 cookie 并确定其格式。

对于在会话期间用户提出的每一个应用程序请求，cookie 将作为请求的一部分在 HTTP 标题中传送给 Web 服务器。如果 HTTP 标题中没有有效的 cookie，Web 服务器将不会批准该请求。

注释：如果用户在应用程序会话期间更改口令，会话 cookie 中的口令信息则可能不再允许用户在会话期间访问 Siebel 报表服务器。（如果同时使用数据库验证和口令散列处理，则会出现该问题。）在更改口令之后，用户应该注销，然后重新登录才能运行报表。

Cookieless 模式

本节介绍了 cookieless 模式的行为。Cookieless 模式适用于 SessionTracking 设置为 URL，或者 SessionTracking 设置为自动并且用户的浏览器不接受 cookie 时。

在 cookieless 模式下，会话 ID 作为 SWE 中构成 URL 的参数传送。从浏览器传送至 Web 服务器的任何 URL 请求都必须包括有效的会话 ID，否则，该请求将会被 Web 服务器拒绝。

如果将 eapps.cfg 文件中的 EncryptSessionId 参数设置为 TRUE，URL 中的会话 ID 则被加密。

如果浏览器未将会话 cookie 发送回 Siebel Web 引擎，则调用 cookieless 会话。如果用户的浏览器禁用 cookie 或者浏览器不支持 cookie，则可能导致出现此事件。

您可能出于某些原因（例如，安全要求不允许使用 cookie）希望对于所有会话，Siebel 应用程序都在 cookieless 模式下工作。

自动登录证书 Cookie

自动登录证书 cookie 是“记住我的用户 ID 和口令”功能的基础。该 cookie 由指定用户的用户名和口令以及访问应用程序所用的 URL 字符串组成。自动登录证书 cookie 是持续性的，并且以加密形式存储在用户的浏览器中（它始终被加密）。该 cookie 只适用于 Siebel Web 客户机。

自动登录证书 cookie 不是必备项。它是一种可选方式，允许用户不必在每次登录时都要输入用户名和口令。如果用户以后通过另一个浏览器窗口访问应用程序 URL，用户信息就会被提供给应用程序，从而不需要用户重新登录。

自动登录证书 cookie 的格式如下所示：

```
start.swe=encrypted_user_information
```

注释：自动登录证书 cookie 提供的功能不可用于 cookieless 模式。

Siebel QuickStart Cookie

Siebel QuickStart cookie 是在使用 Siebel QuickStart 时为移动 Web 客户机创建。该 Siebel 客户机只支持高交互模式下的雇员应用程序。

Siebel QuickStart cookie 的名称是 siebel.local.client，它是持续的 cookie，并且不包含 Siebel 会话 ID 数据。

有关 Siebel QuickStart 的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

为 Siebel 应用程序启用 Cookie

本节介绍了如何启用 Microsoft Internet Explorer Web 浏览器以处理 Siebel 应用程序使用的 cookie。

请复审有关所支持浏览器版本的说明。

要使用 Internet Explorer 6.0 启用 cookie

- 1** 选择“工具”>“Internet 选项”。
- 2** 单击“隐私”选项卡。
- 3** 在“隐私”设置中，单击“高级”。
- 4** 验证已选中“覆盖自动 cookie 处理”。同时考虑：
 - 如果“第一方 Cookie”设置为“接受”，则启用所有的 Siebel cookie。
 - 如果无法选择“第一方 Cookie”，您仍然可以通过选择“总是允许会话 cookie”启用会话 cookie。
- 5** 单击“确定”，然后再次单击“确定”。

要使用 Internet Explorer 5.5 启用 cookie

- 1** 选择“工具”>“Internet 选项”。
- 2** 单击“安全”选项卡。
- 3** 在“安全”设置的“允许使用存储在您计算机上的 cookies”下面，选择“启用”或“提示”。

该设置可以持续存储自动登录证书 cookie，并且对于移动 Web 客户机来说，就是存储 Siebel QuickStart cookie。
- 4** 在“安全”设置的“允许使用每个对话 cookies（未存储）”下面，选择“启用”或“提示”。

该设置可以在会话期间存储会话 cookie。
- 5** 单击“确定”，然后再次单击“确定”。

9

用户管理

本章提供了有关注册和管理 Siebel 雇员、合作者和客户应用程序的用户的信息。它包括以下主题：

- 第 147 页的“关于用户注册”
- 第 148 页的“配置匿名浏览”
- 第 150 页的“关于自行注册”
- 第 152 页的“实施自行注册”
- 第 161 页的“管理“忘记口令””
- 第 166 页的“用户的内部管理”
- 第 167 页的“将用户添加到 Siebel 数据库中”
- 第 172 页的“用户的授权管理”
- 第 176 页的“维护用户资料”

关于用户注册

如果用户不是注册的 Siebel 应用程序用户，则不具有用于访问 Siebel 数据库的已验证权限。未注册的用户具有各种访问级别，具体视 Siebel 应用程序而定。用户至少可以访问登录页。缺省情况下，或者视您的配置而定，未注册的用户可能有权访问某个特定 Siebel 应用程序的一些或所有视图。

通常，您为注册用户授予对数据和功能的访问权限要多于为未注册的用户授予的权限。用户可以注册成为一些或所有 Siebel 应用程序的用户。您可以为不同的注册用户授予对数据库和功能的不同访问级别。

通常，在执行以下任务时注册用户：

- 在 Siebel 数据库中创建用户记录。
- 在用户登录时提供验证用户的方法。

用户可以通过以下一种或多种方式进行注册，具体视 Siebel 应用程序而定：

- **自行注册。**用户可以在 Web 站点自行注册。
- **内部注册。**公司的管理员可以注册用户。
- **外部注册。**授权的管理员（客户或合作者公司的某位用户）可以注册用户。

如果您实施外部验证系统，则不管是通过自行注册还是由管理员注册的方式将用户添加到 Siebel 数据库中，都未必能将用户的登录数据传播到外部验证系统中。如果登录证书没有传播到验证系统中，则您必须在验证系统中单独创建登录证书。

如果您实施数据库验证，则将具有用户 ID 和口令的用户添加到数据库中就足以允许对该用户进行验证。

有关验证和传播用户数据的详细信息，请参阅第 6 章“安全适配器验证”。

用户注册的要求

您必须完成以下实施步骤，才能注册用户：

- 安装 Siebel 应用程序。
- 设置和配置用户验证体系结构。
- 根据验证体系结构的要求，为用户创建数据库帐户。

有关用户验证的信息，请参阅第 6 章“安全适配器验证”。

用户注册的 Seed 数据

在安装 Siebel eBusiness Applications 时，系统为您提供的 Seed 数据与用户注册、用户验证及用户对 Siebel 应用程序的访问权限相关。Seed 数据包括用户、职责、职位、组织和数据库登录。对 Seed 数据的引用贯穿本章始末。

有关 Seed 数据的详细信息以及查看和编辑 Seed 数据的过程，请参阅附录 C“Seed 数据”。

配置匿名浏览

本节提供了有关匿名浏览以及如何为 Siebel 应用程序配置匿名浏览的信息。

关于匿名浏览和未注册的用户

一些 Siebel 应用程序允许匿名浏览用于公共访问的视图，这是一项缺省功能。通常，匿名浏览适用于 Siebel 客户和合作者应用程序，而不适用于雇员应用程序。但是，您可以配置任何 Siebel 应用程序，以允许或禁止匿名浏览。

未注册的用户可以通过匿名用户身份访问应用程序视图和数据库。匿名用户是 Siebel 数据库中的一项记录，它还可以在用户验证和用户自行注册期间执行功能。如果您实施外部验证系统，匿名用户则在用户目录中具有相应的记录。

即使应用程序不允许未注册的用户进行访问，仍然需要提供匿名用户。应用程序对象管理器 (AOM) 在初次启动时，将使用匿名用户帐户连接至数据库并检索信息（例如许可证密钥），然后再显示登录页。

有关用户验证中匿名用户角色的信息，请参阅第 6 章“安全适配器验证”。

实施匿名浏览

为了使未注册的用户可以访问视图，您必须执行以下任务：

- 修改匿名用户记录。
- 设置配置参数。
- 修改视图以支持匿名浏览，或者改为要求显式登录。

对于在缺省情况下实行匿名浏览的 Siebel 应用程序，您应该确认已经完成这些任务。

修改匿名用户记录

匿名用户是 Siebel 数据库中的一条记录，而且如果您实施外部用户验证，则在外部的用户目录中将出现相应的记录。匿名用户是用户验证、匿名浏览和自行注册的一个组成部分。对于允许匿名浏览的应用程序，匿名用户可以看到允许匿名浏览的页面。

您应该先设置用户验证体系结构，然后为用户访问配置应用程序。因此，匿名用户应该已存在于 Siebel 数据库和目录中。

为数据库中的用户记录分配的职责包含用户有权访问的一个视图列表。您必须确认用于 Siebel 应用程序的匿名用户包括适当的职责，以便未注册的用户可以看到您希望他们看到的视图。

如果您在验证设置中选择使用 Seed 匿名用户，则应该验证它的 Seed 职责是否包括您要为匿名浏览提供的视图。例如，您将 GUESTCST Seed 用户用于 Siebel 客户应用程序，则应该验证它的职责 Web 匿名用户是否包括所需的视图。如果职责没有包括所需的视图，您可以执行以下操作之一：

- 创建包括所缺少视图的一个或多个附加职责，然后将这些职责添加到匿名用户的“职责”字段中的现有 Seed 职责中。用户有权访问所有已分配职责中的所有视图。
- 复制 Seed 职责记录，将缺少的视图添加到副本中，然后将匿名用户记录中的职责替换为已修改的职责。

注释：您不能直接修改 Seed 职责。

有关创建职责或为职责添加视图的信息，请参阅第 10 章“配置访问控制”。

有关将职责分配给用户的信息，请参阅第 166 页的“用户的内部管理”。

有关 Seed 数据的信息，请参阅附录 C“Seed 数据”。

为匿名浏览设置配置参数

要允许匿名浏览，您必须设置以下配置参数。

- **AllowAnonUsers**。在 Siebel 应用程序配置文件中将该参数设置为 TRUE。
有关在应用程序配置文件中设置参数值的信息，请参阅第 256 页的“Siebel 应用程序配置文件参数”。
- **AnonUserName**。eapps.cfg 文件中的该参数是目录以及 Siebel 数据库中存储的匿名用户的用户名。
匿名用户提供了目录与 AOM 之间的绑定，从而允许向尚未登录的用户显示 Siebel 应用程序主页。同样，该匿名用户还要提供登录才能看到允许匿名浏览的其它页面。
有关在 eapps.cfg 文件中设置参数值的信息，请参阅第 247 页的“eapps.cfg 文件中的参数”。
- **AnonPassword**。eapps.cfg 文件中的该参数是与 AnonUserName 配对的已验证的口令。

为匿名浏览或显式登录配置视图

即使匿名用户的职责中包括某个视图，但是如果该视图被指定为需要显式登录，未注册的用户则仍然无法访问该视图。被指定为需要显式登录的视图要求查看者是经过验证的注册用户。

以下过程展示了 Siebel Tools 任务中的主要步骤。有关在 Siebel Tools 中修改视图属性的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要设置或删除视图的显式登录要求

- 1 打开 Siebel Tools。
- 2 选择“工具”>“锁定项目”。
- 3 在“对象浏览器”中，选择“视图”对象类型。
此时将出现“视图”列表。
- 4 选择一个视图。
- 5 对于要求显式登录的每个视图，将“显式登录”属性设置为 TRUE。或者，将其设置为 FALSE 以允许匿名浏览。
- 6 重新编译 Siebel 库文件，并取消锁定项目。

关于自行注册

一些 Siebel 应用程序允许用户自行注册，这是一项缺省功能。本节遵守有关自行注册功能的以下原则，自行注册功能是 Siebel 应用程序提供的缺省功能：

- 自行注册适用于 Siebel 客户和合作者应用程序。
- 自行注册只能在其客户机使用标准交互的 Siebel 应用程序中实施，但是无法在 Siebel 雇员应用程序或使用高交互客户机的其它任何 Siebel 应用程序中实施。
- 您可以配置任何符合条件的 Siebel 应用程序，以允许或禁止自行注册。
- 您可以通过允许自行注册的 Siebel 应用程序实施 LDAP/ADSI 安全适配器验证。

要为使用 Web SSO 用户验证的应用程序实施自行注册，您应该负责在 Web 站点级别配置自行注册功能，并负责使用户数据与 Siebel 数据库同步。Siebel 应用程序文档中未提供配置准则。在您实施数据库验证时，自行注册不可行。

注释：如果您在用户验证环境中使用适配器定义的用户名，则无法实施一些工具，这些工具使您可以在 Siebel 应用程序中管理存储在目录中的用户的 Siebel 用户 ID，包括用户自行注册。有关用户验证的信息，请参阅第 6 章“安全适配器验证”。

Siebel 客户和合作者应用程序的自行注册功能随 Siebel eBusiness Applications 一起安装。

自行注册的用户体验

最终用户的自行注册体验随应用程序而有所不同。特定于应用程序的一些功能是：

- **Siebel eService。**用户自行注册以访问更多的服务。
- **Siebel eSales。**用户自行注册以获得在线采购的许可。
- **Siebel Partner Portal。**用户作为个人自行注册以成为具有有限访问权限的合作者用户，或者用户按照他或她公司申请获得批准以成为合作者的请求自行注册。在任何一种情况下，都会为用户分配有限的职责，职责中包含数据的视图，但不包含交易数据的视图。该职责不同于所批准的合作者公司中合作者用户的职责。

有关在 Siebel Partner Portal 的注册合作者和合作者用户的详细信息，请参阅 *Siebel Partner Relationship Management Administration Guide*。

要自行注册

- 1 用户在 Siebel 应用程序页（例如，Siebel eService 的主页）中单击“新建用户”。

此时将出现“个人信息”表单。

- 2 用户填写表单，然后单击“下一步”。例如，Siebel eService 的字段如下所示。

字段	准则
名字	必需。输入任何名称。
姓氏	必需。输入任何名称。
电子邮件	必需。输入任何有效的电子邮件地址。
时区	必需。指定时区。
用户 ID	必需。输入简单且连续的用户 ID，每个用户的用户 ID 必须唯一。通常，由用户提供该用户 ID 以便登录。 根据您的配置验证的方式，用户使用该标识符可能可以，也可能无法登录。
口令	可选（对于某些验证实施是必需项）。 输入简单且连续的登录口令。口令必须符合验证系统的语法要求，但是在该表单中不会检查口令是否符合要求。 如果是 LDAP/ADSI 安全适配器验证，口令将传播至用户目录。如果是数据库验证，口令将传播至数据库。 有关用户验证体系结构的信息，请参阅第 6 章“安全适配器验证”。
验证口令	在需要提供口令时必需。
口令提示问题	必需。用户输入一个问题短语，该问题的答案通常只有该用户才知道。如果该用户单击“忘记口令？”，将会显示该短语，然后该用户必须输入正确的答案，才能收到新的口令。
口令提示问题答案	必需。用户提供被视为提示问题正确答案的单词或短语。

此时将出现“联系人信息”表单。该表单中的字段随应用程序而有所不同。

- 3 用户填写“联系人信息”表单，然后单击表单底部的一个按钮以继续。按钮的名称和数量随应用程序而有所不同。
- 4 如果应用程序是 Siebel Partner Portal 或 Siebel eSales，则用户可以执行以下操作之一：
 - Siebel Partner Portal 自行注册的用户选择作为个人注册，或者按照他或她公司申请获得批准以成为合作者的请求注册。在任何一种情况下，用户都要填写要求提供公司信息的表单。
 - Siebel eSales 自行注册的用户填写表单，提供以下部分或全部信息：付款信息、地址信息或无线访问信息。
- 5 在“使用条款”表单中，用户必须同意接受许可协议的条款才能注册。

此时将出现“注册确认”消息。

实施自行注册

自行注册包含以下组成部分：

- Siebel Seed 工作流程过程为用户提供了一系列用于收集新用户数据的交互表单。这些流程还会验证数据，并将许多数据写入到 Siebel 数据库的新用户记录中。
- 数据库的新用户记录中的一些字段将根据匿名用户记录中的字段自动填入内容。
- 在用户目录中创建新记录。安全适配器根据该记录验证用户。字段将根据用户在表单中输入的数据自动填入内容。

您必须执行以下一项或多项任务才能实施自行注册：

- （可选）修改匿名用户记录。
- 设置配置参数。
- 激活自行注册的工作流程过程。

修改匿名用户记录

匿名用户是 Siebel 数据库中的一项记录，并且在用户目录中有相应的记录。匿名用户是用户验证、匿名浏览和自行注册的一个组成部分。

您应该先设置用户验证体系结构，然后为用户访问配置应用程序。因此，匿名用户应该已存在于 Siebel 数据库和您的用户目录中。

有关用户验证的信息，请参阅第 6 章“安全适配器验证”。

同一实施中的不同 Siebel 应用程序可能使用不同的匿名用户。在 Siebel 数据库中提供了两种用户记录（分别由其用户 ID GUESTCST 和 GUESTCP 标识）作为 Seed 数据，以用作匿名用户。附录 C“Seed 数据”介绍了 Seed 数据用户、职责及其适用的 Siebel 应用程序。

在用户自行注册时，“用户注册”业务组件中将创建一个新记录。“用户注册”业务组件与“用户”业务组件基于相同的表，因此，实际上创建了新的用户记录。

注释：在用户通过合作者应用程序（例如，Siebel Partner Portal）自行注册时，数据也会被写入到“联系人”业务组件（或等效的业务组件）。

以下关键字段将根据 Siebel 数据库的匿名用户记录中的字段自动填入内容：

- **职责。**新用户的职责从匿名用户的“新职责”字段中继承。用户的职责决定了用户有权访问的视图列表。
- **新职责。**新用户的“新职责”字段值也是从匿名用户的“新职责”字段中继承。以常规方式注册的用户不使用“新职责”字段。一些 Siebel 应用程序允许将客户或合作者用户升级为授权的管理员。授权的管理员可以注册其他用户，这些用户从授权的管理员的“新职责”字段中继承职责。

“新职责”字段是一个单值字段。因此，如果匿名用户的“新职责”字段中的 Seed 职责没有为自行注册的用户提供所需的所有视图，您必须执行以下任务之一：

- 使用您创建的职责替换“新职责”值。
- 复制 Seed 职责记录，将缺少的视图添加到副本中，然后将新职责替换为已修改的职责。

注释：您不能直接修改 Seed 职责。

有关创建职责或为职责添加视图的信息，请参阅第 10 章“配置访问控制”。

有关 Seed 数据的信息，请参阅附录 C“Seed 数据”。

为自行注册设置配置参数

如果您实施安全适配器验证，则可以通过 Siebel 应用程序管理用户目录。内部管理员、授权的管理员或用户自行注册时所做的更改（例如，添加用户或更改口令）将传播到用户目录。

在用户从 Siebel Web 客户机自行注册时，为了使用户数据（包括用户名和口令）传播到用户目录中，请将安全适配器的 PropagateChange 参数设置为 TRUE。有关设置该参数的信息，请参阅第 251 页的“Siebel 网关名称服务器参数”。

注释：如果您未按照此处的介绍配置安全适配器验证体系结构以允许通过 Siebel Web 客户机进行管理，则无论何时在 Siebel 数据库中创建该应用程序的新用户时，您都必须在用户目录中手动创建记录。

激活自行注册的工作流程过程

在您安装 Siebel eBusiness Applications 时，系统会为您提供一些工作流程过程，用于控制一些 Siebel 应用程序的自行注册。

注释：有关如何查看、修订、激活和部署工作流程过程的信息，请参阅 *Siebel Business Process Designer Administration Guide*。

自行注册工作流程过程将同时提供一系列供用户填写、执行数据验证和调用数据库操作的表单。

- **用户注册 - 初始流程。**为了进行自行注册，在用户单击登录表单中的“新建用户”或者在 Siebel eSales 的购物过程中单击“结帐”时，便会调用该流程。在登录表单中单击“忘记口令？”时，也会调用该流程。该流程将分支为以下子流程之一：
 - 用户注册流程
 - 用户注册 - 忘记口令流程
- **用户注册流程。**这是自行注册的主流程。它将更新数据库，包括：
 - 创建新的用户记录
 - 检查重复的用户记录
 - 如果找到重复的记录，则使用新信息更新现有的用户记录
- **用户注册子流程。**该流程是用户注册流程的子流程。它执行所有的信息收集和验证工作。验证的信息包括：
 - 数据库中不存在重复的用户 ID
 - “口令”与“验证口令”录入值相同
 - 填写所有必需字段

注册工作流程过程在各阶段的分支取决于以下情况：

- 应用程序是 Siebel Partner Portal。
- 应用程序是 Siebel Partner Portal 之外的其它应用程序。这是缺省情况，它包括 Siebel eSales、Siebel eService、Siebel eCustomer、Siebel Training、Siebel Events 和 Siebel eMarketing。

第 154 页的表 16 列出了工作流程过程中指定的视图，这些视图在自行注册期间提供交互表单。

表 16. 自行注册工作流程视图

视图名称	使用该视图的应用程序	说明
VBC 用户注册 - 初始表单视图 VBC 用户注册 - 口令错误消息视图 VBC 用户注册 - 缺少信息消息视图 VBC 用户注册 - 法律确认视图 VBC 用户注册 - 登录错误消息视图 VBC 用户注册 - 确认消息视图 VBC 用户注册 - 拒绝视图 VBC 用户注册 - 创建用户错误消息视图 VBC 用户注册 - 安全设置错误消息视图	全部	<p>这些视图是使用用户注册流程的所有应用程序的公共视图，它们由以下两个组组成：</p> <ul style="list-style-type: none"> ■ “个人信息”表单以及因现有用户记录存在错误条目或重复的用户 ID 而产生的消息。 ■ “使用条款”表单以及因同意或拒绝接受条款而产生的消息。
VBC 用户注册 - 联系人信息视图	缺省	该视图是缺省情况下使用的“联系人信息”表单。
VBC 用户注册公司信息 - 公司视图 (SCW) VBC 用户注册公司信息 - 个人视图 (SCW) VBC 用户注册 - 联系人信息视图 (SCW)	Siebel Partner Portal	这些视图用于收集联系人信息以及用户所在公司的相关信息。

要调用自行注册工作流程过程，这些过程必须处于“活动”状态。

修改自行注册视图和工作流程

您可以在自行注册工作流程过程中修改现有视图，或者按照业务规则的要求创建新视图。您可以修改用于自行注册的 Seed 工作流程过程。

您可以通过多种方式修改缺省的自行注册功能。您可以执行以下一项或多项任务：

- 替换许可协议的文本
- 修订工作流程过程，包括创建定制的业务服务
- 重新定义要求用户填写的字段
- 在视图中添加或删除字段

- 更改视图或子视图的实际外观，例如，移动字段或更改颜色
- 创建新视图
- 修改“清除用户重复项”

修改自行注册视图、子视图和工作流程过程包括一些标准流程，这些流程是修改其它视图、子视图和工作流程过程的公共流程。

自行注册工作流程过程中使用的视图基于“VBC 用户注册”虚拟业务组件，该组件用于收集用户数据。只有在完成收集用户数据的所有阶段后，数据才会被写入到“用户注册”业务组件和 Siebel 数据库中。在进行修改之前，您应该了解这些组件是如何处理用户数据的。

“用户注册”和“用户”业务组件都基于相同的数据库表：S_PARTY、S_CONTACT 和 S_USER。因此，通过“用户注册”业务组件写入记录与通过“用户”业务组件写入记录等效。在任何一种情况下都会创建新用户。

用户注册流程提供以下优点：

- 如果自行注册流程在完成之前被终止，则不需要在数据库中执行撤消部分写入的新记录这一耗时流程。该流程需要搜索多个表。
- 可以在写入记录之前防止用户记录重复。

替换许可协议的文本

您可以替换在“用户注册 - 法律确认”视图中为自行注册的用户显示的缺省许可协议。

DotCom Applet License Base 1 Column Web 模板包括名称为 DotCom Applet Form Base 1 Column 的 Web 模板文件，它是名称为 dCCAppletLicenseBase1Col.swt 的文件。许可协议包含在 dCCAppletLicenseBase1Col.swt 文件中，前面包含这样一行文本 <!--This is where we include the html license agreement-->。您可以替换许可协议的文本。

有关处理 Web 模板的信息，请参阅 *Configuring Siebel eBusiness Applications*。

修订工作流程过程

您的业务方案适用的自行注册工作流程过程可能要求您修改 Seed 自行注册工作流程过程，例如：

- 替换或插入视图
- 插入或删除步骤
- 修改步骤

您不能直接修改 Seed 工作流程过程，例如，任何自行注册流程。您必须改为创建流程副本，然后修订该副本。

按照惯例，为了避免重命名流程，您可以使用“修订”按钮，制作名称相同的流程副本，但是版本号递增。请为具有相同名称的所有其它流程分配“已过时”状态，以便新版本成为唯一的活动版本。建议在修改任何工作流程过程（而不仅仅是 Seed 流程）时遵循该惯例。

注释：有关如何查看、修订、激活和部署工作流程过程的信息，请参阅 *Siebel Business Process Designer Administration Guide*。

创建定制的业务服务

Siebel 应用程序提供了预定义的业务服务，您可以在工作流程过程的某个步骤中使用这些服务。您还可以编写自己的定制业务服务脚本，然后在工作流程过程的步骤中运行这些脚本。

有关预定义的业务服务和创建业务服务的信息，请参阅 *Configuring Siebel eBusiness Applications*。

有关在工作流程过程中运行业务服务的信息，请参阅 *Siebel Business Process Designer Administration Guide*。

重新定义必需字段

作为一项缺省功能，自行注册的用户必须为某些字段录入值。这些字段可能随应用程序而有所不同。必需字段在用户界面中通过星号标注，字段显示在用户界面的表单中。

对于自行注册工作流程过程中使用的视图，您可以更改字段，确定它是否为必需字段。

请使用 Siebel Tools 确定包含自行注册字段的视图。

注释：有关如何查看、修订、激活和部署工作流程过程的信息，请参阅 *Siebel Business Process Designer Administration Guide*。

CSSWEFrameUserRegistration 框架类适用于视图中使用的子视图，这些视图出现在 Seed 自行注册工作流程过程中。该类允许您指定必需的自行注册字段。

要指定自行注册表单中的必需字段，请使用 Siebel Tools 修改包含表单的子视图。

以下过程展示了 Siebel Tools 任务中的主要步骤。有关在 Siebel Tools 中处理子视图和视图的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要指定自行注册表单中的必需字段

- 1** 打开 Siebel Tools。
- 2** 锁定“用户注册”项目。
- 3** 在“对象浏览器”中，展开“视图”对象类型。
此时将出现“视图”列表。
- 4** 选择包含自行注册字段的视图。
- 5** 在“对象浏览器”中，展开“视图 Web 模板”子对象类型，然后展开其子对象类型“视图 Web 模板项”。
自行注册视图通常包含一个单一表单子视图。它列在“视图 Web 模板项”列表中。
- 6** 在“视图 Web 模板项”列表中，向下搜索到子视图字段中所列单一子视图的链接。如果列出多个子视图，请向下搜索到您认为最有可能包含要查找的字段子视图。
此时将出现包含一项记录（您向下搜索到的子视图）的“子视图”列表。
- 7** 在“对象浏览器”中，展开“子视图”对象类型，然后展开“控件”子对象类型。
“控件”列表显示在“子视图”列表下面。
- 8** 在“控件”列表中选择记录，该记录的“标题”字段是用户界面中为您要求用户填写的字段显示的名称。请记录“名称”列中出现的值（例如，MiddleName）。

- 9 在“对象浏览器”中，单击“子视图用户属性”对象类型。
- “子视图用户属性”列表显示了“子视图”列表中子视图的用户属性。
- 10 在“子视图用户属性”列表处于活动状态时，选择“编辑”>“新记录”。
- 此时将出现新用户属性记录。
- 11 填写以下字段。请使用下面提供的准则。

字段	准则
名称	必需。输入显示必需项以及比现有的最大序号大 1 的序号。例如，如果“显示必需项 6”是最大的序号，则输入显示必需项 7。该项区分大小写。
值	必需。您在第 156 页的步骤 8 中记录的字段名称，例如 MiddleName。

- 12 重新编译 Siebel 库文件，并取消锁定“用户注册”项目。
- 在自行注册界面中显示时，新的必需字段带了一个星号。

注释：要使用户界面中的必需字段不再成为必需字段，请执行前面过程中的步骤，不同之处在于：在“子视图用户属性”列表中，为您在第 157 页的步骤 10 中添加的记录核选“不活动”列，或者删除该记录。

在现有的视图中添加或删除字段

您可以将在 Seed 自行注册工作流程过程使用的视图中收集的所有数据写入到“用户注册”业务组件中的字段。以下流程介绍了如何在用户界面中收集数据以及如何将其写入到数据库中的用户记录：

- 用户在表单的文本框中输入数据，例如，用户的姓氏。
- 该文本框映射至“VBC 用户注册”虚拟业务组件中的字段，例如 LastName。因此，此数据也被写入到该字段中。
- “VBC 用户注册”虚拟业务组件中的数据被写入到“用户注册”业务组件中。“用户注册”业务组件将数据写入到与“用户”业务组件相同的数据库表中。因此，每个字段实际上都是作为用户记录的一部分存储。

注释：在完成自行注册流程之前，“VBC 用户注册”虚拟业务组件中的数据不会被写入到“用户注册”业务组件字段中。

要在自行注册工作流程过程中使用的视图中添加或删除字段，您必须按以下顺序执行任务：

- Siebel Tools 任务
- Siebel Workflow 任务（使用 Siebel Tools 中的业务流程设计器）

用于执行添加或删除字段操作的 Siebel Tools 任务

要在自行注册工作流程过程中使用的某个视图中添加字段，您必须使用 Siebel Tools 以执行以下过程中的一个或多个步骤。

该过程用于确定所需的主要任务。有关修改视图和子视图的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要在自行注册工作流程过程中使用的视图中添加字段

- 1 打开 Siebel Tools。
- 2 锁定“用户注册”项目。
- 3 确定作为新字段基础的业务组件和基本数据库表。
- 4 如果新字段不是基于现有的数据库表列，请在相应表的扩展表中定义一个列。
- 5 在适当的业务组件中根据新表列或现有表列创建新字段。
- 6 如果新字段基于“用户注册”业务组件，请在“VBC 用户注册”虚拟业务组件中创建新字段。使用完全相同的字段名称。
- 7 配置适当的子视图以显示新字段。
- 8 如有必要，请配置新字段，以便要求自行注册的用户填写该字段。
- 9 重新编译 Siebel 库文件，并取消锁定“用户注册”项目。

注释：要从自行注册用户界面中删除字段，您不必从该字段所在的子视图中将其删除，而是改为配置子视图，以便不显示该字段。

更改视图或子视图的实际外观

有关更改视图或子视图实际外观（例如，移动字段或更改颜色）的信息，请参阅 *Configuring Siebel eBusiness Applications*。

为自行注册创建新视图

您可以创建一个新视图，以将其插入到其中一个自行注册工作流程过程中，执行此操作时采用的方式与为任何其它用途创建视图的方式相同。

您可以将新的子视图包括在所创建的视图中，该视图包括在自行注册工作流程过程中。您可以创建新子视图，并将其包括在此视图中，执行这些操作时采用的方式与为任何其它用途执行这些操作的方式相同，不过您同时需要考虑以下事项：

- 如果子视图以“用户注册”业务组件为基础，请对该子视图应用 `CSSWEFrameUserRegistration` 类，从而允许您定义在用户界面上标有星号的字段。按照惯例，您要求用户在自行注册流程期间填写的字段均标有星号。

有关处理视图的信息，请参阅 *Configuring Siebel eBusiness Applications*。

管理重复的用户

在用户自行注册时，“用户注册流程”工作流程过程尝试确定数据库中是否已经存在该用户。“清除用户重复项”是一项缺省功能，它是一项可配置功能。

作为一项缺省功能，如果自行注册用户输入的以下所有非 NULL 的字段值与现有用户的字段值相匹配，这些用户则被视为是同一位用户。

- 名字
- 姓氏
- 电子邮件地址

如果自行注册用户与现有用户相匹配，则会更新现有的用户记录，而不是写入新的用户记录。如果现有用户记录的字段中的值与自行注册用户的非 NULL 录入值不相同，则会使用新的数据更新现有的字段。其它所有现有字段值保留不变。

在“用户注册子流程”工作流程过程中，使用“用户注册”业务服务中的 ValidateContact 方法进行重复项比较。此比较在“检查用户密钥”步骤完成。

修改重复用户的已更新字段

您可以指定在确定重复用户时不更新“用户注册”业务组件中的某些字段。

以下过程用于列出您必须执行的主要步骤。有关执行这些步骤的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要在确定重复用户时不更新某个字段

- 1 打开 Siebel Tools。
- 2 锁定“用户注册”项目。
- 3 确定“VBC 用户注册”虚拟业务组件中不要更新的字段。
 - a 在“对象浏览器”中，单击“业务组件”。
 - b 在“业务组件”列表中，查询或滚动以选择“VBC 用户注册”业务组件。
 - c 在“对象浏览器”中，展开“业务组件”项，然后选择“字段”子项。
 - d 在“字段”列表中，查询或滚动以选择要不更新的字段。
- 4 添加适当的业务服务用户属性。
 - a 在“对象浏览器”中，单击“业务服务”。
 - b 在“业务服务”列表中，查询或滚动以选择“用户注册”业务服务。
 - c 在“对象浏览器”中，展开“业务服务”项，然后选择“业务服务用户属性”子项。
 - d 在“业务服务用户属性”列表中创建新记录。
 - e 只填写列出的字段。使用下面提供的准则。

字段	准则
名称	输入 Exclude From Update <i>number</i> ，其中 <i>number</i> 是特定用户属性的下一个序号。 例如，输入 Exclude From Update 3。该录入值区分大小写。
值	输入您在第 159 页的步骤 3 中注明的“VBC 用户注册”虚拟业务组件的字段名称。

- 5 重新编译 Siebel 库文件，并取消锁定“用户注册”项目。

修改用于确定重复用户的字段

您可以更改用于确定是否存在重复用户的字段。

以下过程列出您在修改用于确定重复用户的字段时必须执行的主要步骤。有关执行这些步骤的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要修改用于确定重复用户的字段

- 1 打开 Siebel Tools。
- 2 锁定“用户注册”项目。
- 3 在“用户注册”业务组件中确定要从重复项比较中添加或删除的字段。
 - a 在“对象浏览器”中，展开“业务组件”，然后展开“字段”子项。
 - b 在“业务组件”列表中，查询或滚动以选择“用户注册”业务组件。
- 4 在“对象浏览器”中，展开“业务服务”，然后单击“业务服务用户属性”子项。
此时将出现“业务服务”列表和“业务服务用户属性”子列表。
- 5 在“业务服务”列表中，选择“用户注册”。
- 6 从重复项比较中删除字段：
 - a 在“业务服务用户属性”列表中，选择名称为 App User Key: Default *number* 或 App User Key: Siebel eChannel *number*（适用于 Siebel Partner Portal）的记录，记录的值是您需要从比较中删除的“用户注册”业务组件字段。
 - b 单击以核选“不活动”字段，然后提交记录。
- 7 在重复项比较中添加字段：
 - a 在“业务服务用户属性”中创建新记录。
 - b 只输入以下列出的字段。请使用下面提供的准则。

字段	准则
名称	输入 App User Key: Default <i>number</i> 或 App User Key: <i>application number</i> ，其中 <i>application</i> 是 Siebel 应用程序的名称， <i>number</i> 是该特定用户属性的下一个序号。该录入值区分大小写。 例如，您可能输入 App User Key: Default 2，为 Siebel eService 添加一个字段，或者输入 App User Key: Siebel eChannel 4，为 Siebel Partner Portal 添加一个字段。
值	为要添加到重复项检查的“用户注册”业务组件的字段输入名称。

- 8 重新编译 Siebel 库文件，并取消锁定“用户注册”项目。

禁用重复用户检查

您可以禁用重复用户检查。

以下过程用于显示禁用重复项检查的主要步骤。有关处理工作流程过程的详细信息，请参阅 *Siebel Business Process Designer Administration Guide*。

要禁用自行注册清除重复项检查

- 1 在 Siebel Tools 中，选择“对象编辑器”中的“工作流程过程”。
- 2 查询或滚动以选择“用户注册”子流程。
- 3 按照第 154 页的“修改自行注册视图和工作流程”中的说明，创建修订后的“用户注册”子流程副本。
- 4 右键单击并选择“编辑工作流程过程”，以便编辑修订后的副本。
此时将出现“过程设计器”，其中显示当前的工作流程过程。
- 5 对于应用于应用程序的每个流程步骤，记录连接到该步骤的所有连接器的来源以及从该步骤连接的单一连接器的目标。重新路由连接器以绕过该步骤。对于所有的 Siebel 应用程序，请选择“检查用户密钥”步骤。
- 6 删除绕过的流程步骤，它现在应该不是任何连接器的来源或目标。
- 7 右键单击并选择“所有流程”。
此时将再次出现“工作流程过程”列表。修订后的流程仍被选定。
- 8 单击“部署”。

管理“忘记口令”

如果以前在 Siebel 客户或合作者应用程序中自行注册的用户忘记了自己的口令，他（她）可以通过单击登录对话框中的“忘记口令？”链接来获取新的口令。

注释：“忘记口令？”是 Siebel 客户和合作者应用程序的缺省功能，但是只有在您实施 LDAP 或 ADSI 安全适配器验证或数据库验证时，该功能才可用。如果您要在 Web SSO 验证环境中实施类似的功能，则要负责在外部验证应用程序、用户目录和安全适配器中配置该功能。有关执行这些任务的详细信息，请参阅第三方供应商的文档。

忘记口令的用户体验

以前自行注册的用户如果忘记现有的口令，可以重新找回新的口令。在以后登录时，该用户可以在“用户资料”视图中更改此新口令。

要重新找回新口令

- 1 在登录对话框中，用户可以单击 *忘记口令?*。
此时将出现“用户信息”表单。
- 2 用户填写表单中的所有字段，然后单击“提交”。
 - 数据库中的记录与“姓氏”和“名字”字段中录入值之间的比较区分大小写。
 - 将“工作电话号码”中的录入号码与数据库中的记录进行比较。比较时忽略任何分隔符。
 如果找到匹配的记录，则会出现“口令提示问题”表单。
- 3 用户输入口令提示问题的答案。
如果正确地回答了口令提示问题，则会出现“新口令确认”对话框，并且对话框中提供了用户的新口令。
- 4 单击“继续”。

忘记口令的体系结构

“忘记口令？”在“用户注册 - 忘记口令流程”工作流程过程中实施。该流程是“用户注册 - 初始流程”中的一个子流程。

按照第 161 页的“[忘记口令的用户体验](#)”中的介绍，要接收系统生成的新口令，该用户必须提供用以与数据库用户记录进行比较的标识数据。如果四个字段全部返回与现有记录大小写匹配的结果，用户则必须回答与该记录相关联的口令提示问题。口令提示问题的答案也必须返回大小写匹配的结果。

用户在用户界面的比较字段中输入值时，该值被写入到“用户注册”业务组件的字段中。该业务组件与“用户”业务组件基于相同的表。虚拟字段值不会被写入到数据库中，但会与那些基本表中的字段值进行比较。用户在用户界面的以下字段中输入的值将与所提供表中的字段值进行比较：

- “姓氏”、“名字”、“电子邮件”和“工作电话号码”字段值与 S_CONTACT 字段值进行比较。
- “口令提示问题答案”字段值与 S_USER 字段值进行比较。

“用户注册 - 忘记口令流程”工作流程过程使用以下视图：

- 用户注册 - 忘记口令信息视图
- 用户注册 - 忘记口令提示问题视图
- 用户注册 - 忘记口令确认视图
- 用户注册 - 忘记口令提示问题答案错误视图
- 用户注册 - 忘记口令拒绝视图

修改“忘记口令”工作流程过程

您可以通过以下方式修改“用户注册 - 忘记口令流程”工作流程过程：

- 比较 NULL 字段以及用户提供了值的字段。
- 要求用户提供其它标识数据。

在“用户注册 - 忘记口令流程”工作流程过程中，“查询用户”步骤调用“用户注册”业务服务的 FindContact 方法。该方法在数据库中查询其数据与用户提供的标识数据相匹配的用户记录。如果查询返回唯一的记录，用户可以通过回答提示问题，证明他（她）是记录的所有者。

第 163 页的表 17 介绍了 FindContact 方法的参数。

表 17. FindContact 方法的参数

列表	记录	关于值的注释
输入参数	EmailAddress FirstName LastName WorkPhoneNum	“输入参数”字段值是“用户注册”业务组件中 FindContact 业务服务用来查询是否有匹配项的字段名称。它与“属性名称”字段中提供的流程属性值进行比较。这些流程属性收集了用户录入的信息。
	输出字段：ID 输出字段：登录名	“输入参数”字段值指定了 FindContact 方法，要求该方法为其字段值与用户的录入值匹配的每项用户记录返回 ID 和“登录名”字段值。定义了值的临时表，在该表中，行是返回的记录，而列由“值”字段的值提供。“ID”列中所返回记录的 ID 包含在临时表的一个行中，而该记录的登录名包含在“登录名”列中。
输出参数	登录名 Siebel 操作对象 ID RegError	<ul style="list-style-type: none"> ■ 每个“属性名称”字段值是一个流程属性名称。如果 FindContact 返回唯一的匹配记录，则“登录名”和“Siebel 操作对象 ID”流程属性将接收值。如果未确定与该标准匹配的唯一记录，RegError 则接收错误值。 ■ “Siebel 操作对象 ID”用来为工作流程过程中的后续操作确定用户记录，并且它从临时表的 ID 列中接收值，即用户记录的 ID。“登录名”流程属性从临时表的“登录名”列中接收值，即用户记录的登录名。

修改工作流程过程以查询 NULL 字段

缺省情况下，如果用户在“用户信息”表单中填写的字段少于四个，则查询时只使用用户填写的字段来查找数据库中的唯一匹配记录。例如，如果用户只输入名字和姓氏，则查询不会对“电子邮件”或“工作电话号码”字段做任何比较。

您可以指定“查询用户”步骤（“用户注册”业务服务中的 FindContact 方法）还必须检查用户留空的字段在数据库记录中是否确认为 NULL，从而断定某项记录是否为匹配项。为此，您必须在“查询用户”流程步骤中添加值为 Y 的 QueryAllFields 输入参数。缺省情况下，该输入参数的值为 N。

您可以通过以下操作执行此更改：为修订后的“用户注册 - 忘记口令流程”工作流程过程副本修改“查询用户”步骤，然后激活该副本。在您创建输入参数时，请输入以下字段和值：

表 18. QueryAllFields 输入参数的值

字段	值
输入参数	QueryAllFields
类型	说明
值	Y

有关修改工作流程过程的详细信息，请参阅 *Siebel Business Process Designer Administration Guide*。

修改工作流程过程以请求其它标识数据

该流程将“用户信息”表单中要求用户提供的数据与现有用户记录中的数据进行比较，以找到唯一的数据库记录。除了在 Seed “用户注册 - 忘记口令流程”工作流程过程中比较的那些数据之外，如果您要比较其它数据，必须执行以下任务：

- 修改用户界面
- 修改“用户注册 - 忘记口令流程”输入参数

修改用户注册的用户界面

要在“用户信息”表单中添加或删除字段，您必须使用 Siebel Tools 修改基本的子视图。以下过程用于列出您在“用户信息”表单中添加或删除字段时必须执行的主要步骤。有关执行这些步骤的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要在“用户信息”表单中添加或删除字段

- 1 打开 Siebel Tools。
- 2 锁定“用户注册”项目。
- 3 如果您要添加字段，请确定要添加什么字段。然后在“VBC 用户注册”虚拟业务组件和“用户”注册业务组件中添加字段，该字段与您要添加的字段相对应。这些字段使用相同的名称。

有关详细信息，请参阅第 154 页的“修改自行注册视图和工作流程”。

- a 在“对象浏览器”中，单击“业务组件”。
- b 在“业务组件”列表中，查询或滚动以选择“用户注册”业务组件。
- c 在“对象浏览器”中，展开“业务组件”，然后单击“字段”子项。
- d 在“字段”列表中，为该业务组件添加所需的字段。
- e 为“VBC 用户注册”虚拟业务组件重复该流程。

- 4 配置子视图“VBC 用户注册 - 初始表单子视图”，以显示或隐藏字段。
- a 在“对象浏览器”中，单击“子视图”。
 - b 在“子视图”列表中，查询或滚动以选择子视图“VBC 用户注册 - 初始表单子视图”。
 - c 在对象编辑器中，展开“子视图”，然后单击“控件”子项。
 - d 在“控件”列表中：
 - 如果您要隐藏字段，请在“控件”列表中选择记录，并核选其“不活动”字段。
 - 如果要添加字段，请在“控件”列表中添加新记录。只填写列出的字段。请使用下面提供的准则。

字段	准则
名称	输入该字段的名称，例如城市
标题	输入希望该字段在用户界面中使用的标题，例如城市
字段	输入在 第 164 页的步骤 3 中确定的字段，例如城市
HTML 显示模式	删除缺省值，从而让字段为空白
HTML 行 - 敏感	核选
HTML 类型	选取文本
排序	核选
文本对齐	选取对齐方式
可视	核选
可视 - 语言覆盖	输入 Y

- 5 为“VBC 用户注册 - 初始表单子视图”配置适当的子视图 Web 模板，以显示或隐藏该字段。
- 6 重新编译 Siebel 库文件，并取消锁定“用户注册”项目。

要从自行注册用户界面中删除字段，您不必从该字段所在的子视图中将其删除，而是改为配置子视图，以便不显示该字段。

有关配置 Web 模板和子视图的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

修改工作流程过程的输入参数

您可以在“用户注册 - 忘记口令流程”的“查询用户”步骤中，为“用户注册”业务服务中的 FindContact 方法指定输入字段，这些字段用于查找匹配的用户记录。您必须修改该步骤，以添加或删除输入字段。

您可以通过以下操作执行此更改：为修订后的“用户注册 - 忘记口令流程”工作流程过程副本修改输入参数，然后激活该副本。在您创建输入参数时，请输入以下字段和值：

表 19. “查询用户”步骤中的输入参数值

字段	准则
输入参数	为您在第 164 页的“修改用户注册的用户界面”的第 164 页的步骤 3 中注明的“用户注册”业务组件的字段输入名称，例如城市。这是现有用户记录中的字段，该字段与数据库中的记录进行比较。
类型	选择流程属性。
属性名称	选择与在第 164 页的“修改用户注册的用户界面”的第 164 页的步骤 3 中注明的“用户注册”业务组件字段对应的流程属性，例如城市。按照惯例，流程属性的名称与字段的名称相同。
属性数据类型	该字段自动填入流程属性的数据类型。

用户的内部管理

您可以执行以下任务，为雇员、客户或合作者用户提供一个或多个 Siebel 应用程序的访问权限：

- 为用户提供进行验证以便连接至数据库帐户的方法。
- 内部管理员使用 Siebel 雇员应用程序（例如 Siebel Call Center），将用户添加到 Siebel 数据库中。

用户验证要求

您应该在添加新用户之前先实施验证体系结构。作为一项正在进行的任务，您必须计划在登录时可以对每位新用户进行验证。您必须为每位新用户执行的设置和管理工作取决于您实施的验证体系结构。

有关以下说明中提到的用户验证概念的信息，请参阅第 6 章“安全适配器验证”。

- **数据库安全适配器验证。**您必须在用户的“用户 ID”字段中输入有效的数据库帐户的用户名。您必须为新用户提供数据库帐户的用户 ID 和口令。
- **LDAP/ADSI 安全适配器验证。**您可以配置应用程序，以便在您创建或修改 Siebel 数据库中的用户记录时，安全适配器将所做更改传播到用户目录中，从而不需要对用户目录单独进行管理。

注释：要使 Siebel 安全适配器将 Siebel 数据库中的新用户数据或修改后的用户数据传播到用户目录中，修改数据库记录的管理员必须通过相同的安全适配器登录。

如果您在用户验证环境中使用适配器定义的用户名，则无法实施一些工具，这些工具使您可以在 Siebel 应用程序中管理存储在目录中的用户的 Siebel 用户 ID。这包括将对 Siebel 用户 ID 传播到目录中的用户进行内部管理。

有关用户验证的信息，请参阅第 6 章“安全适配器验证”。

警告：请确保应用程序用户对用户目录具有写权限。应用程序用户是指唯一可以在目录中创建或修改用户的用户。

- **Web SSO 验证。**您必须维护每位用户在外部分验证系统、用户目录和 Siebel 数据库中的对应记录。如果要实施一种机制以使这些记录同步，必须单独开发实用程序，并在 Web 站点级别实施。Siebel 应用程序文档中未提供配置准则。您必须为新用户提供验证证书。

将用户添加到 Siebel 数据库中

Siebel 应用程序的用户是“用户”业务组件中的记录。Siebel 数据库中的 S_PARTY、S_CONTACT 和 S_USER 表是“用户”业务组件的基础。您可以为每位用户分配职责、用户 ID 和口令（取决于使用的验证体系结构）。

雇员或合作者用户是指在 Siebel 数据库的内部或外部部门中具有职位的用户。其他用户（例如，使用 Siebel eSales 等客户应用程序的用户）没有职位或不属于某个部门。除了作为“用户”业务组件基础的表之外，S_EMP_PER 表是雇员和合作者用户所属的“雇员”业务组件的基础。

有关职责、职位、部门和组织功能的详细信息，请参阅第 10 章“配置访问控制”。

尽管每位用户在“用户”业务组件中均有记录，但是，管理员使用不同的视图添加雇员、合作者用户和其它用户。

警告：您可以修改现有雇员、合作者用户或联系人用户的字段值，例如在名称发生更改时。但是，更改此类用户的用户 ID 会产生特殊的问题，因为该 ID 可能通过 CREATOR_LOGIN 等字段存储在其它各种类型的记录中（在这些记录中不使用用户记录的外部关键字）。在更新用户 ID 时，这些字段的值不会自动被更新。如果您更改用户 ID，则还必须更新其它记录中的此类值。

添加新雇员

雇员至少必须具有职位、职责和 Siebel 用户 ID。

您还可以将属性与雇员记录（例如，技能、工具、分配规则和可用性）进行关联，从而让您可以在 Siebel Assignment Manager 和 Siebel Professional Services 自动化等功能中使用雇员记录及其属性。

以下过程只是为雇员创建用户记录，它是允许雇员访问数据库的一个阶段。

要添加新雇员

- 1 以管理员身份登录到雇员应用程序（例如 Siebel Call Center），然后选择“导航”>“场地图”>“管理 - 用户”>“雇员”。
此时将出现“雇员”列表。
- 2 添加新记录。
- 3 填写以下字段，然后保存记录。请使用下面提供的准则。

字段	准则
姓氏	必需。输入任何名称。
名字	必需。输入任何名称。
用户 ID	必需。输入简单且连续的用户 ID，每个用户的用户 ID 必须唯一。通常，由用户提供该用户 ID 以便登录。 根据您配置验证的方式，用户使用该标识符可能可以，也可能无法登录。如果您实施数据库验证，则该字段必须是数据库帐户的登录名。

字段	准则
口令	<p>可选（对于某些验证实施是必需项）。</p> <p>输入简单且连续的登录口令。口令必须符合验证系统的语法要求，但是在该表单中不会检查口令是否符合要求。</p> <p>如果是 LDAP/ADSI 安全适配器验证，口令将传播至用户目录。如果是数据库验证，口令将传播至数据库。</p> <p>有关用户验证体系结构的信息，请参阅第 6 章“安全适配器验证”。</p>
职责	<p>必需。选取一个或多个职责，这些职责包括雇员的相应视图。如果创建该用户的管理员在其“新职责”字段中具有值，则在缺省情况下该职责被分配给此用户有关“新职责”字段的信息，请参阅第 171 页的“用户记录的“新职责”字段”。</p>
新职责	<p>可选。如果创建该用户的管理员在其“新职责”字段中具有值，则在缺省情况下该职责被分配给此字段。有关“新职责”字段的信息，请参阅第 171 页的“用户记录的“新职责”字段”。</p>
职位	<p>必需。要成为雇员，用户必须具有职位。如果您分配了多个职位，指定为“主要”的那个职位就是用户登录时采用的职位。</p>
部门	<p>必需。该字段自动填入主要职位所属的部门。</p>
地区	<p>该字段是只读的多值组。您不能手动输入值。在您填写“职位”字段时，“地区”字段将自动填入与该职位关联的地区。（该字段出现在“详细信息”表单中。）</p>
组织	<p>虽然该字段值从创建此用户的其它用户中继承，但是您可以编辑该字段。其职位在该组织中的用户有权访问此雇员记录。（该字段出现在“详细信息”表单中。）</p> <p>有关组织访问控制的信息，请参阅第 10 章“配置访问控制”。</p>

完成雇员设置

您可以在为雇员分配职责之前或之后设置雇员。有关完成雇员设置的详细信息，请参阅*应用程序管理指南*的初始设置部分。

另请参阅 *Siebel Assignment Manager Administration Guide* 和 *Siebel Professional Services Automation User Guide*。

禁用雇员

您可以按以下方式禁用雇员：断开雇员记录与其职责的关联、更改用户 ID，然后删除雇员对数据库的访问权限。

要禁用雇员

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 用户”>“雇员”。
- 此时将出现“雇员”视图。
- 2 在“雇员”列表中，选择要禁用的雇员。

3 在“详细信息”视图选项卡中，从“职责”字段中删除所有记录。

4 对用户 ID 稍作改动，以指明该雇员不再是当前雇员。

在禁用雇员时，您可能需要制定重命名用户 ID 的惯例。一种可行的惯例就是在用户 ID 后面附加一些文本，例如“expired”。例如，您可能将 CARD 更改为 CARD-expired。通过这种方式，您可以继续在历史记录中查看与以前活动关联的人员姓名。

5 删除雇员对数据库的访问权限。

如果您实施了数据库用户验证，则应该删除用户的数据库帐户。如果您实施了外部验证，则应该从检索用户数据库证书的目录中删除用户。

注释：如果使用了外部验证，并且外部用户目录由多个应用程序共享（例如 LDAP 或 ADSI），请不要从目录中删除该用户。请确保该用户的数据库访问用户名和口令不同于他（她）的目录用户名和口令。否则，该用户可能会直接使用一些数据库连接工具访问数据库。

添加新的合作者用户

合作者用户通常是指合作者公司的雇员或贵公司的顾问。

合作者用户在合作者组织中必须具有与该组织关联的职位，或者该职位属于基于职位的团队，例如，商机或客户团队。

您可以将以下来源的职位分配给新的合作者用户：

- 您在内部创建并与授权管理员的合作者组织相关联的职位
- 合作者组织中的授权管理员创建的职位

您可以在 Siebel 合作者管理器或其它 Siebel 雇员应用程序的“管理 - 合作者”屏幕（您拥有许可证的此屏幕）注册和管理合作者用户。

有关使用“管理 - 合作者”屏幕的信息，请参阅 *Siebel Partner Relationship Management Administration Guide*。

添加新的联系人用户

非雇员或合作者用户的用户没有职位。例如，这些用户包括使用 Siebel eSales 的客户或使用 Siebel Training 的学生。这些用户被称为客户或联系人用户，以便与雇员和合作者用户区分开来。

联系人（例如，客户帐户的联系人）可以存在于数据库中，但不能登录。您可以在“管理 - 用户”屏幕中创建此类联系人作为“人员”。本节中的过程适用于您提供了 Siebel 数据库登录权限的联系人用户。

警告：您可以修改现有联系人用户的字段值，例如在名称发生更改时。但是，更改此类用户的用户 ID 会产生特殊的问题，因为该 ID 可能通过 CREATOR_LOGIN 等字段存储在其它各种类型的记录中（在这些记录中不使用用户记录的外部关键字）。在更新用户 ID 时，这些字段的值不会自动被更新。如果您更改用户 ID，则还必须手动更新其它记录中的此类值。

要添加新联系人用户

- 1 以管理员身份登录到 Siebel 雇员应用程序，然后选择“导航”>“场地图”>“管理 - 用户”>“用户”。
此时将出现“用户”列表。
- 2 添加新记录。
- 3 填写以下字段，然后保存记录。请使用下面提供的准则。

字段	准则
姓氏	必需。输入任何名称。
名字	必需。输入任何名称。
用户 ID	必需。输入简单且连续的用户 ID，每个用户的用户 ID 必须唯一。通常，由用户提供该用户 ID 以便登录。 根据您配置验证的方式，用户使用该标识符可能可以，也可能无法登录。
口令	可选（对于某些验证实施是必需项）。 输入简单且连续的登录口令。口令必须符合验证系统的语法要求，但是在该表单中不会检查口令是否符合要求。 如果是 LDAP/ADSI 安全适配器验证，口令将传播至用户目录。如果是数据库验证，口令将传播至数据库。 有关用户验证体系结构的信息，请参阅第 6 章“安全适配器验证”。
帐户	选择与用户关联的一个或多个帐户。指定一个帐户作为主要帐户。有关帐户在授权管理中的功能的信息，请参阅第 172 页的“用户的授权管理”。
职责	为该用户选取一个或多个职责，职责包括了客户应用程序（例如，Siebel eService）中的相应视图。如果创建该用户的管理员在其“新职责”字段中具有值，则在缺省情况下该职责被分配给此用户。
新职责	如果创建该用户的管理员在其“新职责”字段中具有值，则在缺省情况下该职责被分配给此字段。有关“新职责”字段的信息，请参阅第 171 页的“用户记录的新职责”字段”。
时区	选择时区，这样可以按照该时区显示事件的时间。
用户类型	该字段用作筛选器，从而让不同的应用程序可以查询只适用于每个特定应用程序的联系人用户。
工作电话号码	应用程序只解释用户提供的数字。任何分隔符都被忽略。
住宅电话号码	
传真号码	

新用户出现在“用户”列表中。

将联系人提升为联系人用户

您可以通过将用户证书和职责分配给人员记录（联系人），将现有的联系人提升为联系人用户。

要将现有的联系人提升为联系人用户

- 1 以管理员身份登录到 Siebel 雇员应用程序。
- 2 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 用户”>“人员”。
此时将显示“人员”列表。
- 3 选择要提升的联系人记录。
- 4 为“用户 ID”、“口令”、“职责”和“新职责”字段输入值，这在第 169 页的“添加新的联系人用户”中有介绍。

用户记录的“新职责”字段

用户记录在“用户”视图的“新职责”字段中不一定具有值。如果存在值，只要该用户创建新用户，在缺省情况下，系统会为新用户的“职责”字段分配执行创建的该用户“新职责”字段中的值。此原则适用于那些要创建任何类型用户（只要他们的应用程序允许）的任何类型的用户（雇员、合作者用户、联系人用户）。

用户自己的“新职责”字段将通过以下某种方式填入值：

- “新职责”字段值从创建该新用户的用户的“新职责”字段中继承。
- 为用户手动分配“新职责”字段值。

只有内部管理员才可以修改用户的“新职责”字段。

Siebel 客户和合作者应用程序的授权管理员可以升级用户的职责，但是，他们不能编辑“新职责”字段。因此，内部管理员控制任何客户或合作者用户从授权的管理员处继承的缺省职责。如果您打算让新客户和合作者用户拥有“新职责”值（例如，为此类用户提供的 Seed 职责），确保授权的管理员拥有这样的“新职责”值这一点很重要。

在管理员创建新的雇员记录时，您不一定需要使用“新职责”字段的功能。如果为新雇员分配了各种职责，将雇员的“新职责”字段留空可能有意义。如果为大多数新雇员分配了相同的职责，或者您要创建一批职责相同的新雇员记录，那么，为添加雇员的管理人员分配“新职责”值会更加有效。

内部管理员可以在同一个管理屏幕中修改雇员、合作者用户和联系人用户的“新职责”值。

要修改用户的“新职责”字段值

- 1 以管理员身份登录到 Siebel 雇员应用程序，然后选择“导航”>“场地图”>“管理 - 用户”>“用户”。
此时将出现“用户”列表，其中包含数据库中的所有雇员、合作者用户和联系人用户。
- 2 在“用户”列表中，选择要修改的用户记录。
- 3 在表单中选取“新职责”字段中的新值，然后保存记录。
用户必须注销并再次登录，才能使“新职责”值生效。

用户的授权管理

授权的管理员是 Siebel 客户或合作者应用程序的用户，其职责提供的视图允许授权的管理员注册和管理该应用程序的其他用户。授权管理通常在 B2B 关系中实施。

用户的授权管理将一部分管理负担转移给客户或合作者公司的管理员，从而最大限度地降低了内部管理成本。

授权管理的用户验证要求

授权管理是大多数 Siebel 客户和合作者应用程序的缺省功能，但是，只有在您实施 LDAP 或 ADSI 安全适配器验证时，该功能才可用。

如果您使用数据库验证，则不能实施授权管理。如果您要在 Web SSO 验证环境中实施授权管理，则要负责在外部验证应用程序、用户目录和安全适配器中配置该功能。Siebel 应用程序文档中未提供此类配置准则。

授权管理要求您配置 LDAP 或 ADSI 安全适配器，将 Siebel 数据库中的新用户数据和修改后的用户数据传播到用户目录中。

如果您在用户验证环境中使用适配器定义的用户名，则无法实施一些工具，这些工具使您可以在 Siebel 应用程序中管理存储在目录中的 Siebel 用户 ID，包括用户的授权管理。有关用户验证的信息，请参阅第 6 章“安全适配器验证”。

警告： 确保 Siebel 客户或合作者应用程序的应用程序用户对用户目录具有写权限。

授权管理的访问注意事项

授权的管理员具有访问用户数据的有限权限。

■ **客户应用程序。** 授权的管理员只能看到与客户关联、而客户又与此授权的管理员相关联的用户。“我的客户用户管理视图”以“客户”（授权的管理员）业务组件为基础。该业务组件基本上限制了授权的管理员访问与客户关联、而客户又与此授权的管理员相关联的数据。

■ **合作者应用程序。** 授权的管理员只能看到其职位与授权管理员的职位共同属于同一个合作者组织的合作者用户。

授权的管理员可以添加以常规方式注册的用户或其它授权的管理员。但是，主机公司的管理员必须添加第一个授权的管理员，用于管理：

■ Siebel 客户应用程序的每位客户

■ Siebel 合作者应用程序的每个合作者组织

在内部创建授权的管理员要求您为用户提供一个职责，该职责包括授权管理所需的视图。您的 Siebel 应用程序为客户和合作者应用程序的授权管理员提供了 Seed 职责。

有关 Seed 职责的信息，请参阅附录 C“Seed 数据”。

注释： 各个 Siebel 应用程序之间的授权用户管理屏幕、导航和过程有所不同。剩下的章节介绍了在客户和合作者应用程序中具有代表性的授权管理。

注册联系人用户 — 授权管理

使用 Siebel 客户应用程序的授权管理员至少必须属于一个帐户。授权的管理员注册当前活动帐户中的用户。新用户将继承该帐户中的成员资格。

授权的管理员必须为新用户至少分配一个职责。授权的管理员只拥有可用于分配给用户的职责（包括 Seed 职责），主机公司将这些职责与组织（授权的管理员与该组织相关联）进行关联。授权的管理员与应用程序的代理雇员所属的组织相关联。公司的管理员使用雇员应用程序（例如，Siebel Call Center）将职责与组织进行关联。

要注册新的客户用户（由授权的管理员进行）

- 1 登录到实施授权管理的 Siebel 客户应用程序，例如，Siebel eSales 或 Siebel eService。

注释：授权管理员的用户类型必须是“Web 授权客户管理员”。

- 2 单击“我的帐户”，然后单击“我的公司”下面的“用户管理”。

此时将出现授权帐户和关联用户的列表，如下所示。列表可能随应用程序而有所不同。

Delegated Accounts							
No Records							
Name	Street Address	City	State	Zip Code	Country	Phone #	Email

Users							
No Records							
New	Query						
Last Name	First Name	Middle Initial	User ID	Email	Responsibility	User Type	Delete

- 3 在“授权帐户”列表中，选择您要与新用户关联的帐户。

该帐户中的用户出现在“用户”列表中。

- 4 创建新记录。

5 填写以下字段，然后保存记录。请使用下面提供的准则。

字段	准则
姓氏	必需。输入任何名称。
名字	必需。输入任何名称。
用户 ID	必需。输入简单且连续的用户 ID，每个用户的用户 ID 必须唯一。通常，由用户提供该用户 ID 以便登录。 根据您配置验证的方式，用户使用该标识符可能可以，也可能无法登录。
口令	可选（对于某些验证实施是必需项）。 输入简单且连续的登录口令。口令必须符合验证系统的语法要求，但是在该表单中不会检查口令是否符合要求。 如果是 LDAP/ADSI 安全适配器验证，口令将传播至用户目录。如果是数据库验证，口令将传播至数据库。 有关用户验证体系结构的信息，请参阅第 6 章 “安全适配器验证”。
职责	选择一个或多个职责，例如，为联系人用户提供的 Seed 职责。如果创建该用户的授权管理员在“新职责”字段中具有值，则在缺省情况下，该职责将分配给此用户。有关“新职责”字段的信息，请参阅第 171 页的“用户记录的“新职责”字段”。
住宅电话号码	应用程序只解释这些电话号码录入值中的数字。 任何分隔符都被忽略。
工作电话号码	
工作传真号码	

新记录出现在“用户”列表中。

注册合作者用户 — 授权管理

使用合作者应用程序（例如，Siebel Partner Portal）的授权管理员在合作者部门中具有职位。授权的管理人员只能为新合作者用户分配合作者部门所属的合作者组织中包括的职位。

合作者用户在合作者组织中必须具有与该组织关联的职位，或者该职位属于基于职位的团队，例如，商机或客户团队。

合作者公司中的授权管理员可以为新的合作者用户分配以下来源中的职位：

- 您在内部创建并与授权管理员的合作者组织相关联的职位
- 合作者组织中的授权管理员创建的职位

授权的管理人员只拥有可用于分配给合作者用户的职责，主机公司将这些职责与授权管理员的合作者组织进行关联。公司的管理人员使用雇员应用程序（例如，Siebel Partner Manager）将合作者组织与职责相关联。

要为新的合作者用户提供对数据库的访问权限，授权的管理人员在注册合作者用户时必须分配职责。

要注册新的合作者用户（由授权的管理员进行）

- 1 登录到实施授权管理的合作者应用程序，例如，Siebel Partner Portal。

注释：授权管理员的用户类型必须是“Web 授权客户管理员”。

- 2 选择“场地图”>“管理”。
- 3 在浏览器中，展开要在其中创建合作者用户的组织。
- 4 单击“用户”子项，显示该组织中的用户。
- 5 在“编辑用户”表单中，创建新记录以便添加新用户。填写以下字段，然后保存记录。请使用下面提供的准则。

字段	准则
姓氏	必需。输入任何名称。
名字	必需。输入任何名称。
用户 ID	必需。输入简单且连续的用户 ID，每个用户的用户 ID 必须唯一。通常，由用户提供该用户 ID 以便登录。 根据您的配置验证的方式，用户使用该标识符可能可以，也可能无法登录。
口令	可选（对于某些验证实施是必需项）。 输入简单且连续的登录口令。口令必须符合验证系统的语法要求，但是在该表单中不会检查口令是否符合要求。 如果是 LDAP/ADSI 安全适配器验证，口令将传播至用户目录。如果是数据库验证，口令将传播至数据库。 有关用户验证体系结构的信息，请参阅第 6 章“安全适配器验证”。
职位	如果您分配了多个职位，指定为“主要”的那个职位就是他（她）登录时采用的职位。
职责	选择一个或多个职责，例如，为合作者用户提供的 Seed 职责。如果创建该用户的管理员在其“新职责”字段中具有值，则在缺省情况下该职责被分配给此用户。有关“新职责”字段的信息，请参阅第 171 页的“用户记录的“新职责”字段”。
工作电话号码	应用程序只解释这些电话号码录入值中的数字。 用户可以输入任何分隔符。
住宅电话号码	
工作传真号码	
寻呼机号码	

新合作者用户记录出现在“用户”列表中。

维护用户资料

系统为每个雇员、合作者用户和客户用户都提供了一个用于更新标识和验证数据的资料屏幕。根据您实施的应用程序和验证体系结构，用户可以执行以下任务：

- 编辑个人信息，例如，地址或时区。
- 在合作者应用程序中编辑公司信息。
- 更改登录口令。
- 更改雇员应用程序中的活动职位。
- 更改合作者应用程序中的主要职位。

各 Siebel 应用程序的资料表单、名称和导航路径有所不同。本节中的过程在 Siebel 雇员、合作者和客户应用程序中很有代表性。各个应用程序中的过程各不相同。

编辑个人信息

用户可以在资料表单中更改各种个人信息。在此上下文中，验证和访问控制数据（例如，口令和职位）不包括在内。

要编辑个人信息

- 1 视应用程序而定，用户执行以下任务之一：
 - 在 Siebel 客户应用程序中，用户单击“我的客户”，然后单击“我的设置”下面的“用户资料”。此时将出现“用户资料”表单。
 - 在 Siebel 合作者应用程序中，用户单击“资料”。此时将出现“个人资料”表单。
 - 在 Siebel 雇员应用程序中，用户选择“导航”>“场地图”>“用户首选项”>“资料”。此时将出现“用户资料”表单。
- 2 如有必要，用户可以单击“编辑”，使表单字段成为可编辑字段。
- 3 用户在可编辑字段中输入或更改数据，然后保存记录。

更改口令

如果您实施数据库或安全适配器验证，用户则可以更改登录口令。

注释：如果您要在 Web SSO 验证环境中实施类似的功能，则负责在外部验证应用程序、用户目录、安全适配器和 Siebel 应用程序视图中配置该功能。Siebel 应用程序文档中未提供配置准则。

要更改口令，用户可以访问第 176 页的“编辑个人信息”中介绍的资料表单，然后填写相应的字段。如果在当前验证体系结构中不能更改口令，则不可以编辑与口令有关的字段。

使用 Siebel 移动 Web 客户机的移动用户还可以更改本地数据库和同步的口令。有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

更改活动职位

Siebel 应用程序的雇员或合作者用户可能具有一个或多个职位，其中一个职位是主要职位。在用户登录时，用户只采用主要职位以及该职位决定的数据访问权限。

雇员可以采用除主要职位之外的其它职位，并且该职位立即成为活动职位。然后，该雇员只能访问新的活动职位决定的数据。

更改活动职位并不会更改雇员的主要职位。雇员在以后登录时，该主要职位将成为活动职位。

用户的数据可视性通常由活动职位决定，而不是由用户关联职位的组合决定。但是，目录和组的可视性以用户的雇员记录为基础，并且与用户的活动职位无关。与多个职位关联的用户可以看到与目录关联、而该目录又与此用户的任何职位关联（或与另一个适用的访问机制关联）的所有记录。

要了解用户的数据可视性，您必须考虑哪些访问控制机制与用户关联（职位、用户列表、访问组等等），以及那些机制与哪些目录或类别关联。

要在 Siebel 雇员应用程序中更改活动职位

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“用户首选项”>“更改职位”。

此时将出现“更改职位”列表。

- 2 单击职位记录以将其选定，然后单击“更改职位”。

此时“活动职位”字段中将为所选职位显示一个选中标志。

合作者用户可以更改主要职位。用户在下次登录时采用该主要职位登录。

要在 Siebel 合作者应用程序中更改主要职位

- 1 合作者用户单击“资料”。

此时将出现“个人资料”表单。

- 2 合作者用户单击“活动职位”选择按钮。

此时将出现“职位”列表。

- 3 合作者用户核选某个职位，使其成为新的主要职位，然后单击记录的“保存”按钮。

- 4 合作者用户单击“确定”。

此时“个人资料”表单中将显示新的主要职位。

- 5 合作者用户注销，然后重新登录，使新的主要职位生效。

10 配置访问控制

本章介绍了您可用于控制访问数据和 Siebel 应用程序功能的机制。它包括以下主题：

- 第 179 页的“关于访问控制”
- 第 185 页的“访问控制机制”
- 第 192 页的“对访问控制的计划”
- 第 197 页的“实施访问控制”
- 第 212 页的“实施访问组访问控制”
- 第 224 页的“通过职责管理选项卡布局”
- 第 226 页的“通过职责管理任务”
- 第 227 页的“清除高速缓存的职责”
- 第 227 页的“附加访问控制机制”
- 第 230 页的“当事方数据模型”

关于访问控制

访问控制是一个术语，用于描述 Siebel 应用程序中控制用户访问数据和应用程序功能的一组机制。

注释：您在阅读本章时，应该确定这里介绍的术语和概念与贵公司的内部术语和结构是如何对应的。本章介绍了此机制及其一般用法，但是您必须确定在计划阶段如何组合此机制，以满足您在业务和安全方面的需要。

在 Siebel 应用程序术语中，屏幕表示一个大块的功能区域，例如处理客户。每个屏幕表现为窗口顶部的一个选项卡。以下示例显示了“客户”屏幕。

每个屏幕包含多个视图，用于提供对数据的各种访问。对于用户而言，一个视图只是一个网页。在一个视图中，用户可能会看到用于显示个人或多个记录的数据记录列表或表单，并且有时还包含子记录。（这些列表和表单在配置上下文中是指子视图。）每个视图（或视图分组）均通过屏幕选项卡下面链接栏中的文本表现。

例如，第 180 页的图 9 显示“客户列表”视图，与子视图标题“我的客户”相对应（当前的可视性筛选器选择）。多个可视性模式提供了对不同视图的访问，不同的视图以不同的方式筛选数据。在“客户列表”视图中，当前的用户可以查看自己的客户或为其分配的客户。该视图包括一个“客户”列表，并且附带了包含选定客户详细信息的表单。从可视性筛选器中选择“全部客户”，可以显示“全部客户列表”视图 - 假设用户有权访问该视图。

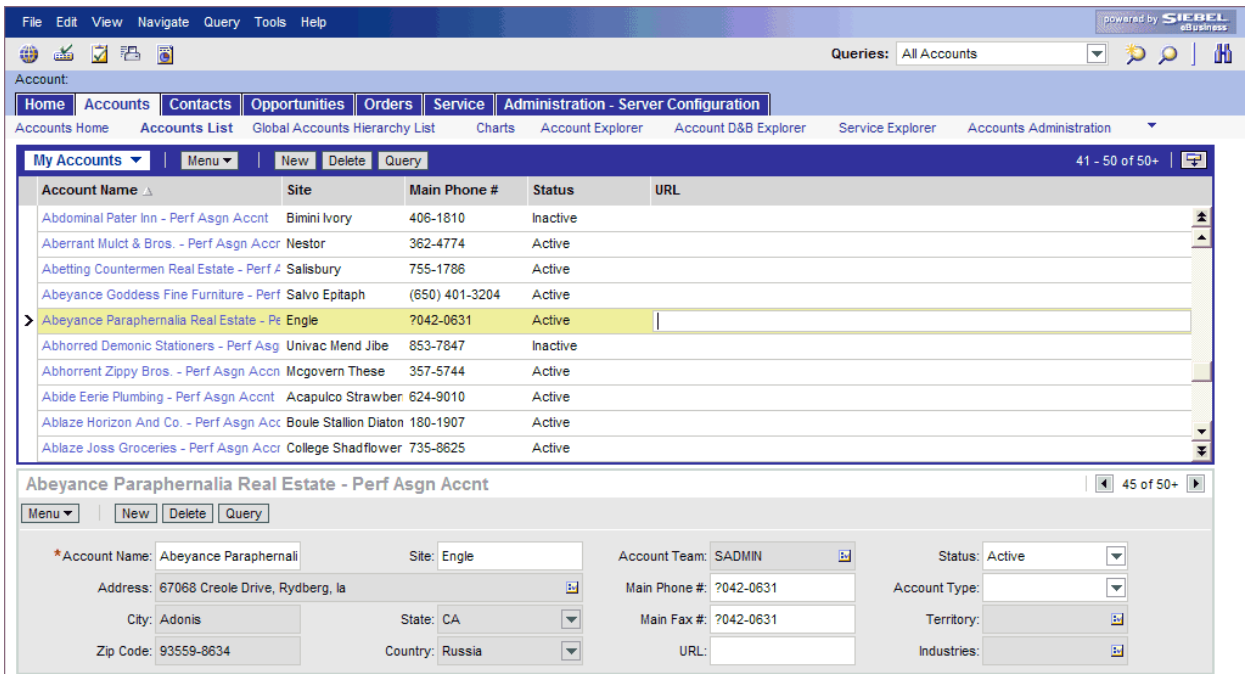


图 9. 我的客户视图

访问控制元素包括以下项：

- **应用程序级别访问控制。**用户可访问的一组屏幕由公司购买的应用程序决定。每个应用程序由一组可用屏幕组成。
- **视图级别访问控制。**在可用屏幕中，您可以通过职责控制可用于特定用户的视图。职责定义了一个视图集合，用于表示执行某个工作职能所需的数据和功能。
- **记录级别访问控制。**您可以通过各种机制控制每一位用户可以看到的数据记录，包括用户的直接记录所有权、以团队方式共同处理记录或者作为该记录所有者成为同一个组织中的成员。

以下小节进一步检查访问控制：

- **当事方。**人员、表示人员的实体以及人员集合统称为当事方。不同当事方类型具有不同的可用访问控制机制。有关详细信息，请参阅第 181 页的“[当事方的访问控制](#)”。
- **数据。**数据类型以及数据是否分类决定了可以应用哪些访问控制机制。有关详细信息，请参阅第 183 页的“[数据的访问控制](#)”。
- **访问控制机制。**您对当事方和数据应用的访问控制机制决定了用户可以看到哪些数据。

有关详细信息，另请参阅以下内容：

- 第 185 页的“访问控制机制”
- 第 192 页的“对访问控制的计划”
- 第 197 页的“实施访问控制”
- 第 212 页的“实施访问组访问控制”

当事方的访问控制

个人、人员分组以及表示人员或组的实体统称为 **当事方**。

注释：有关当事方如何在数据模型级别发挥作用的技术信息，请参阅第 230 页的“当事方数据模型”。

当事方分为以下几种当事方类型：人员、职位、组织、家庭、用户列表和访问组。第 181 页的表 20 描述了不同当事方之间的本质区别，并且为每一个当事方确定了适用的当事方类型。

表 20. 当事方类型和当事方

当事方	当事方类型	示例	区分特征
人员（或联系人）	人员	<ul style="list-style-type: none"> ■ 客户公司的雇员。 ■ 竞争对手公司的雇员。 	<ul style="list-style-type: none"> ■ 人员是指通过数据库中的人员记录表示的个人。 ■ 如果没有附加的属性，人员无权访问您的数据库。
用户	人员	<ul style="list-style-type: none"> ■ 您的 Web 站点的注册客户。 ■ 自行注册的合作者用户，即没有职位的人员。 	<ul style="list-style-type: none"> ■ 用户是指可登录到数据库并且具有某项职责（用于确定哪些应用程序视图可访问）的人员。 ■ Siebel 合作者应用程序中自行注册的合作者具有某项职责，但是不具有与真正的合作者用户类似的职位。
雇员	人员	<ul style="list-style-type: none"> ■ 您的公司的雇员。 	<ul style="list-style-type: none"> ■ 雇员是指与您的公司中某个部门的某个职位关联的用户。
合作者用户	人员	<ul style="list-style-type: none"> ■ 合作者公司内部的雇员。 	<ul style="list-style-type: none"> ■ 合作者用户是指与外部组织中某个部门的某个职位关联的用户。因此，合作者用户也是雇员，但不是内部雇员。

表 20. 当事方类型和当事方

当事方	当事方类型	示例	区分特征
职位	职位	<ul style="list-style-type: none"> ■ 您的公司内部的职称。 ■ 合作者公司内部的职称。 	<ul style="list-style-type: none"> ■ 职位的存在是为了表明报告关系。 ■ 您的公司内部的一个职位与一个部门关联，并且与该部门所属的组织关联。 ■ 合作者公司内部的一个职位与一个部门关联，并且与该部门所属的合作者组织关联。 ■ 一个职位只能与一个部门关联。 ■ 一个职位可能具有一个父职位，还可能具有多个子职位。 ■ 一位或多位雇员可以与一个内部职位关联，并且一位或多位合作者用户可以与一个外部职位关联。 ■ 一位雇员或合作者用户可以与多个职位关联，但是无论何时只有一个职位处于活动状态。
客户	组织	<ul style="list-style-type: none"> ■ 与您有业务往来的公司或个人组合。 	<ul style="list-style-type: none"> ■ 客户通常由联系人组成。 ■ 客户不是一个部门、内部组织或外部组织。 ■ 一个客户可能具有一个父客户，还可能具有多个子客户。 ■ 客户可以被提升为合作者组织。
部门	组织	<ul style="list-style-type: none"> ■ 您的公司内部的组织单位，例如制造部或企业。 ■ 在某个特定国家（地区）工作的一组人员。 	<ul style="list-style-type: none"> ■ 部门的存在是为了将公司的实际结构映射至 Siebel 数据库，并且为职位结构提供一个容器。 ■ 一个部门可能具有一个父部门，还可能具有多个子部门。 ■ 数据不能直接与部门关联。（未指定为组织的部门不能操纵可视性。）
组织	组织	<ul style="list-style-type: none"> ■ 您的公司内部的组织单位，例如欧洲组织。 ■ 合作者公司。 	<ul style="list-style-type: none"> ■ 组织是一个指定为组织的部门。 ■ 组织的存在是为了提供在其中可将职位与数据关联的一个容器。 ■ 组织可以是内部组织，也可以是合作者组织。 ■ 一个部门只能与一个组织关联：部门本身或者也是组织的一个祖先部门。

表 20. 当事方类型和当事方

当事方	当事方类型	示例	区分特征
家庭	家庭	<ul style="list-style-type: none"> ■ 一组人员，通常是居住在同一住所的一个家庭。 ■ 一组居住在不同住所的采购员。 	<ul style="list-style-type: none"> ■ 通常，家庭是指在经济上密切相关并且有共同的采购或服务兴趣的一组个人消费者。 ■ 家庭可能包含联系人、用户、雇员和作为成员的合作者用户的任意组合。 ■ 任何个人均可以属于多个家庭。
用户列表	用户列表	<ul style="list-style-type: none"> ■ 由一些内部雇员和一些合作者用户组成的支持团队。 	<ul style="list-style-type: none"> ■ 用户列表是一个特别的人员组。它可能包含联系人、用户、雇员和作为成员的合作者用户的任意组合。 ■ 用户列表不能具有父项或子项。
访问组	访问组	<ul style="list-style-type: none"> ■ 您的合作者 IT 服务提供商和购买网络设备的 B2B 客户公司。 ■ 合作者团体，例如，您的某个特定产品系列分部的分销商。 	<ul style="list-style-type: none"> ■ 访问组是指一组类型为职位、组织和用户列表的当事方的任何组合，也就是说，它是一组组合。 ■ 一个访问组可能具有一个父访问组，还可能具有多个子访问组。

数据的访问控制

要讨论访问控制，则必须提供以下数据分组：

■ 客户数据

- 客户数据包括联系人和交易数据，例如，商机、订单、报价、服务请求和客户。
- 访问在数据项目级别，通过个人记录所有权或组织所有权等机制进行控制。

■ 主数据

- 主数据包括以下参考数据：产品、说明、解决方案、解决方案项目、决策问题、事件、培训课程和竞争对手。
- 主数据可以归为由类似项目组成的类别，例如，硬盘驱动器。类别然后又可以被组织为目录（例如计算机硬件），这是一些类别的结构。访问在目录和类别级别通过访问组进行控制，这是用于控制对主数据访问的推荐策略。有关创建目录的详细信息，请参阅 *Siebel eSales Administration Guide*。
- 主数据可以与组织关联。通过将主数据与组织关联，可以在数据项目级别控制访问。与访问组策略相比，这种策略需要完成更多的管理工作。

注释：部门提供了一种将职位进行逻辑分组并分配货币的方法。组织提供了一种控制数据访问的机制。

■ 其它数据

- 其它数据包括非主数据的参考数据，例如，价格表、成本列表、费率表和 SmartScript。
- 访问在数据项目级别进行控制。

主数据的数据分类

主数据可以被组织为由分层类别组成的目录。按这种方式组织数据有两个目的：

- **易于浏览。**分类的数据更便于进行导航和搜索。例如，在按产品系列和相关产品子组织的产品目录中，可以很轻松地找到您感兴趣的产品。例如：“计算机硬件” > “硬盘驱动器” > “服务器驱动器”。
- **访问控制。**可以为一个用户集合授予对主数据目录和类别的访问权限。在给定的业务方案中，这是一种控制数据访问的有效方式。例如，您可以控制合作者用户对内部说明的访问。

您可以将主数据进行分类以表现分层结构，例如，产品目录、地理类别、服务授权级别、培训主题区域或渠道合作者。

目录是一个单一的类别结构，如第 184 页的图 10 所示。

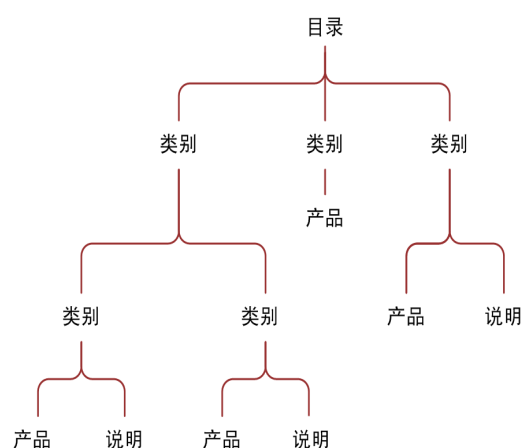


图 10. 目录/类别结构示例

以下属性适用于目录和类别：

- 目录是类别的集合或结构。
- 个人数据项目包含在类别中。
- 一个类别可以包含一个或多个主数据类型。
- 类别可以是唯一一个目录中的一个节点。
- 一个数据项目可以位于一个或多个目录的一个或多个类别中。
- 目录可以是公共目录或私有目录。如果是私有目录，则在目录级别应用某个访问控制。如果是公共目录，所有用户都可以看到该目录，但是不一定可以看到该目录中的类别，具体取决于该类别是私有还是公共。

访问控制机制

主要访问控制机制包括以下几种机制，这些机制将在随后小节中进行介绍：

- **个人访问控制。**有关详细信息，请参阅第 185 页的“关于个人访问控制”。
- **职位访问控制。**包括单一职位、团队和经理访问控制。有关详细信息，请参阅：
 - 第 186 页的“关于职位访问控制”
 - 第 186 页的“关于单一职位访问控制”
 - 第 187 页的“关于团队（多职位）访问控制”
 - 第 187 页的“关于经理访问控制”
- **组织访问控制。**包括单一组织、多组织和子组织访问控制。有关详细信息，请参阅：
 - 第 188 页的“关于组织访问控制”
 - 第 189 页的“关于单一组织和多组织访问控制”
 - 第 190 页的“关于子组织访问控制”
- **全部访问控制。**有关详细信息，请参阅第 191 页的“关于全部访问控制”。
- **访问组访问控制。**有关详细信息，请参阅第 191 页的“关于访问组访问控制”。

关于个人访问控制

如果个人数据可以与数据库中用户的人员记录关联，您则可以限制只有该人员才能访问此数据。

通常，您可以在数据具有创建者或者为该数据分配人员（通常是所有者）时实施个人访问控制。以下是一些示例：

- 在“我的服务请求”视图中，Web 站点访客只能看到他或她已创建的服务请求。
- 在“我的费用报表”视图中，雇员只能看到自己已提交要补偿的费用报表。
- 在“我的活动”视图中，用户只能看到自己拥有的活动。

应用个人访问控制的一些视图包括“我的活动”、“我的个人联系人”、“我的更改请求”和“我的服务请求”。

单词*我的*和*我的个人*经常出现在应用个人访问控制的视图标题中。然而，*我的*并不始终意味着是个人访问控制。有些*我的*视图应用职位或组织访问控制。例如，“我的商机”视图应用职位访问控制。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

关于职位访问控制

职位是内部组织或合作者组织部门中的职称。职位结构表示职位之间的报告关系。在许多方案中，职位提供了一个适当的访问控制基准，因为组织中的职位通常比个人对该职位的分配更稳定。

客户数据和某些参考数据类型可以与一个或多个职位关联。如果个人数据可以与职位关联，您则可以通过以下一种或多种方式，将职位访问控制应用于此数据：

- **单一职位访问控制。**您可以将单一的职位与个人数据记录关联。有关详细信息，请参阅第 186 页的“关于单一职位访问控制”。
- **团队访问控制。**您可以以团队形式将多个职位与个人数据关联。有关详细信息，请参阅第 187 页的“关于团队（多职位）访问控制”。
- **经理访问控制。**您可以同时授予对与职位相关联的数据以及与报告结构中下属职位相关联的数据的访问权限。有关详细信息，请参阅第 187 页的“关于经理访问控制”。

雇员或合作者用户可以与一个或多个职位关联，但是在某个给定时间只有一个职位处于活动状态。雇员或合作者用户的所有职位访问控制类型由活动的职位决定。

用户的其中一个职位被指定为主要职位。在用户登录时，该主要职位是活动的职位。要将其它职位作为活动的职位，则必须具备以下条件之一：

- 雇员必须从“用户首选项”屏幕中将另一个职位指定为活动的职位。
- 合作者用户必须将另一个职位指定为主要职位，然后重新登录。
- 您可以配置座席，让座席使用 Siebel CTI 根据为传入的呼叫提供的数据自动更改职位。

有关 Siebel CTI 和相关模块以及设置座席的信息，请参阅 *Siebel Communications Server 管理指南*。

关于单一职位访问控制

您可以将单一职位与个人数据关联。例如，在“我的报价”视图中，使用特殊职位登录的雇员只能看到与该职位关联的报价。应用单一职位访问控制的其它一些视图包括“我的预测”和“我的报价”。

单词 *我的* 经常出现在应用单一职位访问控制的视图标题中。但是，*我的* 并不始终意味着是单一职位访问控制。有些 *我的* 视图应用个人、组织或团队访问控制。例如，“我的活动”视图应用个人访问控制。

业务组件的视图模式决定了是否可在基于业务组件的视图中应用单一职位访问控制。要使单一职位访问控制可用，业务组件必须具有所有者类型为“职位”、并且在“可视性字段”列（而不是“可视性 MVField”列）中输入值的视图模式（通常是“销售代表”）。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

关于团队（多职位）访问控制

您可以以团队形式将多个职位与个人数据关联。例如，在“我的商机”视图中，具有特殊活动职位的内部雇员或合作者可以看到在商机的销售团队中包括该职位的所有商机。

一个团队可以包括内部职位和合作者职位。

代表职位团队的字段的显示名称可能随团队所在视图而有所不同。有些应用团队访问控制的常用视图参照代表该团队的字段显示名称：

- “我的商机”视图有一个“销售团队”字段。
- “我的客户”视图有一个“客户团队”字段。
- “我的联系人”视图有一个“联系人团队”字段。
- “我的项目”视图有一个“访问列表”字段。

尽管团队的字段可能包含多个职位，如果不向下搜索，则仅显示一个名称。在使用团队访问控制的视图（例如，“我的项目”）中，显示活动登录的名称。而其它视图（例如，使用组织访问控制的那些视图）可能还包含用于该团队的字段。在其它这些视图中，则显示占据主要职位的登录名称。

单词 *我的* 经常出现在应用团队访问控制的视图标题中。然而，*我的* 并不始终意味着是团队访问控制。有些 *我的* 视图应用个人、组织或单一职位访问控制。例如，“我的活动”视图应用个人访问控制。

业务组件的视图模式决定了是否可在基于业务组件的视图中应用团队访问控制。要使团队访问控制可用，业务组件必须具有所有者类型为“职位”、并且在“可视性 MVField”和“可视性 MVLink”列（而不是“可视性字段”列）中输入值的视图模式（通常是“销售代表”）。

团队的某个成员被指定为主要成员。主要成员是经理访问控制中的一个因素，但不是团队访问控制中的因素。

如果为团队访问控制配置了业务组件，为该类型组件添加的任何新记录将遵循此规则：将创建记录的用户添加到记录的团队中并且将该用户设置为主要用户。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

关于经理访问控制

您可以间接地将职位与数据关联，而该数据同时又与报告结构中的下属职位关联。例如，在“我的团队商机”视图中，具有特殊活动职位的雇员可以看到与该职位关联的商机以及与下属职位关联的商机。

经理 - 下属关系由职位结构决定。在您安装 Siebel 应用程序时，一个职位结构将作为 seed 数据被包括在内。

您可以为职位指定一个父职位，表明该职位是此父职位的直属下司。内部职位的父职位可能与该职位在同一个部门，也可能在不同部门。例如，销售部门的销售经理可能向公司的销售副总裁报告工作。

在使用经理访问控制的视图中，该雇员或合作者用户具有对数据的访问权限，具体取决于以下行为：

- 如果该视图所基于的业务组件使用的是单一职位访问控制，用户则看到直接与其活动职位或下属职位关联的数据。
- 如果该视图所基于的业务组件使用的是团队访问控制，用户则看到其活动职位在团队中或作为该团队主要成员的任何下属职位的数据。这是标准行为，称为主要经理可视性。

- 您可以配置使用团队访问控制的业务组件，以允许用户看到所有下属职位的数据，而不考虑这些下属职位是否是记录的主要职位。这称为非主要经理可视性。

要配置非主要经理可视性，请为该业务组件定义称为“经理列表模式”的用户属性，并将其设置为“团队”（而不是缺省值“主要”）。

有关“经理列表模式”用户属性的详细信息，请参阅 *Siebel Developer's Reference*。

警告：要配置非主要经理可视性以支持移动用户，则需要更改同步可视性规则。需要该功能的客户必须预定 Siebel 专家服务。

- 如果视图所基于的业务组件使用的是个人访问控制，其行为与职位访问控制的行为类似：

- 对于单一所有者访问控制，用户则看到直接与其活动职位或下属职位关联的数据。
- 对于多所有者访问控制，用户则看到其活动职位在该团队中或作为该团队主要成员的下属职位的数据。

应用经理访问控制的视图一般在标题中包含短语 *我的小组的*，例如，我的小组的客户。（在某些情况下，省略了单词 *我的*。）

不存在特定于经理访问控制的业务组件视图模式。经理访问控制在视图级别进行设置。它要求视图所基于的业务组件具有所有者类型为“职位”的视图模式。

注释：在使用经理访问控制的视图中，如果经理用户没有所定义的下属职位，该用户则无法在此视图中创建新记录。“新建”按钮和“新建记录”命令不可用。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

关于组织访问控制

如果个人数据可以与组织关联，您则可以通过以下一种或多种方式，将组织访问控制应用于数据：

- **单一组织访问控制。**您可以将单一组织与个人数据关联。有关详细信息，请参阅第 189 页的“关于单一组织和多组织访问控制”。
- **多组织访问控制。**您可以将多个组织与个人数据关联。有关详细信息，请参阅第 189 页的“关于单一组织和多组织访问控制”。
- **子组织访问控制。**您可以同时授予对与组织相关联的数据以及与报告结构中下属组织相关联的数据的访问权限。有关详细信息，请参阅第 190 页的“关于子组织访问控制”。

注释：Siebel Assignment Manager 也启用了组织，也就是说，分配规则可以使用组织作为一项标准。

用户可以在任何给定时间与其活动职位所属的组织关联。有关更改雇员或合作者用户的活动职位的信息，请参阅第 186 页的“关于职位访问控制”。

联系人用户通过为 Siebel 客户应用程序指定的代理雇员间接地与组织关联。

有关代理雇员的信息，请参阅第 6 章“安全适配器验证”和第 261 页的“Seed 数据”。

关于单一组织和多组织访问控制

根据数据的类型，您可以将一个或多个组织与个人数据关联。用户可以看到与其活动组织关联的数据。例如，在“全部服务请求”视图中，用户可以看到与其活动组织关联的所有服务请求。

对于可与多个组织关联的数据，其中一个组织被指定为主要组织。

主要组织是子组织访问控制中的一个因素，但不是多组织访问控制中的因素。

第 189 页的表 21 列出了您可以应用组织访问控制的数据以及可与该数据关联的是单一组织还是多组织。

表 21. 启用组织的数据

对象类型	对象	关系
客户数据	客户	多个
	竞争者	多个
	联系人	多个
	预测系列	多个
	家庭	多个
	市场事件/活动	多个
	商机	多个
	订单	多个
	合作者	多个
	产品缺陷	多个
	项目	多个
	报价	多个
	服务请求	多个
	用户列表	多个
参考数据（包括主数据）	SmartScript	多个
	说明	多个
	价格表	多个
	成本列表/费率表	多个
	期间	单一
	产品	多个
	目录	不适用（目录使用访问组访问控制）

表 21. 启用组织的数据

对象类型	对象	关系
管理数据	雇员	多个
	部门	单一
	值列表类型	多个
	值列表	单一
	职位	单一
	职责	多个

注释：使用 Siebel Configurator 创建的可定制产品包括一些不使用组织访问控制的例外产品。有关可定制产品可视性的信息，请参阅 *Product Administration Guide*。

全部（但不是跨...的所有）经常出现在应用单一组织或多组织访问控制的视图的标题中。例如，“全部联系人”视图应用单一组织访问控制，而“全部产品缺陷”视图应用多组织访问控制。但是，**全部**并不始终意味着是单一组织或多组织访问控制。有些**全部**视图应用**全部**访问控制。例如，“全部服务请求”视图应用**全部**访问控制。

业务组件的视图模式决定了是否可在基于该业务组件的视图中应用单一组织或多组织访问控制。

- 要使单一组织访问控制可用，业务组件必须具有所有者类型为“组织”、并且在“可视性字段”列（而不是“可视性 MVField”列）中输入值的视图模式（通常是“组织”）。
- 要使多组织访问控制可用，业务组件必须具有所有者类型为“组织”、并且在“可视性 MVField”和“可视性 MVLink”列（而不是“可视性字段”列）中输入值的视图模式（通常是“组织”）。

有关**全部**访问控制的信息，请参阅第 191 页的“关于全部访问控制”。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

关于子组织访问控制

子组织访问控制以分层组织为基础，它与经理访问控制相类似，后者以分层职位为基础。

对于组织结构中的任何组织，您可以授予访问与下属组织关联的数据的权限。该访问控制机制用于提供累计数据视图。

例如，某个洲际销售组织的总监可以看到其下属区域性销售组织的累计数据。总公司销售组织的副总裁则可以看到各个洲际销售组织和区域性销售组织的累计数据。

下属关系从组织结构决定，而管理员可以通过选择“导航”>“场地图”>“管理 - 组”>“组织”进行查看。

在您安装 Siebel 应用程序时，组织结构将作为 seed 数据被包括在内。在组织结构中，您可以为内部组织结构和合作者组织结构创建分支。

您可以为组织指定一个父组织。

在使用子组织访问控制的视图中，用户可以访问以下数据：

- 如果视图所基于的业务组件使用的是单一组织访问控制，用户则看到直接与其活动组织或后代组织关联的数据。
- 如果视图所基于的业务组件使用的是多组织访问控制，用户则看到其活动组织或后代组织是主要组织的数据。

应用子组织访问控制的缺省视图的标题按跨我的组织的所有业务组件名称构建，例如，跨我的组织的所有商机。

不存在特定于子组织访问控制的业务组件视图模式。子组织访问控制在视图级别进行设置。它要求视图所基于的业务组件具有所有者类型为“组织”的视图模式。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

关于全部访问控制

全部访问控制按业务组件的任何视图模式定义，提供了对具有有效所有者的所有记录的访问权限。所有者可能是人员、职位、团队中有效的主要职位或组织，具体取决于业务组件的可用视图模式。

在其职责中存在应用了全部访问控制的视图的所有用户都可以在该视图中看到相同的数据。用户的人员或职位不需要与此数据关联。

全部访问控制主要提供了跨所有组织的数据视图。例如，在“跨组织的所有报价”视图中，用户则看到与企业中任何内部或外部组织关联的、具有有效人员、职位或组织所有者的所有报价。

短语跨...的所有和全部经常出现在应用全部访问控制的视图标题中。例如，“跨组织的所有商机”和“全部服务请求”视图应用全部访问控制。然而，全部并不始终意味着是全部访问控制。有些全部视图应用单一组织或多组织访问控制。例如，“全部联系人”视图应用单一组织访问控制。

单独的属性（管理模式）提供了查看使用团队访问控制的视图中的所有记录的方式，包括没有有效所有者的那些记录。管理模式使管理员可以修改其它任何人无法看到的记录。您可以在“管理模式标志”属性中为视图指定管理模式。

不存在特定于全部访问控制的业务组件视图模式。全部访问控制在视图级别进行设置。

有关业务组件视图模式的信息，请参阅第 203 页的“业务组件视图模式”。

有关在视图中实施访问控制的信息，请参阅第 208 页的“视图访问控制属性”。

有关管理模式的信息，请参阅第 208 页的“视图访问控制属性”。

关于访问组访问控制

访问组用于控制各种当事方类型组对主数据的访问。

有关管理访问组访问控制的信息，请参阅第 212 页的“实施访问组访问控制”。

访问组是职位、组织、客户、家庭和用户列表任何组合的集合。其成员是当事方类型的实例，而不是人员类型的实例，也就是说，其成员不能是个人。例如，访问组可能由多个合作者组织以及您要为其授予对一组特定销售工具访问权限的用户列表组成。

注释：尽管您可以将部门添加到访问组，但是这样做对可视性没有影响。请改为使用组织。

如果在当前会话期间，用户与作为某个访问组成员的职位、组织、客户、家庭或用户列表关联，用户则与该访问组关联。

您可以创建访问组的结构。访问组只能属于一个访问组结构，也就是说，访问组只能有一个父访问组。例如，前面提到的访问组可能要属于访问组的某个结构，才能被授予对销售工具的不同访问级别。

您还可以为访问组授予对主数据目录和类别的访问权限：产品、说明、解决方案、决议项、决策问题、事件、培训课程和竞争对手。例如，可以为上述访问组结构中的分支授予对分层目录中类别的访问权限，在分层目录中每个类别都包含销售说明和决策问题项。有关访问组结构（主数据）的图示，请参阅第 183 页的“数据的访问控制”。

主数据类别可以包含主数据项目的任何组合。您只能控制对主数据的目录和类别的访问，但不能控制对使用访问组访问控制的单个主数据项目的访问。

如果访问组与目录或目录中的类别关联，则可以应用访问组访问控制。您可以通过以下方式之一控制对数据的访问：

- **组。**如果在给定类别中，用户则看到该类别中他（她）有权访问的第一级子类别列表或当前类别中的所有数据记录，具体视使用的子视图而定。如果用户位于目录级别，用户则看到第一级类别。
- **目录。**用户则看到跨所有目录的类别中的所有数据组成的平面列表，这些目录是指此用户有权访问的所有目录。此访问控制类型通常用于产品选取列表和其它产品列表中，例如，推荐产品列表。

有关数据和数据分类的详细信息，请参阅第 183 页的“数据的访问控制”。

有关当事方的详细信息，请参阅第 181 页的“当事方的访问控制”。

对访问控制的计划

以下两种主要策略可用于控制对 Siebel 应用程序中的数据访问：

- **多组织访问控制。**该策略将数据访问限定为需要查看信息的那些组织。组织访问控制可以跨内部或外部组织执行。该策略可以应用于交易数据、主数据和其它参考数据。
有关详细信息，请参阅第 188 页的“关于组织访问控制”、随后的小节以及第 197 页的“实施访问控制”。
- **对按目录分类的数据的访问组访问。**该策略可以通过所有当事方类型实施。它将分层的用户组与按类似方式组织的数据关联，从而减少了访问控制的管理工作。该策略只能应用于主数据。
有关详细信息，请参阅第 191 页的“关于访问组访问控制”和第 212 页的“实施访问组访问控制”。

有关选择和实施访问控制策略的分析及建议，请参阅 Siebel SupportWeb 上的 *Access Control Upgrade and Migration Guide for Siebel 7*。

访问控制和业务环境结构

作为实施应用程序的访问控制策略的一部分，您必须定义贵公司的结构、外部合作者的关系等等。您还必须定义人们为履行其工作职能而需要访问和使用的数据及对象的类型。您如何定义业务环境结构将会直接影响访问控制如何应用于您的用户。

本小节提供了有关业务环境结构的一些背景信息。如果您的企业规模大而复杂，您可以在设置 Siebel 应用程序时准确地反映企业的结构。您可以建立多级的组织、部门和职位结构。例如，通过父子关系将职位与其它职位关联，即可建立一个结构。

定义业务环境结构涉及设置第 193 页的表 22 中所示的元素。

表 22. 业务环境结构的元素

元素	父子关系	说明
部门	Y	公司（或合作者公司）组织的子单位。用于设置缺省货币。可以用于 Actuate 报表中。不用于控制数据的可视性。
组织	Y	构成您的公司（或合作者公司）的主要部分或实体。用于控制数据的可视性。请参阅第 188 页的“关于组织访问控制”。
职位	Y	控制用户有权访问的数据集（记录）。请参阅第 186 页的“关于职位访问控制”。
职责	N	控制用户有权访问的视图。
雇员	N	您的公司和合作者公司中有权访问您的公司数据的个人用户。

您可以按任意顺序设置部门、组织、职位、职责和雇员，还可以以各种方式将这些记录类型相互关联。例如，要链接职责和雇员，您可以将此雇员与职责记录中的该职责关联，或者将该职责与雇员记录中的此雇员关联。

注释：由于组织以部门为基础，因此，最好先创建部门结构，然后确定将其中哪些部门指定为组织。

警告：更改公司结构（例如，职位和部门）可能会导致 Siebel Remote 组件（交易路由器）重新评估与所更改对象关联的所有对象的访问控制。这可能导致性能下降。有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

多组织的优点

使用组织可以提供以下优点：

- 它允许公司将自己分成多个逻辑组，然后显示其中每个组的适当信息。
- 它提供了根据为其分配职位的组织限制数据可视性（访问权限）的能力。
- 它同时对客户数据（客户、商机、服务请求等等）和主数据（价格表、说明等等）产生影响。
- 它允许您将技能分配给组织，从而允许 Assignment Manager 根据组织进行分配。
- 它允许您设置呼叫中心的多重任务执行。有关详细信息，请参阅 *Siebel Communications Server 管理指南*。

决定是否设置多组织

如果已部署 Siebel 应用程序，并且您不需要更改用户的可视性（访问权限），您的公司可能不需要更多的组织。下面是您的公司可能从多组织中获益的一些情形：

- **内部业务单位。**如果您有少量独特的内部业务单位，则可能要使用组织以支持数据实体数量有限的特定版本，例如，产品和价格表。
- **复杂的全球性企业。**如果您有一家大规模的全球性企业，包括了多项内部和外部业务，并且每一项业务由多个业务单位组成，您的公司则可以从实施多组织获益。在这种情形下，某些数据应当只能用于某些业务单位，而其它信息必须在企业级别共享。

- **内部和外部单位。**如果您的公司与外部合作者公司共享数据，则可以将每一个合作者公司设置为组织。您可以减少可用于这些外部组织的视图，使其小于可用于内部组织的视图。您还可以配置雇员下拉列表，以便只显示属于此用户组织的雇员。
- **不同的业务单位规则。**如果您要将不同的 Siebel Assignment Manager 或 Siebel Workflow 规则应用于公司的不同部分，您的公司将从实施多组织获益。例如，公司可能需要将一些 Assignment Manager 规则应用于电话销售组织，而将其它一些规则应用于 Web 站点客户。
- **启用 Web 的企业。**如果您拥有通过 Web 站点登录的客户，则可以设置客户组织以控制客户对视图和数据的访问。如果您拥有通过 Web 站点登录的渠道合作者，则可以设置渠道合作者组织以控制其访问。

有关将组织与 Siebel 客户和合作者应用程序配合使用的详细信息，请参阅 *Siebel Partner Relationship Management Administration Guide*。

对部门的计划

本节和后面的小节介绍了在 Siebel 应用程序中定义公司结构的公共任务，其中包括定义部门、组织、职责和职位的任务。

部门属于组织，并且对可视性没有直接影响。部门帮助您将职位分组以记录地址和维护缺省货币。用户报告结构由其父职位定义，但是用户运作时所在的国家/地区和货币由其部门定义。

要实施 Siebel eBusiness Applications，您至少必须设置一个部门。

一个组织可以包含多个部门，但是某个给定部门只能属于一个组织。您可以将组织安排到父组织和子组织的结构中。

您还可以将部门提升为组织。您可以通过将一些部门指定为其它部门的父部门，将多个部门安排到多级别的结构中。

您可以将多个职位分配给一个部门。然后在您将雇员与这些职位关联时，该雇员就会与此部门关联。

部门也可用于 Actuate 报表中。有关报表的详细信息，请参阅 *Siebel 报表管理指南*。

注释：您不能删除部门记录，这是因为整个 Siebel 应用程序中的业务组件都引用组织记录。删除部门将导致对交易记录的引用无效，从而导致出现意外的负面效果，例如，有效数据未显示在用户界面中。

对组织的计划

设计组织是为了代表公司中最广泛的部门。组织将控制分配给它的雇员对数据的访问。组织可以是内部组织，也可以是外部组织（如果是 Siebel PRM）。

与雇员的活动职位关联的组织将确定雇员的可视性。相反，与雇员关联的组织（例如使用“雇员”业务组件中的“雇员组织”字段）将确定该雇员对雇员记录的可视性。

设置组织是实施应用程序中的一个可选步骤。如果要从 Siebel 应用程序的以前版本升级，所有数据则自动被分配给一个缺省组织。使用一个组织将对可视性和数据访问不产生影响。然而，如果要将公司分为多个结构单位，则可以创建多个组织。

您可能要将用户的管理工作授权给只访问其用户的组织。为此，您必须使用 Siebel Tools 配置相应的视图。有关配置视图的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

以下是处理组织的最佳惯例：

- 建议不合并组织。由于为多组织访问控制配置了许多业务对象，因此，您可能会在极大范围内破坏这些关系，并产生意外后果。
- 建议不要更改缺省组织的名称，即“缺省组织”。该记录是 seed 数据，在许多位置都被引用。如果您的公司决定更改缺省组织名称，该名称必须唯一，必须不同于其它任何组织或部门的名称，同时还必须在其它位置更改对缺省组织的引用。

例如，您在使用 Siebel Assignment Manager，可能需要将分配对象中的引用重命名为该缺省组织的新名称。有关详细信息，请参阅 *Siebel Assignment Manager Administration Guide* 和 *Configuring Siebel eBusiness Applications*。

注释：您不能删除组织记录。整个 Siebel 应用程序中的业务组件均引用组织记录。删除组织可能导致交易记录上的引用无效。这可能导致出现意外的负面效果，例如，有效数据未显示在用户界面中。

对职位的计划

职位表示公司中的特定工作位置。在您定义公司结构时，请通过部门结构中的每个级别定义特定职位。职位决定了用户有权访问哪些记录。您必须登录到服务器数据库才能添加职位。

注释：雇员应当具有一个职位，才能在 Siebel 应用程序中创建和使用客户、商机、联系人以及其它客户数据对象。

通常每个职位只有一位关联的雇员。在某些情况下（例如共同分担工作），一个职位可能具有多个关联的雇员。一位雇员可以与多个职位关联。一个职位只能具有一位主要雇员，但是，一位雇员可以是多个职位的主要雇员。

将多位雇员与一个职位关联会造成一些不便。由于一个职位只能具有一位主要雇员，因此在“雇员”字段中只有该主要雇员才可见。如果您在职位列表中搜索某位雇员，但是该雇员不是此职位的主要雇员，则可能找不到相关的职位记录。

只有职位的主要雇员才显示在“客户团队”、“商机销售团队”和“联系人访问”列表中。然而，该职位的所有雇员都可以访问“我的客户”、“我的商机”和“我的联系人”视图。

一个职位只能与一个组织关联。如果希望雇员可以看到多个组织，则必须为每个组织创建一个职位，并且将该雇员分配给每个职位。然后，雇员可以通过更改职位一次看到一个组织的数据。

职位可以在多级别的结构中设置，从而允许实施经理访问控制。对于各子职位可视的所有数据集，父职位均可见。（通常，此数据仅显示在子职位是团队或记录的主要职位的位置。）

您的 Siebel 应用程序允许用户将其职位更改为管理员已为其授权的其它职位。用户可以在登录时通过以下方式更改职位：选择“工具”>“用户首选项”>“更改职位”，在列表中选择其它职位，然后单击“更改职位”按钮。例如，销售代表可以将其职位更改为销售主管，并且可以访问与以前职位相同的视图，但是还可以看到其它组织的数据。

注释：您不能通过设置结束日期使职位作废。该字段只为与该职位关联的当前雇员记录结束日期。它不会在到达结束日期之后使该职位作废。

警告：请勿删除职位。这可能会导致出现意外的负面效果。例如，您删除了客户的主要职位，并且您没有为该客户选择新的主要职位，Assignment Manager 可能无法将资源分配给该客户的活动。

如果您重命名某个职位，请在 Siebel 应用程序中的以下区域进行检查，以确保这些区域正确地反映了名称变更：

- 分配规则，如果您在分配规则中使用了这些职位。有关详细信息，请参阅 *Siebel Assignment Manager Administration Guide*。
- 工作流程过程，如果您在工作流程过程中使用了这些职位。有关详细信息，请参阅 *Siebel Business Process Designer Administration Guide*。

- Enterprise Integration Manager (EIM)，如果您在 EIM 导入 SQL 脚本中正引用这些职位。有关详细信息，请参阅 *Siebel Enterprise Integration Manager Administration Guide*。
- “雇员”视图的“职位”字段。

注释：如果您更改了移动用户的职位，该用户的可视性规则将相应地变化。在此情况下，建议该用户重新提取其本地数据库。然而，如果您只更改了职位名称（例如，从销售代表更改为销售助理），则不需要重新提取。这是因为在存储职位名称的数据库表中，此列在整个企业中可视。换句话说，对该列所做的更改将分布到所有的用户。另请参阅第 235 页的“职位数据模型”。

对职责的计划

职责决定了用户有权访问哪些视图。例如，“系统管理员”职责允许访问所有视图。定义职责可以让您限制用户对视图的访问，因此可以限制对 Siebel 应用程序的信息和功能的访问。您必须为所有用户分配职责。用户如果没有职责，就不能使用 Siebel 应用程序，因为他（她）不能访问任何视图。

您还可以为职责分配选项卡布局 and 任务。有关详细信息，请参阅第 224 页的“通过职责管理选项卡布局”和第 226 页的“通过职责管理任务”。

注释：建议您在适用的位置使用作为 seed 数据提供的职责。然后，定义所需的与组织中的主要工作职能相对应的任何附加职责。

例如，您可能使用或创建市场营销管理员、销售经理和销售代表职责。销售代表职责可能有权访问所有视图，但不包括销售管理、市场营销管理和应用程序管理保留的那些视图。销售经理职责可能有权访问与销售代表相同的视图，以及销售经理的视图等等。

如果适用，您可以将某个视图指定为对某个给定职责只读。

要定义职责，您必须指定可用于该职责的视图。您可以使用 Siebel 应用程序附带的 seed 职责。您可以复制然后定制这些职责。

注释：您不能修改或删除 seed 职责。例如，您不能更改 Siebel 管理员职责。您可以复制 seed 职责，然后修改副本。

在定义职责时，请考虑以下问题：

- 您应当仅为某个选定的管理员组授予对“系统首选项”视图的访问权限，而不应当为最终用户授予对“系统首选项”视图的访问权限。“系统首选项”用于控制整个系统的多个项目，包括 Siebel Remote 和 Siebel Assignment Manager 的一些服务器逻辑和处理。
- 您不能为与最终用户关联的职责添加“管理”视图。同样，您应当限制对“主预测”、“移动 Web 客户机”、“职责”、“视图”和“地区”视图的访问。通过这些视图执行的工作对整个应用程序会产生深远的影响。
- 在用户需要访问某个视图中显示的数据，但应当不可以创建或修改数据时，请将此视图指定为对该职责只读。（如果用户的任何一个职责与未标记“只读视图”标志的视图关联，该视图对此用户就不是只读，并不考虑是如何为其它任何职责设置此标志的。）
- 您可能希望通过从用户的职责中删除与许可证密钥有关的视图，隐藏对许可证密钥的访问权限。有关许可证密钥的详细信息，请参阅 *应用程序管理指南*。
- 如果将“内部部门”视图添加到用户的职责中，则将显示组织选取列表中的所有组织。缺省情况下，只有用户所属的组织才显示在此选取列表中。

- 如果您通过正常的 Siebel Web 客户机登录到应用程序中，则可以在“管理 - 应用程序” > “职责”视图中将新的视图添加到职责中。

然而，如果您通过 Siebel 移动或专用 Web 客户机登录到应用程序中，“职责”视图的“视图”子视图中的“新建”按钮将不可用。要激活该按钮，以便您可以将视图添加到使用这些客户机类型的职责中，您可以使用命令行选项 `/editseeddata` 启动 Siebel 客户机。

警告：在使用 `/editseeddata` 命令行选项之前，您必须充分认识到该功能对数据可能造成的影响。通常建议不使用该选项。

有关 Siebel 移动或专用 Web 客户机的启动选项的详细信息，请参阅适用于您正在使用的操作系统的 *Siebel 安装指南*。

实施访问控制

视图中显示的特殊数据以及是否显示视图由相关组件的设置决定。

您可以对 Siebel Tools 中的大多数此类设置进行配置。本节指定在何处找到 Siebel Tools 中的这些设置，但是大多数情况下未提供实施设置的过程。更改 Siebel Tools 中的任何设置均要求重新编译 Siebel 库文件。

有关使用 Siebel Tools 时所需惯例的详细信息，请参阅 *Configuring Siebel eBusiness Applications* 和 *使用 Siebel Tools*。

以下组件决定了用户将看到哪些视图：

- **应用程序。**每个 Siebel 应用程序都包括获得许可的一组视图。如果用户在应用程序中，则无权访问未包括在该应用程序中的视图。
- **职责。**每位用户具有一个或多个职责，用于定义用户有权访问的视图集合。如果某个特殊视图不在用户的职责中，用户则看不到该视图。“跨组织的所有商机”等范围较大的视图通常未包括在地区销售代表等雇员的职责中。

以下组件决定了视图中用户有权访问的数据。

- **业务组件视图模式。**一个视图可以具有多个子视图 - 列表、表单或树。每个子视图都以业务组件为基础。业务组件的视图模式决定了允许将哪些当事方作为该业务组件的访问控制的基础。业务组件的视图模式还决定了如何确定与当事方的关联，例如，是“所有者”还是“创建者”。
- **子视图可视性属性。**一个视图可以将其中一个子视图指定为可视性子视图。可视性子视图用于将业务组件连接到视图。可视性子视图指定了要使用哪些业务组件以及业务组件字段的显示名称。
- **视图可视性属性。**视图的可视性属性确定对该视图所基于的业务组件应用哪种访问控制机制。例如，业务组件可能可以使用个人或职位访问控制。视图指定了要使用其中哪种访问控制机制，以及在哪个表单中使用此机制。

简而言之，应用程序和用户的职责限制了为该用户显示的视图。在视图中，视图的可视性属性确定了在该视图中操纵可视性的子视图，并指定要对业务组件应用的访问控制机制。视图的可视性子视图指定了视图中使用的业务组件。业务组件指定了可以如何将用户与数据关联以提供访问权限。

应用程序和访问控制

每个 Siebel 应用程序都与一组屏幕关联。反过来每个屏幕都由一组视图组成。

在特定应用程序中，所有用户都被限定为只能访问公司获得许可的视图以及为该应用程序定义的视图。获得许可的视图在许可证密钥中指定，后者由您购买的 Siebel eBusiness Applications 的功能决定。

要查看应用程序包括哪些视图

- 1 以管理员身份登录。
- 2 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 应用程序”>“视图”。

下图显示为应用程序定义的一些视图的示例列表。

Views Menu New Delete Query 111 - 122 of 132+			
View Name ▲	Description	Default Local Access	
Activity Attachment View	Activity Attachment	✓	▲
Activity Briefing View	Activity Briefing Vie	✓	▲
Activity Chart View - Activity Analysis	Activity Chart View	✓	
Activity Chart View - Contact Analysis	Activity Chart View	✓	
Activity Chart View - New Activities Analysis	Activity Chart View	✓	
Activity Chart View - Status Analysis	Activity Chart View	✓	
Activity Chart View - Status Analysis by Owner	Activity Chart View	✓	
Activity Chart View - Symptom and Resolution Analysis	Activity Chart View	✓	
Activity Chart View - Trend Analysis by Activity Type	Activity Chart View	✓	
Activity Chart View - Trend Analysis by Product	Activity Chart View	✓	
Activity Contact Employee View	Activity and Multiple	✓	▼
Activity Contacts View	Activity Contacts Vi	✓	▼

有关配置屏幕和视图的信息，请参阅 *Configuring Siebel eBusiness Applications*。

设置部门、组织和职位

本主题介绍如何设置部门、组织和职位。

设置部门

本节介绍如何设置部门。

要设置部门

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 组”>“内部部门”。

此时将显示“内部部门”视图。

- 2 在表单中，添加新记录并填写必需的字段。

下表介绍了其中一些字段。

字段	准则
父部门	如果该部门是子部门，请选择此父部门，从而允许某个部门与另一个部门关联。
组织类型	表示组织的类型，用于控制在应用程序的哪个位置显示该部门以供选择。 例如，“组织类型”为“服务”的部门出现在“服务”屏幕“服务请求”视图的“组”字段中以供选择。
组织标志	如果选定，则表示该部门也是一个组织。系统会将该部门复制到“组织”视图中。

设置组织

本节介绍如何设置组织。

要设置组织

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 组” > “组织”。

此时将显示“组织”视图。

- 2 在表单中，添加新记录并填写必需的字段。

下表介绍了其中一些字段。

字段	准则
父组织	如果该组织是子组织，请选择此父组织，从而允许某个组织与另一个组织关联。
合作者标志	用于 Siebel PRM。这是一个只读复选框。如果选择该复选框，则表示该组织代表的是一个外部企业，它是您公司的父组织。 注释： 如开发和部署 <i>Siebel eBusiness Applications</i> 中所述，使用“管理 - 合作者”屏幕中的“批准合作者”视图，注册合作者并将其提升为组织。

设置职位

本节介绍如何设置职位。

要设置职位

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 组” > “职位”。

此时将显示“职位”视图。

- 2 在表单中，添加新记录并填写必需的字段。

下表介绍了其中一些字段。

注释：表单中的大多数字段将根据活动雇员的雇员记录自动被填入。如果您尚未设置雇员，则可以在以后将雇员与职位关联。

字段	准则
开票产品	用于 Siebel Professional Services 自动化。
可奖励	用于激励奖金。
结束日期	要将当前已关联的雇员与该职位关联的最后一天。
姓氏	选择要担任该职位的一位或多位雇员。在“已分配雇员”对话框中，如果您要将某位雇员作为该职位的主要雇员，请选择该雇员的“主要”字段。
父职位	如果该职位是子职位，请选择此父职位，从而允许将某个职位与另一个职位关联。

字段	准则
职位类型	职位的类型。该字段是一个信息字段，对可视性没有影响。
地区	允许将职位与地区关联。用于 Siebel Assignment Manager。

设置职责并添加视图和用户

本节介绍如何设置职责并添加视图和用户。

要定义职责并添加视图和用户

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 应用程序” > “职责”。

此时将显示“职责”视图。

注释：缺省情况下，“职责”视图显示所有职责，而不考虑其组织。然而，您可能要在 Siebel Tools 中配置新视图，以限制职责的可视性。有关配置视图的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

- 2 在“职责”列表中添加新记录，并输入该职责的名称和说明。

- 3 在“组织”字段中，为职责选择组织。

- 4 要添加视图，请执行以下操作：

- a 在“视图”列表中，添加新记录。

- b 在“添加视图”对话框中选择相应的视图，然后单击“确定”。在添加视图时，如果对于使用此职责的用户而言该视图是只读的，请设置“只读视图”标志。

注释：您还可以从“视图”列表中删除视图。

- 5 要添加用户，请执行以下操作：

- a 在“用户”列表中，添加新记录。

- b 在“添加用户”对话框中选择相应的用户，然后单击“确定”。

注释：您还可以从“用户”列表中删除雇员。

职责和访问控制

一个职责对应于一组视图。必须至少为每位用户分配一个职责。如果为用户分配职责，该用户将有权访问为该用户分配的所有职责中包含的所有视图，这些视图也包括在用户的当前应用程序中。

如果应用程序中的某个视图未包括在用户的职责中，用户将不会在“场地图”、链接栏或任何其它选取列表中看到此视图或此视图的列表。如果用户无权访问某个屏幕中的任何视图，则不会显示“场地图”中该屏幕的列表及其屏幕选项卡。

例如，分配给管理员的职责可能包括“管理 - 应用程序”屏幕中的视图。管理员将在“场地图”中看到列出的该屏幕，并且可以导航到该屏幕包含的视图。通常，客户服务座席的职责中没有管理视图，因此，座席将看不到在任何上下文中列出的该屏幕或其视图。

每位用户的主要职责还控制用户的缺省屏幕或视图选项卡布局。有关详细信息，请参阅第 224 页的“通过职责管理选项卡布局”。

一位用户可以有一个或多个职责。用户有权访问所分配的所有职责组合中的所有视图。例如，您可能为销售经理同时分配了销售经理职责和现场销售代表职责。

注释：在某些情况下，修改应用程序的可视性或职责设置可能需要重新启动相关的应用程序对象管理器 (AOM)，才能使这些新设置对 Siebel Web 客户机的用户生效。如果您只修改了职责，则可以清除高速缓存的职责，而不必重新启动 AOM。有关详细信息，请参阅第 227 页的“清除高速缓存的职责”。

将职责与组织关联

您可以将职责与一个或多个组织关联。

注释：只有在您实施用户的授权管理，例如为 Siebel Partner Portal（适用于 Siebel PRM），才应该将职责与组织关联。

合作者用户可以看到与该组织关联、而该组织又与此用户关联的职责。合作者用户与该组织关联、而该组织又与此用户的主要职位关联。

用户可以跨组织获得职责分配，以便于向用户提供视图的访问权限。然而，用户只能看到与用户的活动组织关联的职责。

例如，您可能决定只能由内部管理员，而不是其他授权的管理员为用户分配授权的管理员职责。然后，用户就可以具有授权的管理员职责，但是，他（她）无法在职责列表中看到该职责。因此，授权的管理员不能将该职责分配给其他用户。要实现此方案，请将授权的管理员职责与某个组织关联，而该组织不是与授权的管理员关联的那个组织。

注释：如果您要在职责中包括使用职位或组织访问控制的视图，则应该将每个职责至少与一个组织关联。

视图和职责的本地访问

每个视图和职责都有一个“本地访问”标志。这些设置共同决定视图是否可供具有特定职责的 Siebel 移动 Web 客户机的用户访问。

“本地访问”标志的设置不会影响使用 Siebel Web 客户机或 Siebel 专用 Web 客户机的用户对视图的访问。

如果“本地访问”设置为 TRUE（选定），其中一个职责中包含此视图的用户可以在使用 Siebel 移动 Web 客户机（连接至本地数据库）时访问此视图。如果“本地访问”设置为 FALSE（取消选定），用户则无法在使用移动 Web 客户机时访问此视图。

“本地访问”标志出现以下位置：

- “视图”列表中的缺省“本地访问”标志位于“导航”>“场地图”>“管理 - 应用程序”>“视图”下面。除非该设置在另一个上下文中被覆盖，否则该设置将为视图定义要继承的缺省设置。
- “视图”列表中的“本地访问”标志位于“导航”>“场地图”>“管理 - 应用程序”>“职责”下面。该设置将显示或覆盖对作为当前职责子项的视图记录适用的缺省设置。只有在通过与特定职责记录关联让用户可以使用视图时，该设置才对视图产生影响。
- “职责”列表中的“本地访问”标志位于“导航”>“场地图”>“管理 - 应用程序”>“视图”下面。该设置将显示或覆盖对作为当前职责父项的视图记录适用的缺省设置。只有在通过与特定职责记录关联让用户可以使用视图时，该设置才对视图产生影响。

第 202 页的图 11 显示了为与职责关联的视图指定的“本地访问”字段（在“职责”视图中可以看到）。

Responsibilities			
Menu New Delete Query Clear Cache 199 - 208 of 210+			
Responsibility	Description	Organization	Web Access
Time & Expense Reporting	Time Sheet and Expense Report	Default Organization	
Training Manager	Training Manager	Default Organization	
Universal Agent	Siebel Universal Agent	Default Organization	
Universal Agent		Siebel Americas	
Universal Agent (B2B+B2C)		Default Organization	
Universal Agent (MME)		Default Organization	
Unregistered Partner Agent	Unregistered Partner Agent (eChannel)	Default Organization	
Unregistered Visitor	Unregistered Visitor	Default Organization	
Usage Accelerator - Administrator		Default Organization	
Usage Accelerator - Sales Executive	Usage Accelerator - Sales Executive	Default Organization	

Responsibilities Tab Layout Tasks			
Views Menu New Delete Query 1 - 12 of 12+			
View Name	Description	Local Access	Read Only View
Web Collab All Activities View	Web Collab All Activ	✓	
Web Collab All Activities Attachme	Web Collab All Activ	✓	
Web Collab Activity List/Detail View	Web Collab Activity	✓	
Web Collab Activity List/Detail View	Web Collab Activity	✓	
Web Collab Activity List/Attachmer	Web Collab Activity	✓	
Visible Contact List View	Visible Contact List	✓	
User Profile Spell Check View	User Profile Spell Ch	✓	

Users Menu New Delete Query 1 - 12 of 12+			
Last Name	First Name	User ID	Job Title
Arnold	Ted	TARNOLD	Telesales representative
Cheng	Casey	CCHENG	Universal Agent (Call Center)
		RAISAKA	
Rubin	Jason	JRUBIN	Director, Product Marketing-F
Collins	Dana	DCOLLINS	Dispatcher
Roper	Deanne	DROPER	Field Engineer
Edwards	Stacey	SEDWARDS	Field Service Engineer

图 11. 职责视图

“本地访问”字段是一种机制，用于控制移动用户在使用 Siebel 移动 Web 客户机时可以使用哪些视图。除根据职责对视图启用或禁用本地访问之外，管理员还可以提供不同的一组视图以供不同的移动用户访问。有关详细信息，请参阅 *Siebel Remote and Replication Manager Administration Guide*。

警告：您应该将“本地访问”字段设置为 FALSE，以禁止对应用了“全部”访问控制的视图进行访问。对于移动用户来说，应用了“全部”访问控制的视图可能具有无法预见和可能不良的后果。有关“全部”访问控制的信息，请参阅第 191 页的“关于全部访问控制”。

为人员分配职责

您可以将职责添加到“人员”、“用户”、“雇员”或“合作者”记录中。以下过程介绍了如何将职责添加到人员记录中。您可以在“管理 - 用户”屏幕的“用户”列表或“雇员”列表中分配职责。

如果个人没有当前职责，该过程会将“人员”升级到“用户”。如果个人至少具有一个职责，则他（她）已经是“用户”、“雇员”或“合作者”。同样，个人的记录也会出现在“人员”列表中，因此，该过程适用于任何方案。

要为人员分配职责

- 1 以管理员身份登录到 Siebel 雇员应用程序。
- 2 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 用户”>“人员”。
此时将显示“人员”列表。
- 3 选择人员记录。

- 4 在此表单中，单击“职责”字段的选择按钮。

此时将显示分配给该人员的职责列表。

- 5 在“职责”列表中，单击“新建”。

此时将显示可分配的职责列表。

- 6 选择一个或多个职责，然后单击“确定”。

选定的职责出现在该人员的职责列表中。

- 7 单击“确定”。

- 8 保存记录。

如果要将同一个职责分配给多位用户，则可以改为通过“管理 - 应用程序”屏幕将这些用户添加到职责中。

业务组件视图模式

业务组件的视图模式决定了可应用于任何视图中业务组件的所允许的访问控制机制。如果视图以特定的业务组件为基础，该视图必须使用为此业务组件指定的视图模式之一。例如，“客户”业务组件只能用于组织视图模式或销售代表视图模式。

每个视图模式还决定了数据如何与用户关联以确定用户是否获得访问权限。例如，允许个人访问控制的业务组件通过将数据的“所有者 ID”字段与人员的用户 ID 相比较，将数据与人员连接。另一个业务组件可能通过数据的“创建者”字段应用个人访问控制。

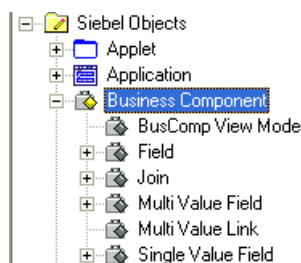
您可以使用 Siebel Tools 来处理业务组件的属性。

注释：如果业务组件没有列出的视图模式，在基于该业务组件的视图中则不存在基于该业务组件的访问控制。

要查看业务组件的视图模式和可视性字段

- 1 启动 Siebel Tools。
- 2 在“对象浏览器”中，单击 +（加号）以展开“业务组件”对象类型。

此时将显示业务组件子树，如下所示。



3 单击“业务组件视图模式”图标。

此时将显示“业务组件”列表及其“业务组件视图模式”明细列表，如下所示。

Business Components					
W	Name	Changed	Project	Cache Data	Class
	Access Group		Access Group		CSSBCGroup
	Access Group Member		Access Group		CSSBCBase
▶	Account		Account		CSSBCBase
	Account (Delegated Admin)		Admin		CSSBCUser
	Account Attachment		Account		CSSBCFile

BusComp View Modes				
W	Name	Changed	Owner Type	Private Field
▶	Organization		Organization	
	Sales Rep		Position	

4 在“业务组件”列表中，选择在“业务组件视图模式”列表中存在记录的业务组件。

“业务组件视图模式”列表中的记录表示业务组件可以假设的一个视图模式。

业务组件视图模式字段

Siebel Tools 的“业务组件视图模式”列表中的以下字段决定了业务组件允许的可视性。

■ **所有者类型。**该字段指定了用于确定用户是否与记录关联的当事方类型，但存在一个例外（以下列表中有说明）。允许的所有者类型包括：

- **人员。**访问控制以用户的人员记录为基础。
- **职位。**访问控制以用户的职位为基础。
- **组织。**访问控制以用户的组织为基础，这一点由用户当前职位所属的组织确定。
- **组。**访问控制以有权访问特定目录和类别的访问组中的成员资格为基础。
- **目录类别。**目录类别不是当事方类型。可将访问限定为跨目录的所有类别中的所有数据，这些目录是指用户有权访问的目录。这些数据包括公共类别中的数据和用户的访问组有权访问的私有类别中的数据。用户可看到数据平面列表（未分类）。

例如，客户业务组件的销售代表视图模式根据用户的职位确定用户与记录的关联。服务请求业务组件的个人视图模式根据用户的人员记录确定用户与记录的关联。

■ **私有字段。**该标志确定记录是私有还是公共。如果不是私有，则显示记录，而不考虑其视图模式。如果设置为私有，则应用由业务组件的“可视性”字段或“可视性 MVField”指定的访问控制。这适用于所有视图模式。

■ **可视性字段。**要求为“可视性”字段或“可视性 MVField”提供值。该字段中的值将与该用户的相应值（在“所有者”类型中指定）进行比较，以确定用户是否与记录关联。如果关联，用户就可以获得此记录的访问权限。

该字段中的值表示在使用此视图模式时只有一个当事方与该业务组件关联。

例如，服务请求业务组件的个人视图模式通过将用户的登录 ID 与“联系人 ID”字段中的值进行比较，确定用户是否与记录关联。

在使用此视图模式时，只有一位用户可以与该记录关联。通常，该用户是服务请求的创建者。

- **可视性 MVField（或多值字段）。**该字段的作用与“可视性”字段相同，不同之处在于，该字段中的值表示在使用此视图模式时可以有多个当事方与该业务组件关联。

例如，客户业务组件的销售代表视图模式通过将用户的职位与“销售代表”字段中的值进行比较，确定用户是否与记录关联。

如果使用此视图模式，则可以将多个职位与记录关联。在一些子视图中，“销售代表”字段具有类似于“客户团队”的显示名称，以表明有多个职位与记录关联。

- **可视性 MVLink（或多值链接）。**如果“可视性 MVField”中包含值，则要求在该字段中输入值。

该字段用于指定应该使用哪一个业务组件多值链接来为该记录确定 MVField 的值。

链接用于建立业务组件之间的父子关系，通常通过指定交集表（如果是多对多关系）来确定。该多值链接的“目标链接”属性表明哪一个链接最终定义此关系。

要在 Siebel Tools 中看到业务组件的多值链接及其属性，请在“对象浏览器”中展开“业务组件”对象，然后单击“多值链接”。“目标链接”属性是每个记录中的一个字段。

例如，客户业务组件的销售代表视图模式将“职位”作为其 MVLink。该多值链接的“目标链接”属性指定此关系使用客户/职位链接。正如在 Siebel tools 中的链接对象类型列表中所看到的，该链接使用 S_ACCNT_POSTN 交集表来查找与客户关联的职位。

- **名称。**该名称通常建议此视图模式。

例如，名称为“组织”的视图模式的所有者类型通常为“组织”。然而，唯一要求是业务组件的视图模式记录必须具有唯一的名称。例如，业务组件不能有两个名为“个人”的视图模式。

- **个人。**此名称通常在所有者类型为“人员”时使用。
- **销售代表。**此名称通常在所有者类型为“职位”时使用。
- **组织。**此名称通常在所有者类型为“组织”时使用。
- **组。**此名称通常在所有者类型为“组”时使用。
- **目录。**此名称通常在所有者类型为“目录”时使用。

例如，客户业务组件的销售代表视图模式根据用户的职位确定用户与记录的关联。

这一典型命名惯例也存在例外，服务请求业务组件就是该例外的一个示例。

个人和销售代表视图模式的所有者类型均为“人员”，一个表示所有者是“联系人 ID”，另一个表示所有者是“所有者 ID”。由于创建者和客户服务座席都需要访问基于人员的数据，因此需要提供这两种视图模式。

有关处理业务组件的信息，请参阅 *Configuring Siebel eBusiness Applications*。

子视图访问控制属性

视图表示一个同时出现的列表、表单和结构树的集合，如第 206 页的图 12 中所示（“组织图”视图）。这些列表和表单在配置上下文中称为子视图。

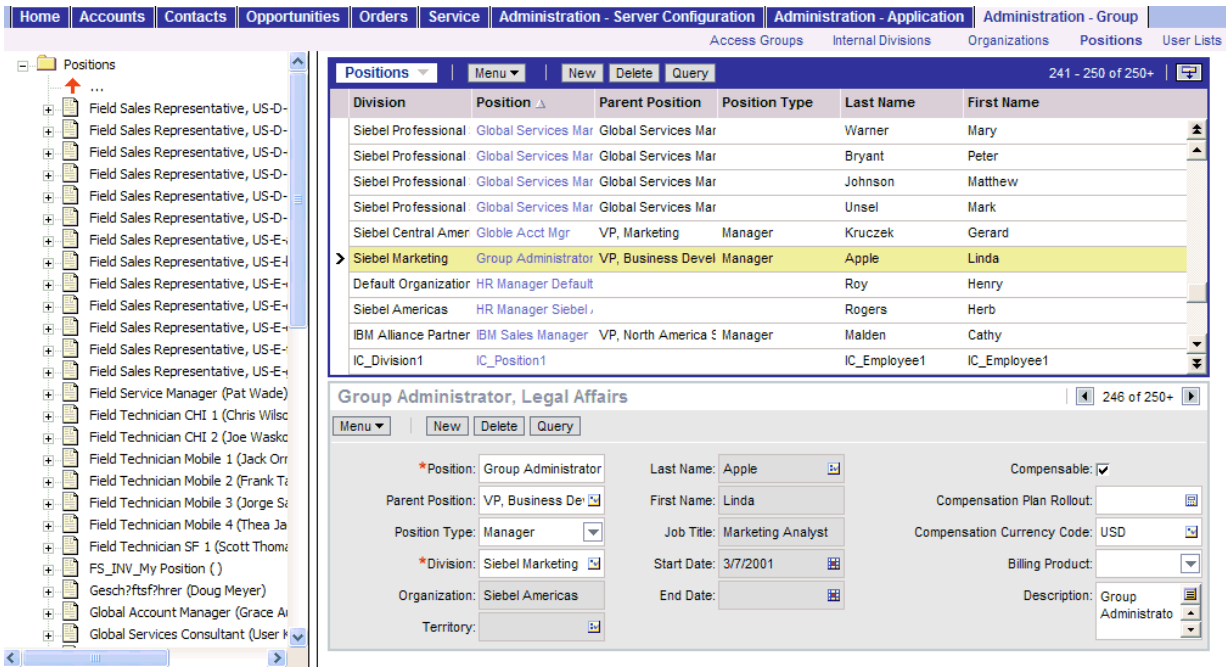


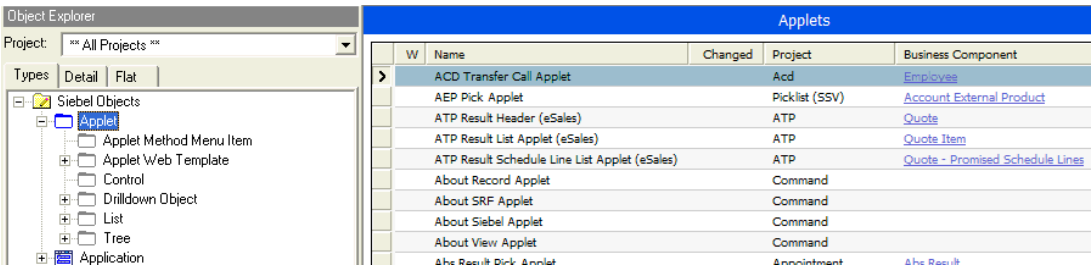
图 12. Siebel 应用程序中的子视图示例

子视图在不同的视图中可重复使用，并且在不同的视图中可以应用不同的访问控制属性。如果专门为视图定义了可视性，则视图中的其中一个子视图被指定为可视性子视图。可视性子视图的几项属性决定了视图中数据的访问控制。

您可以使用 Siebel Tools 处理子视图及其属性。有关详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

要查看子视图的属性

- 1 启动 Siebel Tools。
- 2 在“对象浏览器”中，单击 + 号展开子视图对象类型。
此时将显示子视图子树。同时还显示子视图列表，如下所示。



- 3 要查看特定子视图属性，请单击其子组件的图标，或者单击 + 号展开子组件的子树，然后单击其子组件。
该子组件的明细列表显示在“子视图”列表下面。有两个子视图属性对数据可视性起了很大作用：业务组件和显示名称。
如下所示，“业务组件”字段指定子视图所基于的业务组件。例如，“客户列表”子视图使用“客户”业务组件。

Applets				
W	Name	Changed	Project	Business Component
	Account Form Applet - Short		Account (SSE)	Account
	Account Form ReadOnly Applet		Account (SSE)	Account
	Account List Applet		Account (SSE)	Account
	Account List Applet (Delegated Admin)		Admin	Account (Delegated Admin)

4 在“对象浏览器”中，选择“子视图”>“列表”>“列表列”。

如第 208 页的图 13 中所示，“列表列”列表显示该子视图将显示的业务组件字段。对于每个业务组件字段，伴随的“属性”列表中的“显示名称”项表示该字段如何在子视图中标记。

例如，“客户”业务组件可以使用“销售代表”或“组织”字段确定用户与记录的关联。了解这些字段在“客户列表”子视图中的显示方式将很有用。“组织”字段在子视图中的显示名称是“组织”，但是，“销售代表”字段的显示名称是“客户团队”。

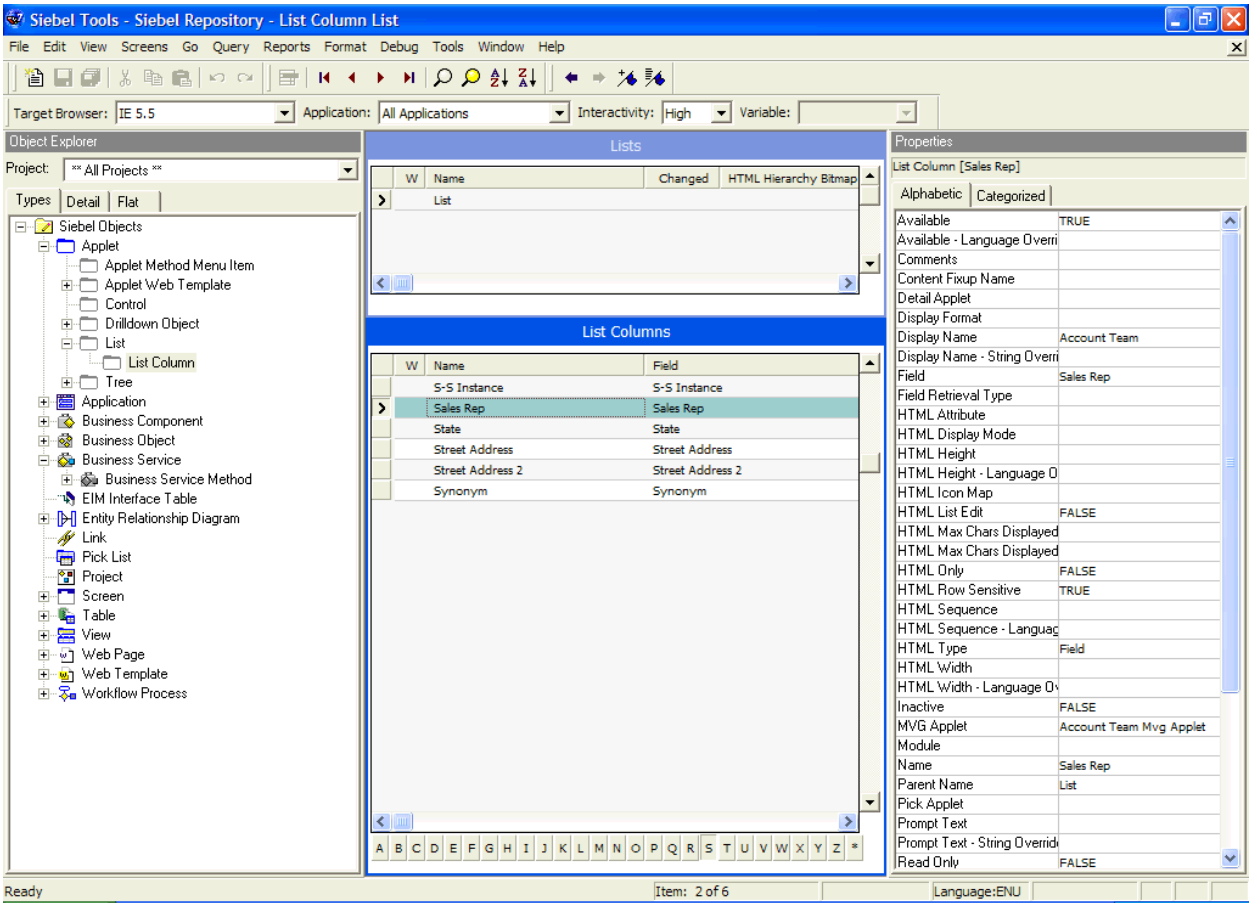


图 13. 子视图的列表和列表列

视图访问控制属性

视图的访问控制属性确定了使用哪些子视图操纵可视性，以及将哪些访问控制机制应用于视图所基于的业务组件。您可以使用 Siebel Tools 来处理视图的属性。

要查看视图的访问控制属性

- 1 启动 Siebel Tools。
- 2 在“对象浏览器”中，单击“视图”对象类型。

此时将显示“视图”列表，如下图所示。该列表的字段包括那些影响可视性的字段。

Views				
W	Name	Change	Project	Admin
>	Access Group Explorer View	✓	Access Group	
	Access Group Member List View		Access Group	
	Account (SCW) Preview View		Account (SCW)	
	Account - Back Office Account Relationship View		Account	
	Account - Oracle 10.7 List View		Oracle Account 10.7	
	Account - Oracle 11i List View		Oracle Account 11i	
	Account - SAP Orders View		SAP Account	
	Account - SAP Orders View (MO)		SAP Account	

“视图”列表中的以下字段有助于确定数据的可视性。

- **标题。**标题是指为用户界面中的视图提供的名称。它应该间接地表示视图数据的访问控制级别。例如，“我的客户”间接地表示它的可视性比“我的团队的客户”限制更严格。
- **可视性子视图。**通常，这是指主要 - 明细子视图关系中的主项目。该子视图定义了视图所基于的业务组件以及业务组件字段的显示方式。

如果在视图中定义了视图属性“可视性子视图”，该视图将被视为与其自身关联，即独立的可视性。Siebel 应用程序将在您选择该视图时，根据“可视性子视图类型”（缺省的“可视性子视图类型”是“全部”）重新查询该视图。

注释：请勿在明细视图中指定“可视性子视图”属性，在明细视图中当前记录上下文和当前查询应该保留。

- 如果视图不是来源于另一个视图，则该字段中应该具有值。例如，在任何屏幕的链接栏中列出的视图都具有可视性子视图，但是通过从另一个视图向下搜索产生的视图却没有可视性子视图。没有可视性子视图的视图通常从来源视图中继承访问控制属性。
- 多个视图可能具有相同的可视性子视图。例如，“全部客户列表”视图和“经理的客户列表”视图都将客户列表子视图作为其可视性子视图。
- **可视性子视图类型。**此字段确定应用于该视图的访问控制机制。它指定将应用业务组件的哪个视图模式以及如何应用。以下是该字段的选取列表中的可用选择：
 - **全部。**此类型的视图应用全部访问控制。
用户可以访问所有记录，但缺少所有者或所有者无效的记录除外。
 - **个人。**此类型的视图应用个人访问控制。
用户可以访问与其人员记录关联的记录，这一点由业务组件的“可视性”字段决定。
要使用该可视性子视图类型，业务组件必须具有其所有者类型为“人员”的视图模式。
 - **销售代表。**此类型的视图应用单一职位或团队访问控制。
用户可以访问由其职位拥有的记录，也可以访问团队包含其职位的记录，这一点由业务组件的“可视性”字段或“可视性 MVField”决定。
要使用该可视性子视图类型，业务组件必须具有所有者类型为“职位”的视图模式。

■ **经理。**此类型的视图应用经理访问控制。

用户可以访问与其职位、其直属下司职位以及其直属下司的下属职位关联的记录。尤其是用户有权访问以下数据：

- 如果视图所基于的业务组件使用单一职位访问控制，用户则看到直接与其活动职位关联或与下属职位关联的数据。
- 如果视图所基于的业务组件使用团队访问控制，用户则看到其活动职位是该团队的主要职位或下属职位是该团队的主要成员的数据。

要使用该可视性子视图类型，业务组件也可以具有所有者类型为“职位”的视图模式。

■ **组织。**此类型的视图应用单一组织或多组织访问控制，这一点由业务组件的“可视性”字段或“可视性 MVField”决定。

用户可以访问与组织关联、而该组织又与用户职位关联的记录。

要使用该可视性子视图类型，业务组件必须具有其所有者类型为“组织”的视图模式。

■ **子组织。**此类型的视图应用子组织访问控制。用户有权访问以下数据：

- 如果视图所基于的业务组件使用单一组织访问控制，用户则看到直接与其活动组织或后代组织关联的数据。
- 如果视图所基于的业务组件使用多组织访问控制，用户则看到其活动组织或后代组织是主要组织的数据。

后代组织由组织结构定义。要使用该可视性子视图类型，业务组件必须具有其所有者类型为“组织”的视图模式。

■ **组。**此类型的视图应用组访问控制，它是一种访问组访问控制的机制。如果在当前会话期间，用户与作为某个访问组成员的职位、组织、客户、家庭或用户列表关联，用户则与该访问组关联。

用户可以访问与其中任何访问组关联、而该访问组又与此用户关联的主数据类别。在提供可导航树的视图中，用户则看到当前类别中可访问的第一级子类别。在提供主数据记录列表的视图中，用户则看到当前（已访问）类别中的所有记录。

要使用该可视性子视图类型，业务组件必须具有其所有者类型为“组”的视图模式。

■ **目录。**该视图应用目录访问控制，它是一种访问组访问控制的机制。如果在当前会话期间，用户与作为某个访问组成员的职位、组织、部门、客户、家庭或用户列表关联，用户则与该访问组关联。

用户则看到跨目录的所有类别中所有数据的平面（未分类）列表，这些目录是指此用户的所有访问组有权访问的目录。该可视性类型通常用于产品选取列表和其它产品列表。

要使用该可视性子视图类型，业务组件必须具有其所有者类型为“目录类别”的视图模式。

注释：尽管将可视性类型设置为“目录”，您仍可以看到产品选取列表和其它产品列表中的其它产品。对于属于公共目录的产品，这是预料之中的行为。

- **管理模式。**该属性的值必须为 TRUE 或 FALSE。如果值为 TRUE，该视图在管理模式下工作。如果视图采用管理模式，对该视图的子视图使用的业务组件进行的所有插入、删除、合并和更新限制均被忽略（包括按以下业务组件用户属性指定的那些限制：未插入、未删除、未合并和未更新）。

管理模式视图的示例包括“客户管理”视图、“商机管理”视图和“产品管理”视图。

管理模式不会覆盖弹出可视性。它不会覆盖对业务组件中字段的只读限制。

在管理模式下，采用团队访问控制的视图中的每个记录都是可视的，甚至包括那些未指定主要职位的记录。（该模式不同于全部可视性，后者显示指定了主要团队成员的所有记录。）

警告：使用管理模式的视图供管理员访问，并且通常包括在管理屏幕中由类似视图组成的分组中，例如“管理 - 应用程序”。如果某个屏幕包含未设置为管理模式的视图，请勿将采用管理模式的视图包括在此屏幕中。如果用户将管理模式的视图过渡到非管理模式的视图，目标视图将仍然停留在管理视图中，因此可能会暴露不打算显示的数据。

灵活构建视图示例

以下示例显示现有的多个视图是如何根据相同的可视性子视图和业务组件进行构建的。它间接地指明如何在 Siebel Tools 中构建类似视图“系列”，但是未提供建立视图的过程。更改 Siebel Tools 中的任何设置都需要重新编译 Siebel 库文件 (SRF)。

有关使用 Siebel Tools 时所需惯例的详细信息，请参阅 *Configuring Siebel eBusiness Applications*。

第 211 页的图 14 显示了 Siebel Tools 中客户业务组件的“业务组件视图模式”列表。如“所有者类型”字段所示，允许使用组织和职位视图模式。如“可视性 MVField”所示，客户可以与多个组织和多个职位关联（例如，销售团队）。

BusComp View Modes						
	Name	Changed	Owner Type	Private Field	Visibility Field	Visibility MVField
Organization	Organization		Organization		Organization	Organization
Sales Rep	Position		Position		Sales Rep	Position

图 14. 客户业务组件视图模式

第 211 页的图 15 显示了 Siebel Tools 的“视图”列表中的 5 个视图。“标题”字段显示了该视图的显示名称。所有的 5 个视图都将客户列表子视图作为其可视性子视图。客户列表子视图以客户业务组件为基础。

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

图 15. 以客户业务组件为基础的示例视图

这 5 个示例视图提供了不同的客户数据列表，因为它们具有所指定的不同可视性子视图类型，如第 212 页的表 23 所示。

表 23. 客户视图和可视性子视图类型示例

视图	可视性子视图类型	数据访问
客户列表视图（显示为“我的客户”）	销售代表	团队访问控制适用。此可视性子视图类型适用于可关联多个职位的业务组件。 对于该视图，将授予对符合以下条件的客户数据的访问权限：用户职位在客户团队中。
经理的客户列表视图（显示为“团队的客户”）	经理	经理访问控制适用。此可视性子视图类型适用于可关联多个职位的业务组件。 对于该视图，将授予对符合以下条件的客户数据的访问权限：用户的活动职位或下属职位是客户团队的主要职位。
全部客户列表视图（显示为“全部客户”）	组织	组织访问控制适用。此可视性子视图类型适用于可关联多个组织的业务组件。 对于该视图，将授予对符合以下条件的客户数据的访问权限：用户的主要组织是与此客户关联的其中一个组织。
跨我的组织的所有客户	子组织	子组织访问控制适用。此可视性子视图类型适用于可关联多个组织的业务组件。 对于该视图，将授予对符合以下条件的客户数据的访问权限：用户的活动组织或后代组织是主要组织。
跨组织的所有客户	全部	全部访问控制适用。客户业务组件只具有职位和组织视图模式。 对于该视图，将授予对符合以下条件的所有客户数据的访问权限：客户团队中存在一个主要职位或存在一个与此客户关联的组织。

实施访问组访问控制

您可以将访问组与主数据的目录或类别关联。如果访问组与目录或类别关联，与访问组关联的用户则可以看到此目录或类别中的数据。

以下原则适用于访问组访问控制。以下上下文中的访问组是访问组结构中的一个单个节点：

- **私有目录和类别。**一个目录是一个类别结构。目录本身不能包含数据。要对目录的所有类别应用访问组访问控制，您必须将该目录指定为私有目录，然后将访问组与目录关联。如果目录不是私有，则任何用户都可以看到其类别中的数据。您可以将公共目录中的单个类别指定为私有。
- **访问组访问被继承。**如果访问组与类别关联，则该组的后代组（子组，孙组等等）将自动与此类别关联。反之，如果访问组与类别断开关联，则其后代组也会断开关联。继承关联将在运行时强制执行。

■ **级联类别可视性可选。**

- 如果访问组与类别关联，使用“级联”按钮则可以让访问组与该类别的后代类别（子类别，孙类别等等）自动关联。因此，与访问组关联的用户有权访问其后代类别中的数据。
- 如果访问组与类别断开关联，此访问组将自动与该类别的后代类别断开关联。如果访问组与其中一个后代类别断开关联，则访问组的级联可视性只能向上传到该后代类别（但不包括该后代类别）。
- 一旦设置了“级联”按钮，级联访问只能通过从类别断开关联访问组来进行禁用。不能对此标志本身取消设置。
- 如果未使用“级联”按钮，访问权限限定为与访问组关联的单个类别。

应用访问组访问控制的方案

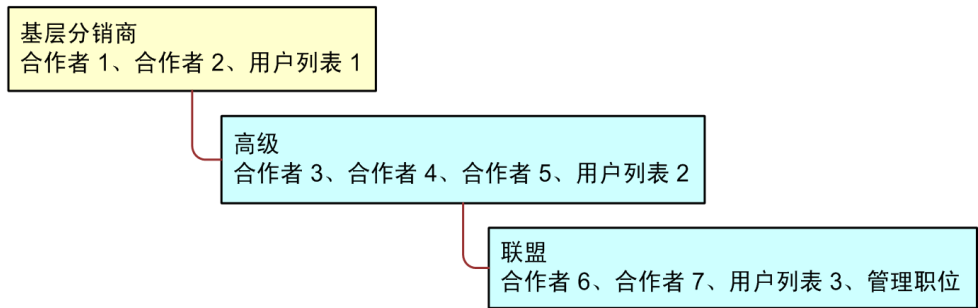
假设您需要知道分销商的状态，以确定他们有权访问哪些知识资源。您的分销商包括合作者组织以及一些未与合作者组织关联的个人顾问。

您的解决方案必须满足以下要求：

- 为基层分销商提供访问基本产品信息资源的权限 — 服务常见问题、产品文档和产品培训课程。
- 除基本产品信息之外，为“高级”分销商提供访问更多特定于销售的资源的权限 — 市场营销常见问题、用于提供解决客户决策问题指导的文档以及销售培训课程。
- 除产品和销售资源之外，为联盟分销商提供访问有助于设计整个市场活动的资源的权限 — 竞争情况简报和培训课程。
- 由于分销商的状态在变化，因此必须尽量减轻更改分销商对数据的访问权限所需的管理工作。

第 214 页的图 16 图示了一个解决此业务问题的访问控制结构。

分销商团体



分销商资源目录

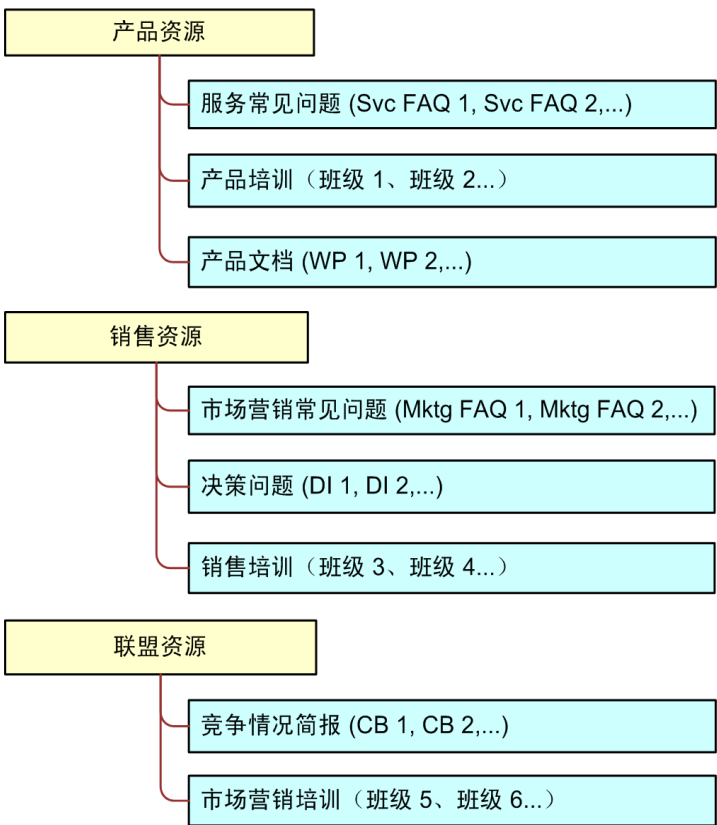


图 16. 分销商资源访问控制示例

该解决方案假设将合作者存储为组织，而在该组织中将合作者用户与职位关联。顾问作为用户存在；他们具有职责，但没有职位，并且与组织不关联。

分销商团体是一个访问组结构。每个节点都是一个访问组，其成员是合作者组织和单一用户列表。每个节点中的用户列表包含适当状态的所有顾问。为了让内部管理员具有目录的可视性，请将其职位包括在“联盟”访问组中。

“分销商资源”目录由包含数据的类别以及节点组成，节点是用于定义访问级别的空白类别。

采用以下原则构建该结构：

- 构建分销商团体，以便最高级别对资源的访问权限最窄。因此，基层分销商访问组是高级访问组的父项，而高级访问组又是联盟访问组的父项。
- 构建分销商资源目录，以便产品资源、销售资源和联盟资源节点是该目录中所有的第一级类别。
- 产品资源节点的子节点包括产品资源的类别。销售资源和联盟资源节点的子节点也按类似方式确定。

以下实施过程限制基层分销商只能访问产品资源，高级分销商可以访问产品资源和销售资源，而联盟经销商可以访问所有资源。

要实施分销商资源访问控制结构

- 1 构建分销商资源目录，将该目录指定为私有，并将访问权限提供给基层分销商访问组。
由于访问组访问被继承，因此高级和联盟访问组也被授予对此目录的访问权限。
- 2 将基层分销商访问组与产品资源类别关联，并使用“级联”按钮。
高级和联盟访问组从基层分销商访问组继承访问权限，而且访问权限从产品资源类别级联到包含数据的子类别。结果是分销商团体中的所有节点都有权访问产品资源类别中的所有子类别。
- 3 将高级访问组与销售资源类别关联，并使用“级联”按钮。
联盟访问组从高级访问组继承访问权限，而且访问权限从销售资源类别级联到包含数据的子类别。结果是高级和联盟访问组有权访问销售资源类别中的所有子类别。
- 4 将联盟访问组与销售资源类别关联，并使用“级联”按钮。
没有访问组从联盟访问组继承访问权限。访问权限从联盟资源类别级联到其包含数据的子类别。结果是只有联盟访问组有权访问联盟资源类别中的子类别。
- 5 将目录的类型设置为“合作者”，使合作者和顾问可以在合作者应用程序（例如 Siebel Partner Portal）中看到此目录，并且使内部管理员可以在 Siebel 雇员应用程序的“信息中心”屏幕中看到此目录。

该结构符合最低维护需求的要求。如果合作者组织的状态发生变化，请将合作者组织添加适当的访问组中，并且从旧访问组中删除此合作者组织。如果顾问的状态发生变化，请将此用户添加到适当的用户列表中，并且从旧用户列表中删除此用户。重新分类的顾问和合作者用户可以获得由结构规定的适当的新访问权限。

类型相同的销售工具（例如，常见问题或产品文档）位于各自的类别中。

有关以下项的信息：

- 创建和管理目录，请参阅 *Siebel eSales Administration Guide*。
- 创建和管理用户列表以及访问组，请参阅第 212 页的“实施访问组访问控制”。

用户的体验

您可以将目录配置为作为一项缺省功能显示在 Siebel 雇员应用程序和选定的客户及合作者应用程序（例如，Siebel eSales 和 Siebel Partner Portal）中。

在雇员应用程序中（例如 Siebel Call Center），用户可以在“信息中心”和“信息中心浏览器”屏幕中看到由访问组成员资格控制的分类数据。

如第 216 页的图 17 所示，“信息中心浏览器”提供了树形界面，用于浏览所有目录以导航到用户有权访问的目录，并向下一级导航到数据项目级别。

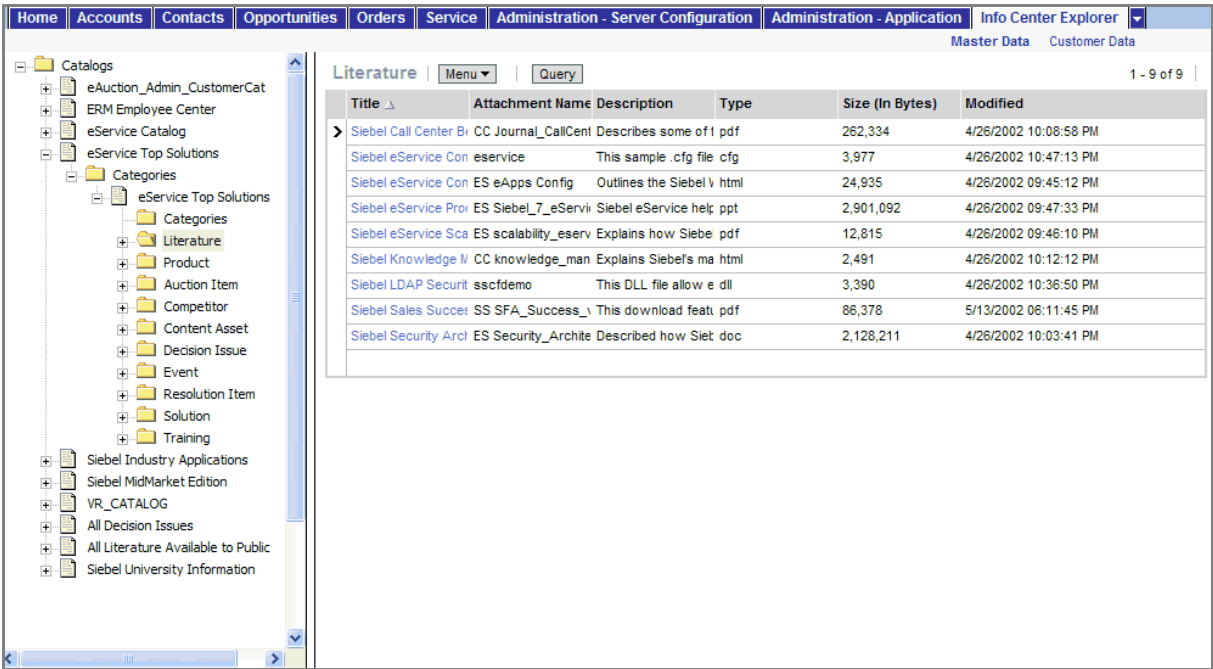


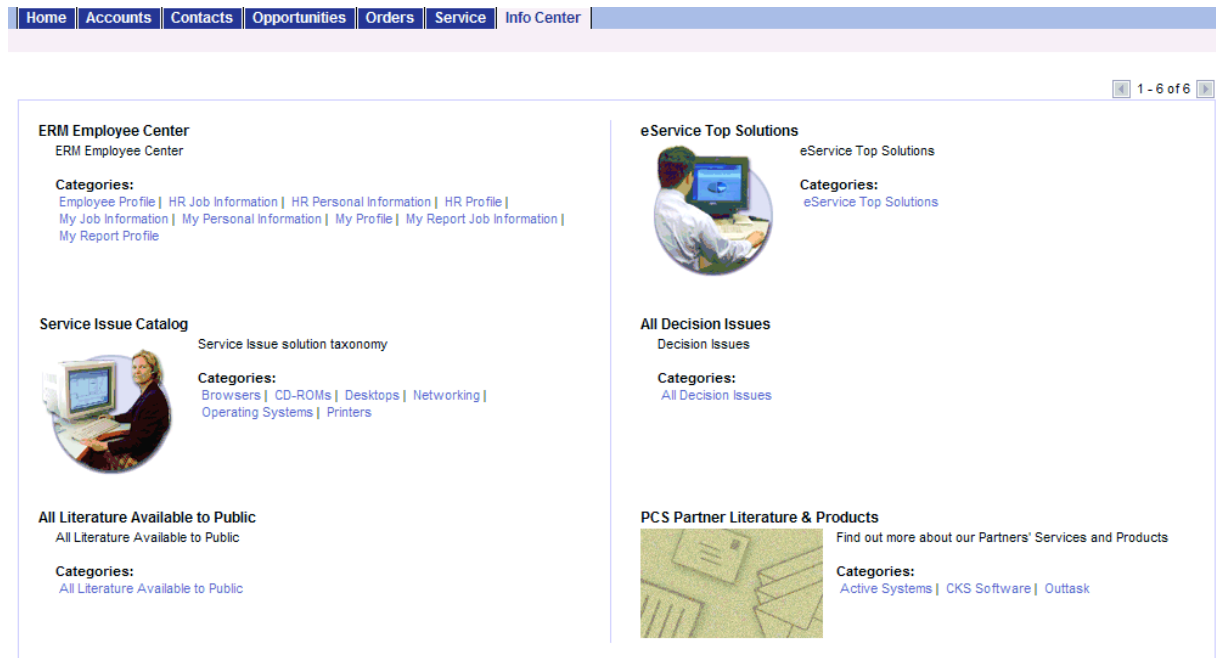
图 17. 信息中心浏览器

与“信息中心浏览器”相比，“信息中心”显示的是如何使用丰富及更开放的用户界面，在 Siebel 应用程序中展示分类数据。

要在信息中心查看分类数据

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “信息中心”。

此时将显示“信息中心”屏幕，如下图所示。它显示了可访问的目录及其第一级类别。



- 2 单击“类别”链接。例如，您可能选择“决策问题”。

如下所示，将显示类别，并显示其数据项以及第一级子类别。

Views Decision Issue Literature	<div> All Decision Issues </div> <div> SubCategories </div> <div> Decision Issues </div> <div> <input type="text" value="Query"/> 1 - 10 of 10+ </div> <table border="1"> <thead> <tr> <th>Name</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Ensuring Sufficient Memory</td><td></td></tr> <tr> <td>Installation</td><td></td></tr> <tr> <td>Network</td><td>Network Support</td></tr> <tr> <td>Performance</td><td>Total performance</td></tr> <tr> <td>Priced within budget</td><td></td></tr> <tr> <td>Service response time of less than 2 hours</td><td></td></tr> <tr> <td>Symmetric Processing</td><td></td></tr> <tr> <td>System Ease of Use</td><td></td></tr> <tr> <td>Upgrade</td><td>General Upgrade Assistance</td></tr> <tr> <td>Upgrading Operating System</td><td></td></tr> </tbody> </table>	Name	Description	Ensuring Sufficient Memory		Installation		Network	Network Support	Performance	Total performance	Priced within budget		Service response time of less than 2 hours		Symmetric Processing		System Ease of Use		Upgrade	General Upgrade Assistance	Upgrading Operating System	
Name	Description																						
Ensuring Sufficient Memory																							
Installation																							
Network	Network Support																						
Performance	Total performance																						
Priced within budget																							
Service response time of less than 2 hours																							
Symmetric Processing																							
System Ease of Use																							
Upgrade	General Upgrade Assistance																						
Upgrading Operating System																							

- 3 单击某个数据项进行查看，或向下搜索到子类别链接以查看其内容。

管理任务

访问组访问控制要求您执行以下任务：

- 管理主数据目录 — 根据需要建立目录和类别、关联数据以及修改目录结构。
- 管理作为访问组成员的当事方类型 — 职位、组织、家庭和用户列表。
- 管理访问组 — 根据需要建立访问组并修改其结构。
- 将访问组与数据的目录和类别关联。

管理数据目录

您可以在“管理 - 目录”屏幕中执行以下目录和类别的管理任务：

- 创建和删除主数据的目录和类别。
- 将数据与类别关联。
- 修改目录中类别的分层职位。

设置目录的主要原则包括但不限于：

- 设置“目录类型”字段，以便除了在 Siebel 雇员应用程序的“信息中心”和“信息中心浏览器”中，还允许在某些 Siebel 客户或合作者应用程序中显示目录。例如，将“目录类型”设置为“合作者”，以便在 Siebel Partner Portal 以及“信息中心”中显示目录。
- 确保设置了“活动”标志，并且“有效开始日期”和“有效结束日期”字段提供了所需时间间隔期间的目录可视性。

有关创建和管理目录的信息，请参阅 *Siebel eSales Administration Guide* 和 *Siebel Partner Relationship Management Administration Guide*。

管理职位、组织、家庭和用户列表

访问组由职位、组织、家庭和用户列表组成。

管理职位

您必须执行以下职位管理任务：

- 创建职位。
- 将职位与雇员和合作者用户关联。
- 维护职位结构。

管理组织

“组织”组类型包括组织、部门和客户。您必须执行以下组织管理任务：

- 创建部门和客户。
- 将部门提升为组织。
- 维护部门结构。
- 将职位与部门和合作者组织关联。

管理家庭

您必须执行以下家庭管理任务：

- 创建家庭。
- 将联系人与家庭关联。
- 维护家庭数据。

有关管理家庭的信息，请参阅[应用程序管理指南](#)。

管理用户列表

您可以将任意用户组成用户列表，以便通过访问组为其授予对数据的访问权限。此上下文中的用户包括联系人用户、雇员和合作者用户。

有关用户列表的信息，请参阅[第 181 页的“当事方的访问控制”](#)。

创建用户列表

您可以在“管理 - 组”屏幕中创建用户列表。

要创建用户列表

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 组” > “用户列表”。
此时将显示“用户列表”列表。
- 2 在“用户列表”列表中添加新记录。
此时将显示新用户列表记录。
- 3 输入用户列表的名称。您可以根据需要更改组类型的缺省录入。
- 4 保存记录。

修改用户列表

您可以通过添加或删除用户来修改用户列表。

要将用户添加到用户列表中

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 组”>“用户列表”。

此时将显示“用户列表”列表。

- 2 在“用户列表”列表选择一个用户列表。

- 3 在视图底部的“用户”列表中，添加一个新记录。

- 4 选择一位或多位用户，然后单击“确定”。

选定的用户将显示在“用户”列表中。如果用户（例如客户用户）属于某个客户，该“客户”字段将自动填入值。

您可以按此类似方式从用户列表中删除用户。

管理访问组

您可以将类型为“职位”、“组织”、“家庭”和“用户列表”的当事方组成访问组，以便控制其个人成员对数据的访问。

您可以通过选择“导航”>“场地图”>“管理 - 组”>“访问组”，在“管理 - 组”屏幕中管理访问组。该屏幕包含访问组树和访问组列表。

访问组树在树的第二级中列出所有访问组。每个访问组都可以展开以显示其后代访问组。因此，访问组可能出现在此树多个分支的不同级别中。

无父访问组的访问组是访问组结构中的顶部节点。

有关访问组的信息，请参阅第 181 页的“当事方的访问控制”和第 191 页的“关于访问组访问控制”。

创建访问组

您可以在“管理 - 组”屏幕中创建访问组。

要创建访问组

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 组”>“访问组”。

此时将显示访问组树和访问组列表。

- 2 在“访问组”列表中添加新记录。

一个新的访问组记录。

- 3** 填写以下字段，然后保存记录。请使用以下准则。

字段	准则
名称	必需。为访问组提供名称。
组类型	选择访问组或合作者团体。这些标签显示的是概念上的差异。从功能上来看，它们是相同的。
父访问组	指定一个父访问组，如果该父访问组有权访问某个数据，此新组将从父访问组继承对此数据的访问权限。

新访问组还会显示在访问组树中。

修改访问组

您可以通过添加或删除成员来修改访问组。

要将成员添加到访问组中

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 组” > “访问组”。
此时将显示“访问组”列表。
 - 2 在“访问组”列表中选择访问组。
 - 3 在“成员”列表中添加新记录。
此时将显示一个弹出列表，其中包含职位、组织、客户、家庭和用户列表。
 - 4 选择一位或多位成员，然后单击“确定”。
所选成员将显示在“成员”列表中。
 - 5 在“访问组”列表中保存记录。
- 您可以按此类似方式从访问组中删除成员。

修改访问组结构

您可以通过更改访问组的父项来修改访问组的结构。

要修改访问组的结构

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 组” > “访问组”。
此时将显示“访问组”列表。
- 2 在“访问组”列表中选择访问组。

3 单击“父访问组”字段。

文本框变为可编辑，并且输入的内容被高亮度显示。

4 请执行以下操作之一以修改此结构：

- 要使访问组成为其自身结构的顶部节点，请删除“父访问组”字段中的录入值。单击“保存”。
- 从“父访问组”字段中选择新父访问组，并单击“确定”。单击“保存”。

访问组树将被更新，以反映访问组在此结构中的新职位。

将访问组与数据关联

您可以通过将访问组与数据的目录或类别关联，为访问组中的个人用户提供对数据的访问权限。

请了解以下用户界面行为，这些行为与将访问组与目录或类别的关联相关：

- **继承访问。**如果您将访问组与类别关联，其后代访问组也与此类别关联。然而，此继承是在运行时实施，并不表现在数据库中。同样，与此类别关联的后代访问组不会显示在与此类别关联的访问组列表中。
- **级联按钮。**单击“级联”按钮可以为给定访问组提供对当前目录或类别中所有子类别的可视性。重复单击该按钮不起作用。您必须手动断开组与子类别的关联，以撤消访问级联。
- **私有目录。**如果将某个目录指定为私有，该目录的所有类别也会设置为私有。如果您在目录级别删除私有设置，此类别仍为私有。然后您必须单独设置或删除类别的私有设置。

将访问组与目录关联

通过将访问组与主数据的目录关联，您可以为访问组中的个人用户授予对此目录中数据的访问权限。

注释：要使目录及其所有子类别仅对与其关联的访问组可视，则必须设置目录的“私有”标志。

要将访问组与目录关联

1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 目录”>“访问组”。

此时将显示“目录”列表。

2 选择一个目录。**3** 在“访问组”列表中添加新记录。

此时将显示一个弹出列表，其中包含访问组。

4 选择访问组，然后单击“添加”。

此访问组将显示在“访问组”列表中。

5 在“访问组”列表中保存记录。**6** 选择访问组，然后单击“添加”。

此访问组将显示在“访问组”选项卡下面。

- 7 填写以下字段，然后保存记录。请使用下面提供的准则。

字段	准则
管理	设置该标志，以允许该访问组中的用户管理目录。
级联	设置该标志，以自动将该访问组与目录的后代类别（子类别、孙类别等等）关联。结果是该访问组中的用户有权访问后代类别中的数据。

您可以按此类似方式断开访问组与目录的关联。

将访问组与类别关联

通过将访问组与主数据的类别关联，您可以为访问组中的个人用户授予对此类别中数据的访问权限。

注释：要使类别及其所有子类别仅对与其关联的访问组可视，则必须设置类别的“私有”标志，或者必须设置作为此类别祖先的目录或类别的“私有”标志。

要将访问组与类别关联

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 目录” > “访问组”。

此时将显示“目录”列表。

- 2 向下搜索到目录名称。

此时将显示目录的类别列表。

- 3 单击“访问组”视图选项卡。

- 4 在“访问组”列表中添加新记录。

此时将出现一个列出了访问组的多值组。

- 5 选择访问组，然后单击“添加”。

此访问组将显示在“访问组”列表中。

- 6 在“访问组”列表中保存记录。

- 7 选择访问组，然后单击“添加”。

此访问组将显示在“访问组”选项卡下面。

- 8 填写以下字段，然后保存记录。请使用下面提供的准则。

字段	准则
管理	设置该标志，以允许该访问组中的用户管理此类别。
级联	设置该标志，以自动将该访问组与此类别的后代类别（子类别、孙类别等等）关联。结果是该访问组中的用户有权访问后代类别中的数据。

您可以按此类似方式断开访问组与目录的关联。如果断开访问组与类别的关联，系统会自动断开该访问组与此类别的所有后代类别的关联。

通过职责管理选项卡布局

Siebel 应用程序管理员可以管理特定于工作职能的缺省屏幕和视图选项卡布局。选项卡布局通过职责进行管理。

管理员可以使用“管理 - 应用程序”屏幕中的“职责”视图（“职责明细 - 选项卡布局”视图），为每个职责定义缺省的选项卡布局。管理员可以从该视图同时管理视图访问和缺省的选项卡布局。

为了减轻设置缺省选项卡布局以及将其与职责关联的管理负担，Siebel 应用程序附带了许多预定义的职责，并且为这些职责预配置了缺省的选项卡布局。

例如，Siebel Call Center 的 Universal Agent 职责具有与其关联的屏幕和视图访问以及缺省的选项卡布局。这些是具有该工作职能的用户最常用的视图。每当具有该职责的用户登录，他（她）就有权访问该职责适用的所有屏幕和视图，以及与该用户关联的所有其它职责适用的所有屏幕和视图。

然而，用户在该应用程序用户界面上看到的只是与用户的主要职责关联的简化的缺省屏幕和视图选项卡布局，例如，如果用户的主要职责是 Universal Agent，则只能看到与该职责关联的布局。

每位用户都可以使用“用户首选项”屏幕（“工具” > “用户首选项”）中的“选项卡布局”视图，修改个人选项卡布局设置。一旦用户修改了选项卡布局，这些设置将始终覆盖与此用户的主要职责关联的缺省选项卡布局。有关详细信息，请参阅[基础](#)。

如果用户从“场地图”中选择了不是选项卡布局一部分的屏幕，则会为该屏幕创建一个屏幕选项卡，而且该选项卡只适用于此会话。

管理选项卡布局

要管理选项卡布局，请导航至“管理 - 应用程序” > “职责”，然后单击“选项卡布局”视图选项卡。

“选项卡布局”视图（“职责明细 - 选项卡布局”视图）用于基本的选项卡布局管理任务，例如，为不同职责重新排序或隐藏屏幕和视图选项卡，以及用于导入和导出选项卡布局。请参阅第 225 页的[“导出和导入选项卡布局”](#)。

为了让您管理多个应用程序的屏幕和视图，选项卡布局管理使用四个列表：

- **职责列表。**包括库中的所有职责。
- **应用程序列表。**包括库中的所有 Siebel 应用程序，并且指定您要管理哪些应用程序的选项卡布局。
- **屏幕选项卡布局列表。**指定为每个应用程序显示哪些屏幕。
- **视图选项卡布局列表。**指定为每个屏幕显示哪些视图。

您必须选择一个应用程序，因为您要为其管理职责的应用程序可能不同于您以管理员身份登录的应用程序。例如，您使用 Siebel 合作者管理器为将使用 Siebel Partner Portal 的合作者管理职责。

要为职责指定选项卡布局

- 1 以管理员身份登录。
- 2 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 应用程序” > “职责”。
- 3 在“职责”列表中，选择要与选项卡布局关联的职责。
- 4 单击“选项卡布局”视图选项卡。
- 5 在“选项卡布局”列表中，选择与职责关联的应用程序。

- 6 “屏幕选项卡布局”列表显示了选定应用程序使用的所有屏幕：
 - a 对于将不显示屏幕选项卡的任何屏幕，请为该屏幕选择“隐藏”复选框。
 - b 更改“顺序”字段中的数值，以更改屏幕选项卡的显示顺序。
- 7 选择“屏幕选项卡布局”列表中的每个记录，“视图选项卡布局”列表将显示该屏幕的所有视图：
 - a 对于不显示视图选项卡的任何视图，请为该视图选择“隐藏”复选框。
 - b 更改“顺序”字段中的数值，以更改屏幕选项卡的显示顺序。

分配主要职责

要提供对所有必需视图的访问权限，每位用户可能被分配有多个职责。其中一个职责被定义为主要职责。用户将看到与他（她）的主要职责关联的选项卡布局。“场地图”向此用户提供了对在其关联职责中定义的屏幕和视图父集的访问权限。

管理员可以通过在“管理 - 用户”屏幕的“职责”对话框中核选“主要”标志，为用户设置主要职责。

注释：缺省情况下，分配给用户的第一个职责（以时间戳为准）成为主要职责。特别是对于要升级的客户，管理员应该验证已经将正确的主要职责分配给每位用户，或者已经指定所需的主要职责。

导出和导入选项卡布局

您可以导入和导出选项卡布局，以便将选项卡布局从一个职责复制到另一个职责。

例如，您有一个与某职责关联的选项卡布局，并且要将其应用于另一个职责，则可以先将所需的选项卡布局设置导出到 XML 文件，根据需要修改此文件，然后将其导入到目标职责中。

注释：与职责关联的选项卡布局将作为附件存储在 Siebel 文件系统中。这些文件将自动被发送给移动用户。

导出选项卡布局

本节介绍将选项卡布局导出到 XML 文件的过程。

要导出选项卡布局

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 应用程序”>“职责”。
- 2 在“职责”列表中，单击“选项卡布局”视图选项卡。
- 3 选择具有所需选项卡布局的职责。
- 4 在“应用程序”列表中选择记录。

注释：您可以选择多个应用程序，并为一个或多个关联应用程序的某个职责导出此选项卡布局。XML 文件将包含所选应用程序的屏幕选项卡和视图选项卡设置。在您以后导入 XML 文件时，该文件中的标记将指定在随后从该文件中导入选项卡布局时将受影响的应用程序。

5 单击“职责”列表中的“菜单”按钮，并选择“导出选项卡布局”。

6 保存 XML 文件。

例如，对于为使用 Siebel Field Service 的现场工程师设计的职责，如果要保存其选项卡布局设置，您可能要导出诸如 Siebel Field Service@Field Engineer.xml 之类的文件。

导入选项卡布局

本节介绍了从您以前导出的 XML 文件导入选项卡布局的过程。

要将选项卡布局导入到目标职责中

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 应用程序” > “职责”。
- 2 单击“选项卡布局”视图选项卡，并在“职责”列表中选择目标职责。
- 3 单击“职责”列表中的“菜单”按钮，并选择“导入选项卡布局”。
- 4 在导入对话框中，选择您要为应用程序选项卡布局导入的 XML 文件。
- 5 单击“导入”。

在导入 XML 文件之后，应用程序中的缺省选项卡与在所导入文件中定义的选项卡对应。

注释：导入选项卡布局文件将为受影响的用户隐藏并重新排列视图。虽然您不能直接恢复导入引起的更改，但是，仍然可以在“职责管理”视图中修改选项卡布局设置，也可以修改 XML 文件并重新导入。

通过职责管理任务

在创建职责之后，您可以输入具有该职责的雇员通常执行的任务。这些任务将出现在这些雇员主页的任务列表中。

请为每项任务输入标题并选择图像文件。每项任务都将作为超级链接显示在任务列表中。输入说明，这也会显示在任务列表中。

此外，请为每项任务指定执行该任务所在的视图。用户在主页中单击该任务的超级链接时，此视图将会出现。

系统已经为各 seed 职责指定了此类型的个性化。

要将任务与职责关联

- 1 以管理员身份登录。
- 2 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 应用程序” > “职责”。
- 3 在“职责”列表中，选择要与任务关联的职责。
- 4 单击“任务”视图选项卡。

- 5 在“任务”列表中，为与该职责关联的每项任务添加新记录，并且在新记录中输入关于每项任务的信息。

字段	准则
名称	输入任务的名称。
标题	输入任务的标题，它将作为超级链接显示在任务列表中。
说明	输入任务的说明，它将显示在任务列表中的标题下面。
目标视图	单击选择按钮，并选择在用户单击该任务的超级链接时将出现的视图。
序列	您可以根据需要指定在主页上此职责的任务列表中该任务的显示顺序。如果将该字段留空，任务将按此处列出的顺序显示。
图像	选择图像，它作为一个超级链接显示在任务列表中该任务的左边。
组	如果应用了搜索规范筛选要显示在任务子视图中的任务，并且多个任务子视图与该职责关联，则使用该字段。

清除高速缓存的职责

在用户以特定职责登录时，该职责将被高速缓存。用户只能访问在登录时已经为适用职责定义的那些视图，即使管理员自用户登录起可能添加了其它视图。

如果您在“职责”视图（职责列表图）中添加、删除或修改了职责，则可以清除高速缓存，以指示 Siebel 应用程序从数据库读取已更新的值。清除高速缓存将使这些更改可供以后登录或已注销又重新登录的用户使用。Siebel 服务器不需要重新启动。

要清除高速缓存的职责

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 应用程序” > “职责”。
- 2 在“职责”列表中，单击“清除高速缓存”。

附加访问控制机制

本节包含访问控制信息，它是对基本访问控制机制的补充。它介绍了如何配置弹出式子视图、选择子视图和向下搜索的可视性。

配置弹出式子视图和选择子视图的可视性

弹出可视性确定在显示弹出式选择子视图时将显示哪些数据，例如在用户将联系人与客户关联或者将销售代表添加到销售团队中时。

弹出可视性通常在 Siebel Tools 中业务组件对象的“弹出可视性类型”属性中进行设置。如果以这种方式设置弹出可视性，基于该业务组件的任何弹出项将向所有用户显示相同的数据。

注释：本节介绍了配置背景信息。它并未介绍使用 Siebel Tools 的详细说明。有关使用 Siebel Tools 的信息，请参阅 *Configuring Siebel eBusiness Applications*。

通常存在这样的情形，即您需要更多的灵活性以确定要在弹出式选择子视图中显示哪些视图。例如：

- 贵公司的大多数雇员在将销售代表分配给销售团队时，只需要查看您所在组织的职位。
- 合作者经理需要查看您所在组织的职位以及他们管理的合作者组织的职位。

此外还有其它许多方案，其中对合作者的可视性限制比您的雇员更严格。

为了满足此业务要求，Siebel eBusiness Applications 提供三个功能，以允许开发人员以另一个设置覆盖在业务组件级别的“业务组件弹出可视性类型”属性中设置的可视性。开发人员可以：

- 设置选取列表对象定义的可视性
- 使用“可视性全部自动”属性
- 使用特殊框架类和用户属性

设置选取列表对象定义的可视性

开发人员可以在“可视性类型”属性中的“选取列表”对象定义上设置其它可视性类型，以覆盖在业务组件级别设置的可视性。

如果这样做，您会覆盖为该业务组件中特定实例的所有用户在此实例中的业务组件级别设置的可视性。

例如，您可能希望合作者可以添加新的资金请求，并将这些资金请求与他们参与的商业活动关联。然而，您希望合作者只看到他们有权访问的商业活动。您可以配置一个特殊的选取列表以用于此目的，并将该选取列表的可视性设置为“销售代表”，以便合作者在与资金请求关联时只能从可访问的商业活动进行选择。

使用“可视性全部自动”属性

对于“选取列表可视性类型”和“业务组件弹出可视性类型”，您都可以使用“可视性全部自动”属性覆盖该可视性类型属性。

该属性将检查当前用户的职责，查看它是否包括基于相同业务组件的“全部跨组织”视图。如果找到此视图，则覆盖该可视性类型，并且用户将获得对出现问题的对象的全部可视性。否则，将不覆盖该可视性类型。

例如，“商机”业务组件上的弹出可视性设置为“组织”，并且“全部自动”设置为 TRUE，大多数用户将会在“商机”选择子视图中看到自己组织的所有商机。另外，还具有访问“跨组织的所有商机”视图权限的用户可以看到所有的可用商机，而不考虑组织。

该属性使可视性在各视图和弹出式选择子视图间保持一致。

该属性可以覆盖其它任何可视性类型，包括销售代表、经理、组织等等。除了“业务组件”和“选取列表”属性之外，还可以对“链接”对象设置该属性。

该属性经常供主管人员或管理用户使用，他们通常有权访问 Siebel 应用程序中的所有数据。

使用特殊框架类和用户属性

开发人员可以使用特殊框架类和用户属性，根据正在使用的应用程序设置子视图对象上选择子视图的可见性。

例如，如果用户正在运行 Siebel Sales，销售团队的“选择职位”子视图将只显示该用户组织的职位。如果用户在运行 Siebel 合作者管理器，子视图则显示用户自己的组织及其子组织的职位，从而允许用户选择他们管理的合作者的职位。

要覆盖在业务组件级别设置的弹出可见性，开发人员必须进行以下更改：

- 如果要覆盖其可见性的子视图是一个关联子视图，请将该子视图的框架类改为 `CSSSWEFrameListVisibilityAssoc`。
- 如果要覆盖其可见性的子视图是一个选择子视图，请将该子视图的框架类改为 `CSSSWEFrameListVisibilityPick`。
- 添加包含以下值并且名称为“覆盖可见性”的子视图用户属性：
 - 名称：覆盖可见性：[*Application Name*]
 - 值：[*visibility Type*]，是开发人员可从标准可见性类型中进行选择的位置。

配置向下搜索

向下搜索可见性可能出现在以下两个不同的方案中：

- **在相同的业务对象中。**如果初始视图和向下搜索视图同时基于相同的业务对象，并且没有在向下搜索视图中指定可见性，无论初始视图采用哪一种可见性，该可见性将继续用于向下搜索视图中。

如果向下搜索对象的向下搜索视图具有不同于初始视图的可见性子视图类型设置，执行向下搜索到某个记录会将用户带到目标视图的第一个可见记录，而不是带到此向下搜索记录。

- **在不同业务对象之间。**如果初始视图和向下搜索视图基于不同的业务对象，要从一个视图移至另一个视图，则可能需要将目标视图中的可见性重新设置为不同于标准设置的其它设置。

如果为子视图的向下搜索对象设置可见性类型属性，将会覆盖该向下搜索视图的可见性子视图类型设置。例如，假设您配置了可见性类型是“全部”的向下搜索对象，在向下搜索时它将覆盖此向下搜索视图中诸如“销售代表”等可见性。

向下搜索对象的“可见性类型”属性只覆盖目标视图的“可见性子视图类型”属性一次，也就是在您执行向下搜索时。如果您导航到屏幕中的另一个视图，然后返回到目标视图，则应用目标视图的初始可见性。每次在您执行向下搜索之后导航到同一个屏幕的其它视图时，可见性均会刷新。

例如，假设您在执行向下搜索之后导航到同一个屏幕中具有个人访问控制的视图，该向下搜索记录将不再可见。如果您之后返回到目标视图（可见性是“销售代表”），向下搜索记录仍然为不可见。如果您导航到可见性为“全部”的第三个视图，则可以再次看到该向下搜索记录。

向下搜索可见性和可见性规则

在使用可将您带到另一个屏幕的向下搜索时，线程栏被更新。当前视图根据旧视图（向下搜索之前）以及当前视图（向下搜索之后）中子视图的业务组件之间定义的链接，使用一种主要 - 明细关系显示其记录。

除了介绍的主要 - 明细关系之外，可以使用由“应用的可见性规则”链接属性确定的可见性规则限制此视图中的检索记录。

如果“应用的可视性规则”设置为“永不”，则不应用附加的可视性规则。线程上下文的主要 - 明细关系确定了视图中的可视记录，而不考虑当前视图的可视性设置。如果您使用视图栏更改了视图，线程上下文仍会保留，并且可能会显示正常情况下（没有线程上下文）在此新视图中不可视的记录。

另一方面，如果“应用的可视性规则”设置为“始终”，则应用附加的可视性规则。Siebel 应用程序在执行向下搜索时可能显示错误消息，从而让用户知道他或她可能没有查看此明细记录的相应权限。

当事方数据模型

S_PARTY 表是第 181 页的表 20 中列出的所有当事方的基本表：人员（联系人）、用户、雇员、合作者用户、职位、客户、部门、组织、合作者组织、家庭、用户列表和访问组。

对于 S_PARTY 表中存储的每个当事方记录，PARTY_TYPE_CD 列的值表示当事方类型。扩展表与当事方类型一起提供了不同当事方之间的主要差别。

有关如何使用连接从多个表中提取数据到单一业务组件（例如，为雇员、客户和其它业务组件提取当事方类型的数据）的信息，请参阅 *Configuring Siebel eBusiness Applications*。

在第 230 页的图 18 中，组成当事方数据模型的基本表和扩展表显示在“当事方”边界（黑色框）内。显示在“当事方”边界之外的表用于定义当事方之间的关系。后面的小节图示了如何对各特定当事方应用此当事方数据模型。

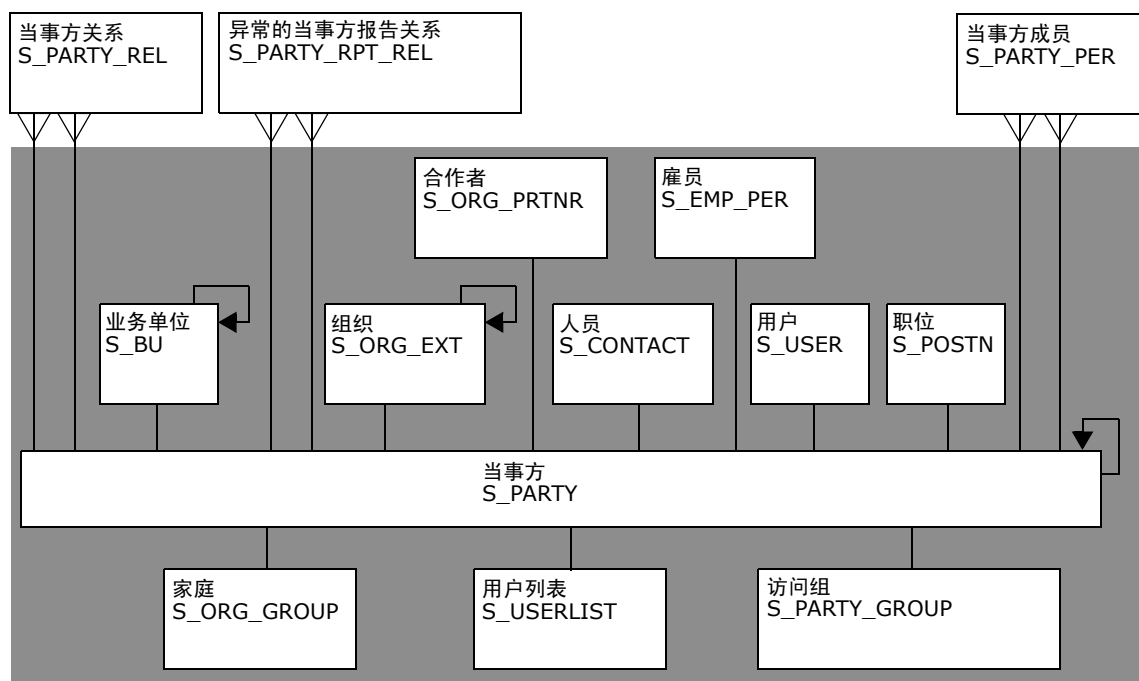


图 18. 当事方数据模型

当事方如何相互关联

当事方具有一些必需关系，如下所述。

- 部门、组织和客户是“组织”当事方类型的实例。
- 如果内部组织标志为 TRUE（INT_ORG_FLG = “Y”）并且具有关联的 S_BU 记录，部门、内部或合作者也是一个组织。
- 每个部门与一个组织关联：可以是部门本身，也可以是关系最近的祖先部门，后者也是一个组织。
- 每个职位与一个部门关联。然后，职位将自动与一个组织关联，即与该部门关联的组织。
- 人员（联系人）、用户、雇员和合作者用户是“人员”当事方类型的实例。
- 通常，您可以将每个雇员和合作者用户与一个或多个职位关联。雇员或合作者用户一次只能有一个活动职位。雇员或合作者用户一次自动与一个部门和一个组织关联，即与该活动职位关联的部门和组织。
警告：建议不要合并雇员记录。否则，您可能会在极大范围内破坏当事方关系，并产生意外后果。
- 要授予数据的可视性，请使用 S_PARTY_PER 表存储“人员”类型的当事方与其它类型的当事方之间的关联关系。例如，客户与联系人关联，用户与职位关联等等。与职位关联的用户可以看到分配给该职位的客户或商机的数据（如果这是一个活动职位）。存储在 S_PARTY_REL 中的关系也会影响给移动用户的数据发送。
- 为了存储当事方之间这种信息型的特殊关系，此类关联通过 S_PARTY_REL 表进行存储。例如，公司及其会计公司可能都作为客户存储。假设您的应用程序提供了定义此关系的功能，它可以存储在 S_PARTY_REL 表中。
- 当事方之间的信息型特殊关系存储在 S_PARTY_REL 表中。例如，公司及其会计公司可能都作为客户存储。这两个客户之间的关系可以存储在 S_PARTY_REL 表中，前提是已经配置您的应用程序以定义这些关系。

人员（联系人）数据模型

在第 232 页的图 19 中，阴影部分是用于定义人员或联系人的基本表和扩展表 (S_CONTACT)。人员是数据库中最简单的表现形式。

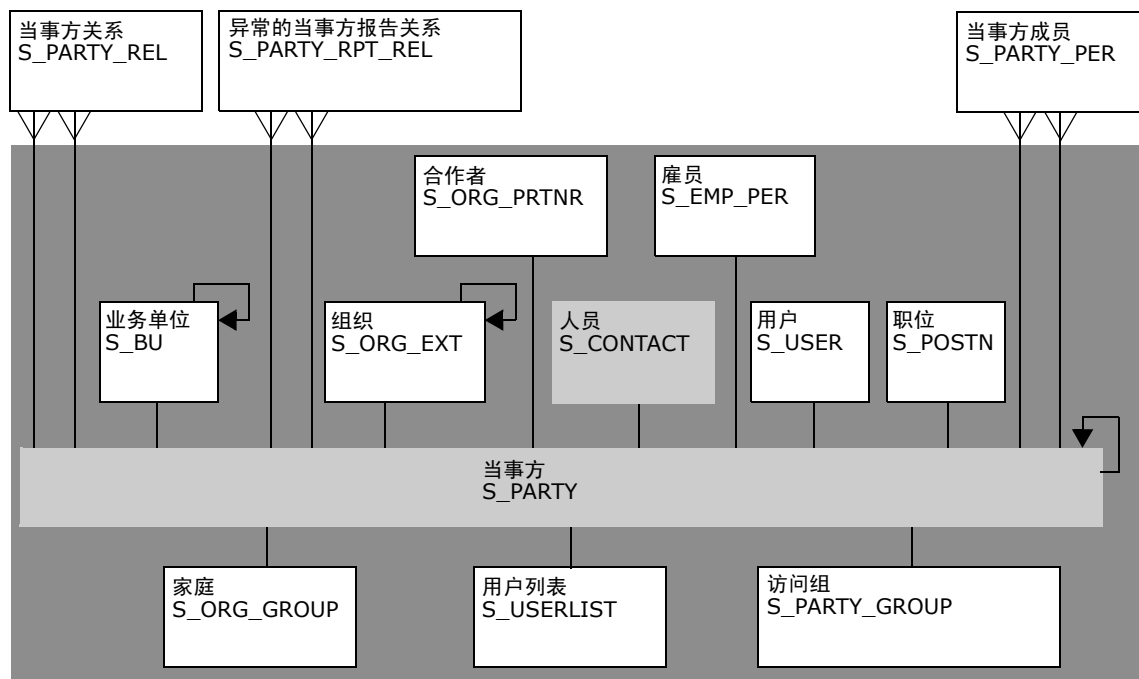


图 19. 人员（联系人）数据模型

用户数据模型

在第 233 页的图 20 中，阴影部分是用于定义用户的基本表和扩展表（S_CONTACT 和 S_USER）。用户是增加了以下特点的人员：

- S_USER 表包含该用户的登录信息。
- S_PER_RESP 交集表（未显示）指定了该用户的职责。
- 可能将联系人提升为用户。例如，在“管理 - 用户”屏幕的“所有人员”视图中为人员添加“用户 ID”值，可导致将该人员作为一位用户显示在“用户”视图中。

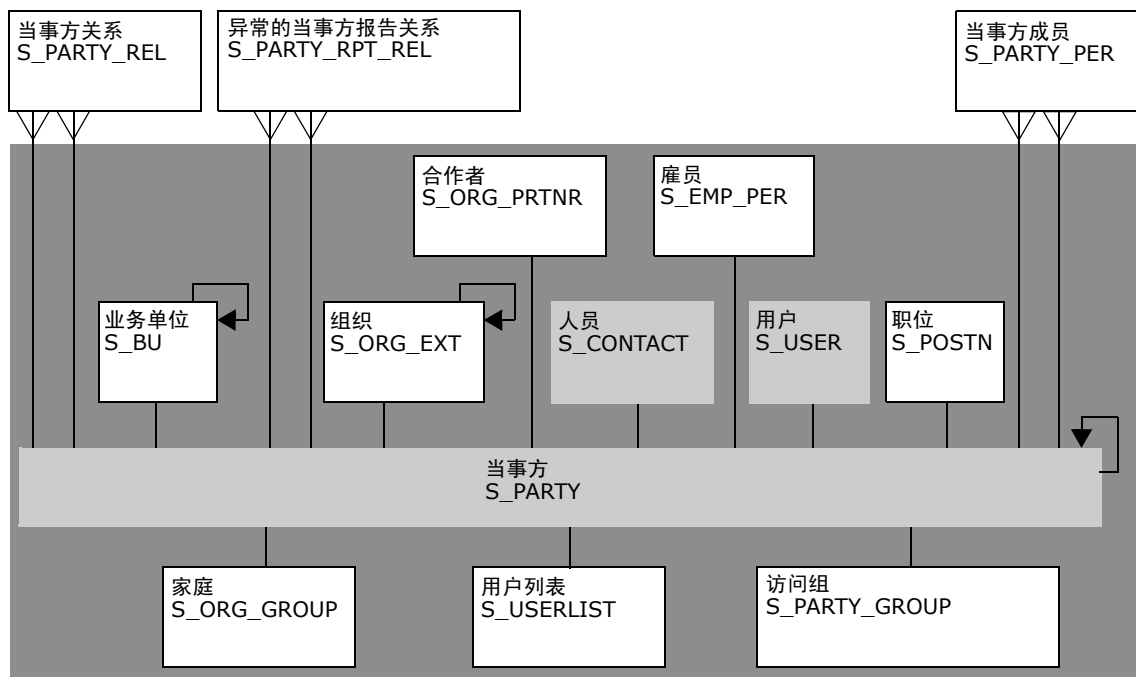


图 20. 用户数据模型

雇员数据模型

在第 234 页的图 21 中，阴影部分是用于定义雇员的基本表和扩展表（S_CONTACT、S_USER 和 S_EMP_PER）。内部雇员和合作者用户是代表“雇员”的记录。

雇员是增加了以下特点的用户：

- S_EMP_PER 提供了该用户的雇员数据。
- 使用 S_POSTN 表定义的职位通常（但不一定）与雇员关联。
 - 如果职位所属的组织不是合作者组织，则该雇员是内部雇员。
 - 如果组织是合作者组织，则该雇员是合作者用户。

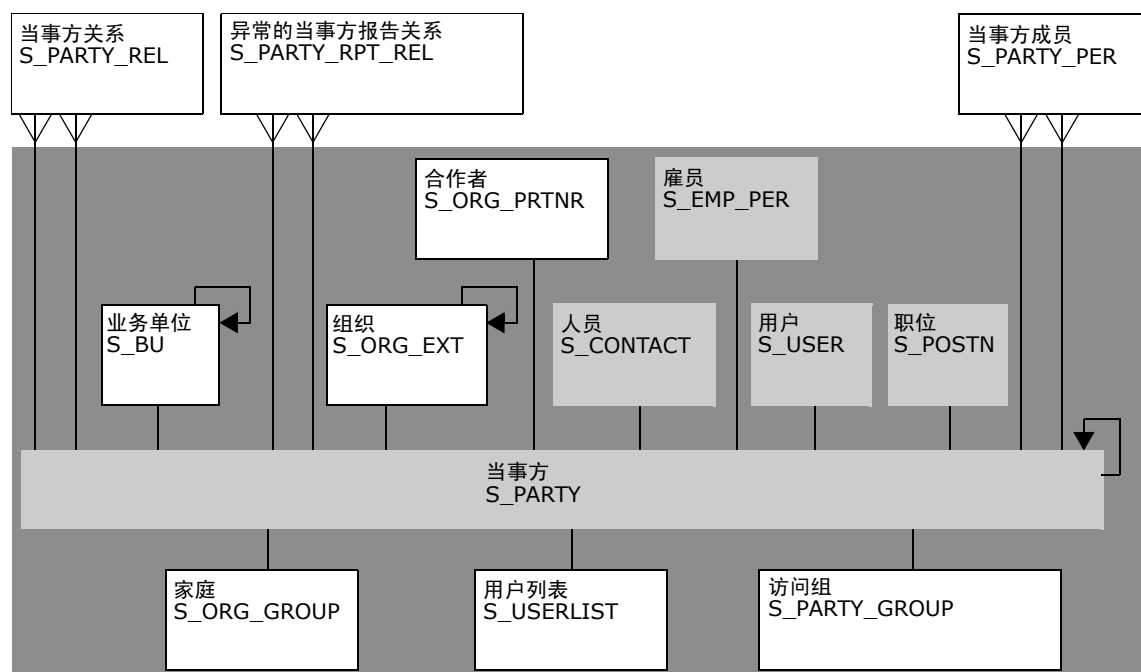


图 21. 雇员数据模型

职位数据模型

在第 235 页的图 22 中，阴影部分是用于定义职位的基本表和扩展表 (S_POSTN)。

注释：在职位中，就象在 Siebel 应用程序的其它区域一样，基本表的 ROW_ID 列使用了外部关键字引用。ROW_ID 列在用户界面中不可视，并且不能手动进行更改。这是因为如果允许用户更改该值，各基本表之间的完整性将丢失。更改职位名称不会影响外部关键字（基础的基本表中的 ROW_ID）。

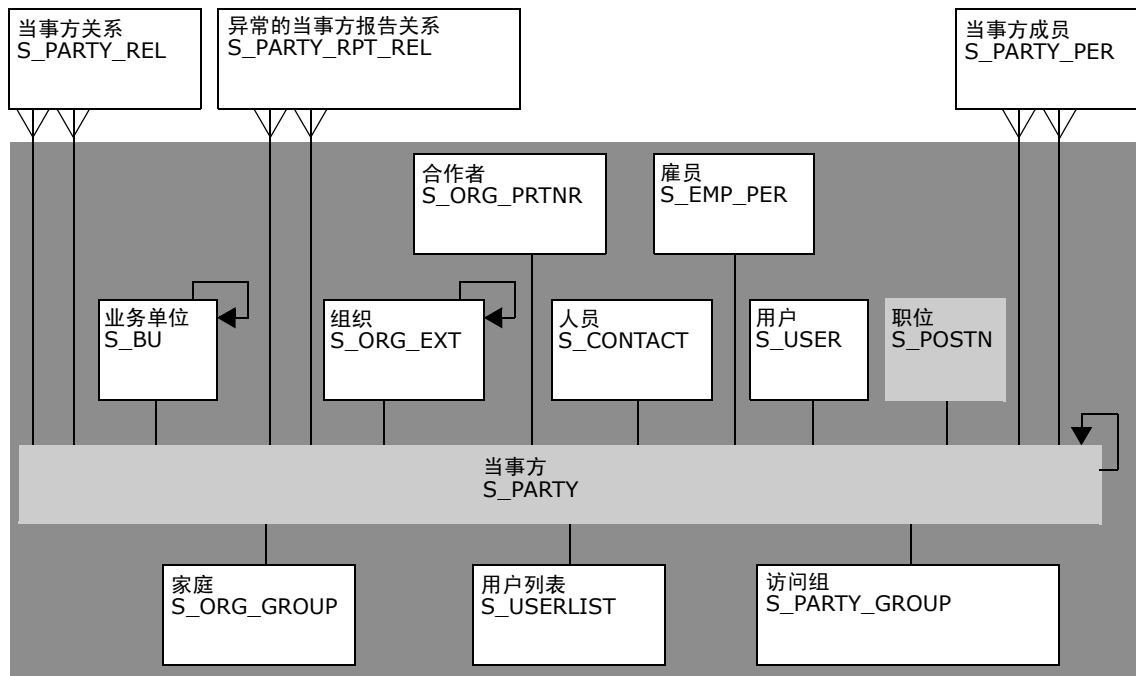


图 22. 职位数据模型

客户数据模型

在第 236 页的图 23 中，阴影部分是用于定义客户的基本表和扩展表 (S_ORG_EXT)。

(客户、部门、组织和合作者组织共享许多相同的数据模型元素。)

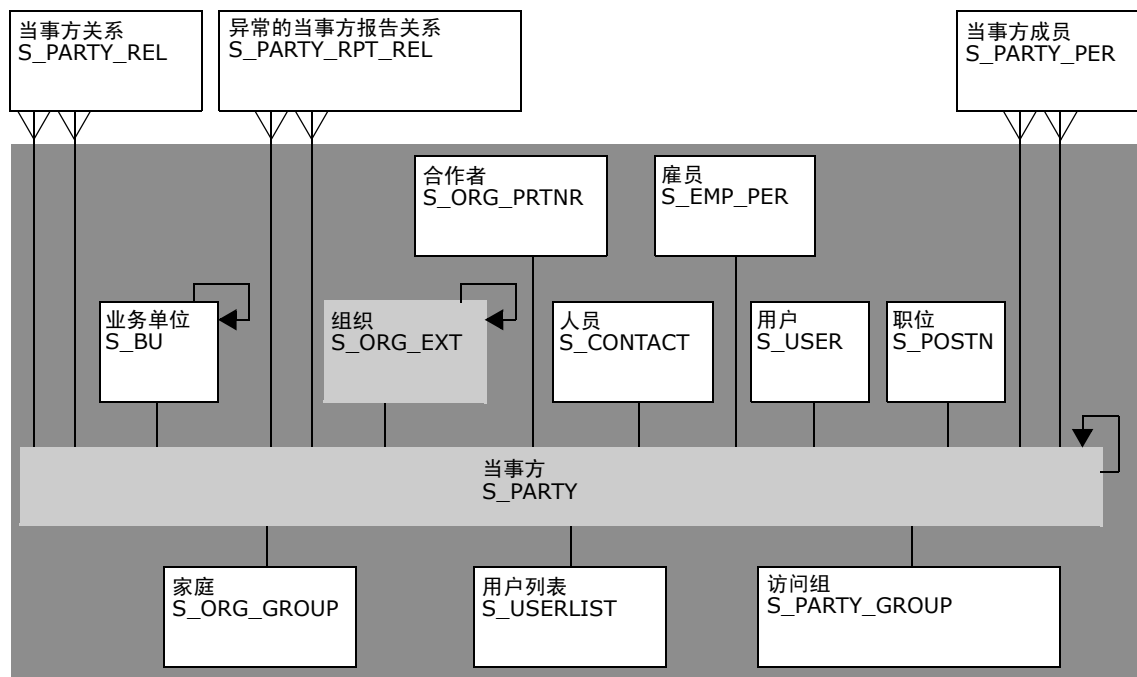


图 23. 客户数据模型

组织数据模型

在第 238 页的图 25 中，阴影部分是用于定义组织的基本表和扩展表（S ORG EXT 和 S BU）。

组织有时也称为业务单位，它也是一个部门，但是在 S BU 表中存在记录。

(客户、部门、组织和合作者组织共用许多相同的数据模型元素。)

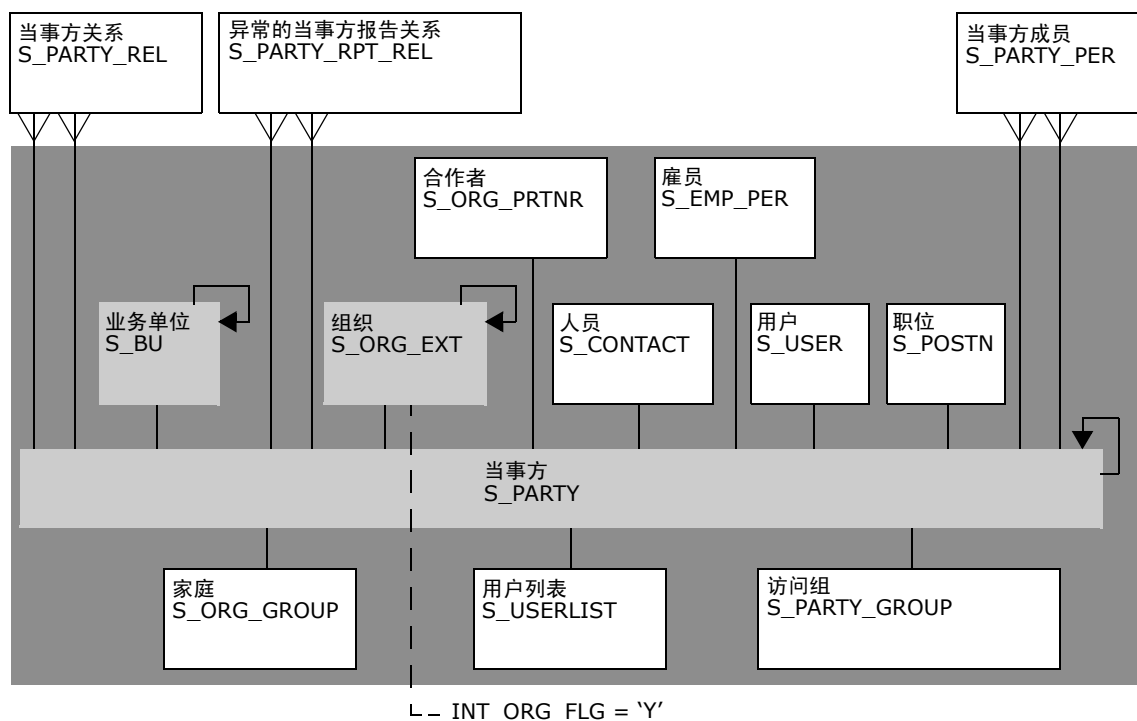


图 25. 组织数据模型

合作者组织数据模型

在第 239 页的图 26 中，阴影部分是用于定义合作者组织的基本表和扩展表（S_ORG_EXT、S_BU 和 S_ORG_PRTNR）。

合作者组织与组织相同，但是 S_ORG_EXT 中的 PRTNR_FLG 标志确定它是否为合作者组织。

（客户、部门、组织和合作者组织共用许多相同的数据模型元素。）

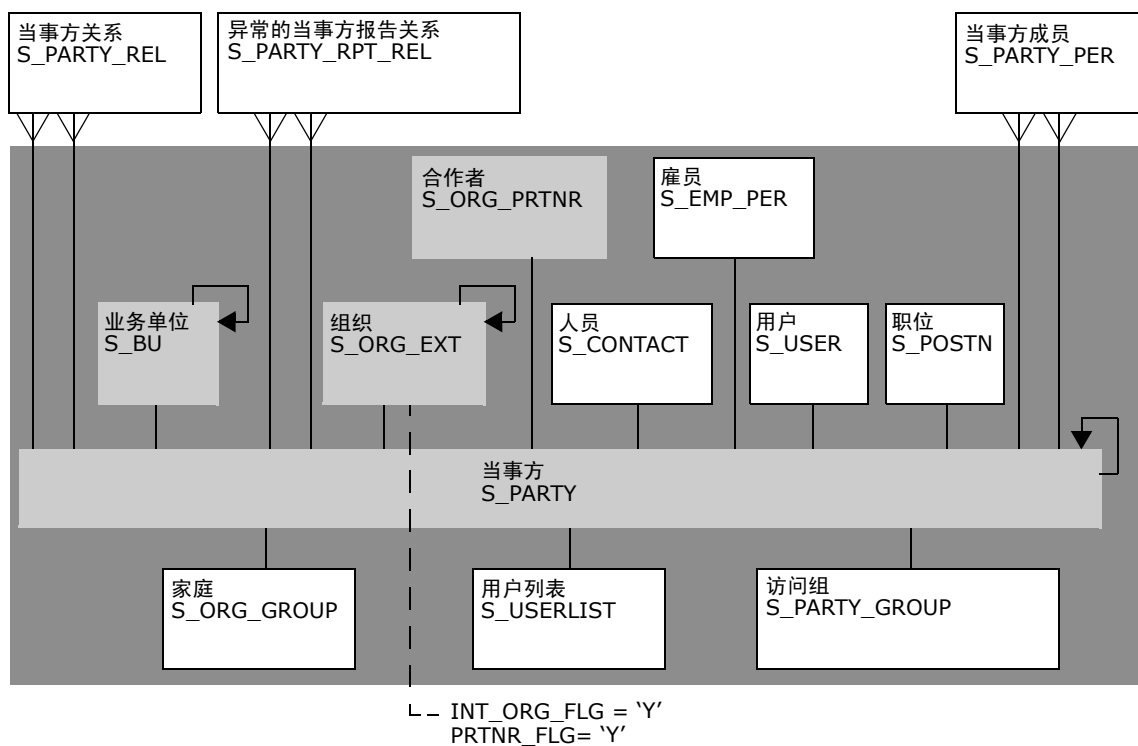


图 26. 合作者组织数据模型

家庭数据模型

在第 240 页的图 27 中，阴影部分是用于定义家庭的基本表和扩展表 (S_ORG_GROUP)。

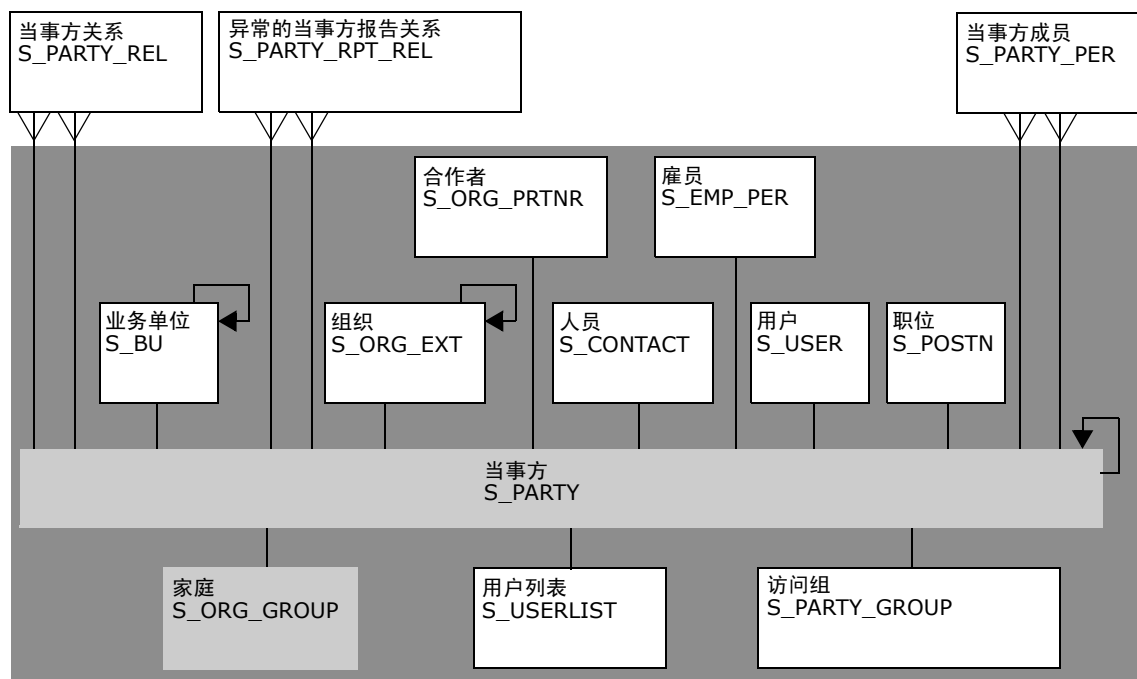


图 27. 家庭数据模型

用户列表数据模型

在第 241 页的图 28 中，阴影部分是用于定义用户列表的基本表和扩展表 (S_USERLIST)。

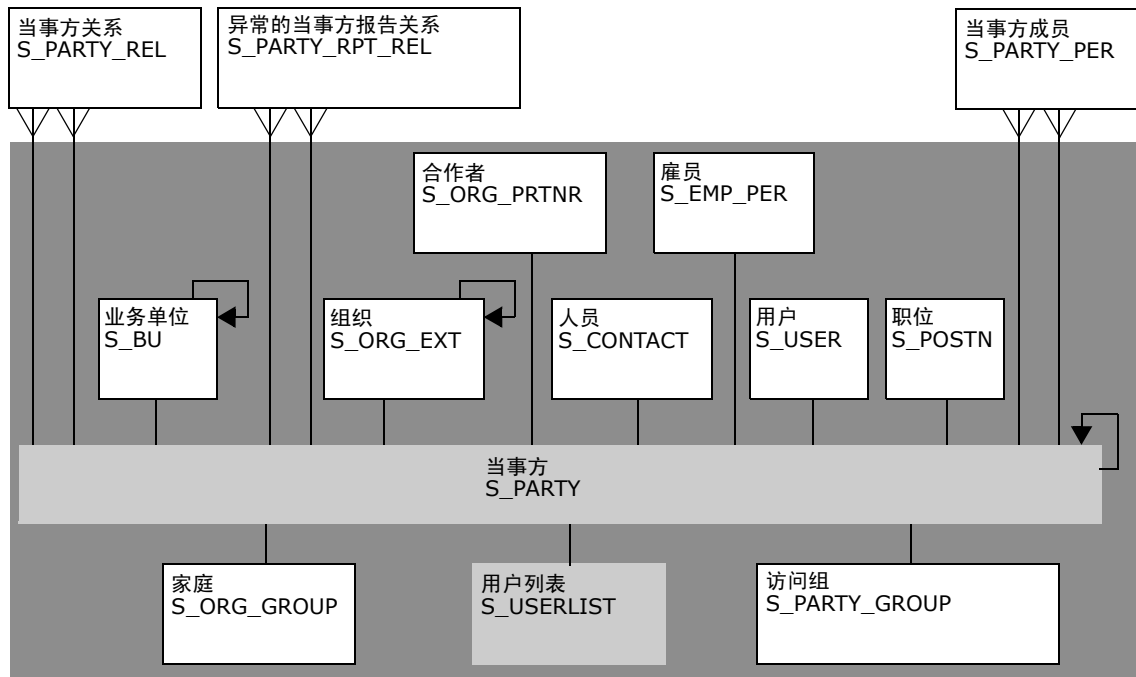


图 28. 用户列表数据模型

访问组数据模型

在第 242 页的图 29 中，阴影部分是用于定义访问组的基本表和扩展表 (S_PARTY_GROUP)。

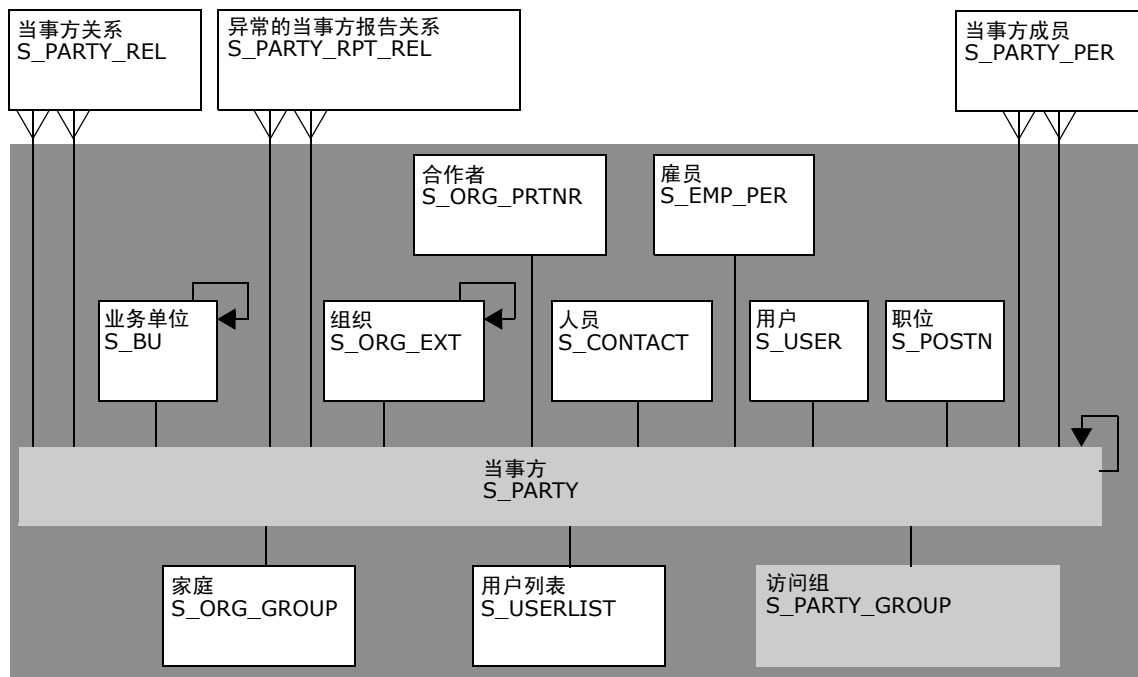


图 29. 访问组数据模型

A

安全问题疑难解答

本附录提供了在 Siebel eBusiness Applications 中可能出现的与安全有关问题的疑难解答提示及信息。它包括以下主题：

- 第 243 页的“用户验证问题”
- 第 244 页的“用户注册问题”
- 第 246 页的“访问控制问题”

用户验证问题

本节介绍了在验证用户时可能出现的问题。

用户无法在“管理 - 服务器配置” / “管理 - 服务器管理”屏幕中工作

服务器管理组件通过验证它从应用程序对象管理器 (AOM) 获取的 Siebel 用户 ID 是数据库帐户的用户名来自行执行验证。外部验证系统 (Web SSO 或 Siebel 安全适配器验证) 返回用户的 Siebel 用户 ID 以及数据库帐户 (通常是 LDAP 或 ADS 目录中的许多用户使用)。

在您使用外部验证时，服务器管理员可能无法访问“管理 - 服务器配置”或“管理 - 服务器管理”屏幕。或者，如果将系统配置为使用审计追踪功能，则可能出现一些审计追踪的问题。

要允许管理员用户在服务器管理屏幕中工作 (并且避免出现审计追踪问题)，请为此规模相对较小的组中的每位用户使用数据库验证，而不是外部验证。管理员用户应该使用不同的 AOM 或 Siebel 专用 Web 客户机登录到应用程序，无论是采用哪一种方式，都必须配置数据库验证。

或者，您可以为辅助数据来源 (例如 Siebel 网关名称服务器) 配置验证。

有关数据库验证的详细信息，请参阅第 68 页的“配置数据库验证”和相关章节。

添加用户或更改口令的结果未反映在目录中

如果您在 Siebel 应用程序中添加用户或更改口令，但是这些更改未反映在目录中，请确保安全适配器的 PropagateChange 参数设置为 TRUE。有关详细信息，请参阅第 251 页的“Siebel 网关名称服务器参数”。

运行 LDAP/ADSI 配置实用程序时出现问题

尝试从作为要配置的 Siebel 应用程序主机的机器上运行此实用程序。该实用程序在本地 (而不是通过网络) 运行时效果最佳。

目录中的职责与 Siebel 应用程序中的职责冲突

建议您在目录中或者使用 Siebel 应用程序分配用户职责，但是不要同时采用这两种方式分配用户职责。有关详细信息，请参阅第 119 页的“配置在目录中定义的角色”。

升级 Siebel 应用程序似乎禁用了 checksum 验证

无论何时升级 Siebel 应用程序，您都必须重新计算安全适配器的 CRC checksum 值。有关详细信息，请参阅第 115 页的“配置 Checksum 验证”。

应用程序日志文件中出现“Web 验证失败”错误消息

如果为 Web SSO 配置安装（不包含匿名浏览），并且未设置 ProtectedVirtualDirectory 参数，则可能出现该消息。

要修复该错误，请将 eapps.cfg 文件中的 ProtectedVirtualDirectory 参数设置为与应用程序目录相同的值。例如：

```
[/eSales]
ProtectedVirtualDirectory=/eSales
```

用户注册问题

本节介绍了在注册用户时可能出现的问题。

工作流程未出现在“业务流程管理”屏幕中

您的服务器或应用程序可能正在以不同于数据库的语言运行。例如，正在运行 DEU 安装，而数据库的语言是 ENU。

请检查您的设置。请使用 Server Manager 连接至该服务器，并运行 list param lang 以验证语言。如果语言代码不正确，您可以运行 change param lang=LANGUAGE，其中 LANGUAGE 是三个字母的数据库语言代码。重新启动服务器。

在我单击“新建用户”时，没有出现任何反应或者出现一则错误消息

原因可能包括：

- 尚未激活一个或多个必需的用户注册工作流程。
- 应用程序设置的语言与数据库的语言不相符。
- 未正确激活此工作流程。

要更正该问题：

- 按照第 153 页的“激活自行注册的工作流程过程”中的介绍激活工作流程过程。
- 使用 Server Manager 连接至该服务器，并运行 list param lang 以验证语言。如果语言代码不正确，您可以运行 change param lang=LANGUAGE，其中 LANGUAGE 是三个字母的数据库语言代码。重新启动服务器。

在我单击“完成”时，出现“在‘插入新用户’步骤中更新业务组件时出错”的消息

此问题的出现通常是因为 LDAP 目录服务器中已存在正在创建的用户。LDAP 目录服务器未被刷新以及让每个人共享。您要尝试创建的用户对于数据库来说可能是新用户，但是该用户可能已存在于 LDAP 目录中。如果在测试部署之后未刷新目录，通常会出现该问题。

请尝试创建另一个用户，或者使用 LDAP 控制台检查目录中是否已存在该用户。请连接至 LDAP 服务器，但不创建新用户，而是右键单击“人员”，然后选择“搜索”。

在我单击“完成”之后，出现“视图无法访问”的消息

已成功创建该用户，并且用户可以登录。但是，所创建的该用户未收到适当的职责，因此无法访问视图。

请将应用程序匿名用户的“新职责”字段更改为包含必需视图的值。

在我单击“新建用户”链接时，没有出现任何反应

出现此问题的原因很可能是，尚未激活有些或所有用户注册工作流程过程，或者如果已经激活，则还需要重新启动服务器。

请在“管理 - 服务器管理”屏幕中，只重新启动必需的 AOM。重新启动服务器也可以解决问题。

在我单击“用户注册”视图中的“下一步”时，没有出现任何反应

可能是正在触发另一个工作流程，并且该工作流程破坏了用户注册工作流程。也可能是尚未激活所有必需的工作流程。您必须激活所有必需的工作流程。

要禁用具有破坏性的工作流程：

- 1 在“管理 - 运行时事件”屏幕中，单击“事件”视图。
- 2 “对象名称查询”为 NULL。

除了某些应用程序类型事件之外，应该没有其它的事件。请特别留意行为组名称以“工作流程”开头的任何记录。此类记录表示，每次发生在“事件”字段中指定的事件时都会触发工作流程。如果它是常见事件（例如 ShowApplet 或 WriteRecord），则特别具有破坏性。对象名称通常将这些行为限定为只有在对象的上下文中发生指定事件的情况下才触发；例如，特定的业务组件或子视图。

- 3 如果存在可疑的事件，请向下搜索到“行为组名称”，并记下“业务服务上下文”字段中 ProcessId 字符串后面的 ID。
- 4 查询数据库以找到可疑的工作流程：从 S_WF_STEP 中选择 NAME，其中 ROW_ID='xxx'，xxx 是以前记下的 ID。

该工作流程是一个具有破坏性的工作流程。请禁用该工作流程。

在我单击“完成”时，返回一则错误

原因可能包括：

- SecThickClientExtAuthent 系统首选项没有设置为 TRUE。
- 自设置了系统首选项之后，尚未重新启动 Siebel 服务器。有关与用户验证相关的系统首选项的信息，请参阅第 260 页的“系统首选项”。

请检查该用户是否存在于“管理 - 用户”屏幕的“人员”视图中。如果该用户存在，但没有在 LDAP 服务器中为其提供一个条目，该用户则无法登录。您可以通过尝试在“用户”视图中创建用户来验证这一点。如果您可以设置用户 ID 和口令，请尝试以该人员身份登录。

访问控制问题

本节介绍了与访问控制有关的问题。

雇员用户在登录到 Siebel 客户应用程序时遇到问题

建议不要使用雇员登录帐户访问客户应用程序（例如 Siebel eSales），而应该为用户提供一个用于该应用程序的独立的登录帐户。

无法删除部门记录

您不能删除部门记录，这是因为整个 Siebel 应用程序中的业务组件都在引用组织记录。删除部门可能导致交易记录引用无效。但是，您可以重命名部门，或者将部门提升为组织。

无法修改 seed 职责

您不能修改或删除 seed 职责，但是，您可以复制要修改的 seed 职责，然后修改此副本。

一些移动用户的同步时间过长

请确保正确设置了“职责视图”列表中的“本地访问”控制字段。该设置决定了移动用户可以在脱机情况下使用哪些视图。为了加快同步速度，请减少具有本地访问权限的视图数。有关详细信息，请参阅第 201 页的“视图和职责的本地访问”。

B

与验证有关的配置参数

本附录介绍了在实施安全适配器时适用的配置参数。它包括以下主题：

- 第 247 页的“eapps.cfg 文件中的参数”
- 第 251 页的“Siebel 网关名称服务器参数”
- 第 256 页的“Siebel 应用程序配置文件参数”
- 第 260 页的“系统首选项”

注释：一般来说，与安全适配器配置有关的参数值应该由 LDAP 或 ADSI 管理员或数据库管理员验证。在此显示的许多值只是一些示例，可能并不适合您的部署要求。

eapps.cfg 文件中的参数

对于所有部署 Siebel Web 客户机的 Siebel 应用程序，eapps.cfg 文件包含控制 Siebel Web 引擎与 Siebel Web Server Extension (SWSE) 之间交互活动的参数。

eapps.cfg 文件位于 *SWEAPP_ROOT*\bin 目录中，其中 *SWEAPP_ROOT* 是安装 SWSE 的目录。

以下列表是 eapps.cfg 示例文件的一部分。该示例包含一些可能无法共存的参数。提供这些参数是为了让您可以看到与验证有关的一系列参数。

警告：通常，口令加密对于 eapps.cfg 文件有效，这是由 `EncryptedPassword = TRUE` 设置决定的。在这种情况下，`webUpdatePassword` 和 `AnonPassword` 的值将被加密。有关详细信息，请参阅第 33 页的“管理 eapps.cfg 文件中的加密口令”。

```
[swe]
Language = enu
Log = all
LogDirectory = D:\sea77\SWEApp\log
ClientRootDir = D:\sea77\SWEApp
WebPublicRootDir = D:\sea77\SWEApp\public\enu
WebUpdatePassword = test
IntegratedDomainAuth = FALSE
```

```
[defaults]
EncryptedPassword = TRUE
AnonUserName = GUESTCST
AnonPassword = GUESTCST
StatsPage = _stats.swe
SingleSignOn = TRUE
TrustToken = HELLO
UserSpec = REMOTE_USER
UserSpecSource = Server
DoCompression = TRUE
SessionTimeout = 300
GuestSessionTimeout = 900
```

```
[/prmpportal_enu]
AnonUserName = guestcp
AnonPassword = ldap
ProtectedVirtualDirectory = /p_prmpportal_enu
ConnectionString = siebel.TCPIP.None.None://172.20.167.200:2320/siebel/echannelobjMgr_enu

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

eapps.cfg 文件包含 [swe]、[defaults] 和 [connmgmt] 等部分以及用于单个 Siebel 应用程序的部分，例如 [/prmpportal_enu] 和 [/callcenter]。除非您使用应用程序自己部分中的某个录入值覆盖 [defaults] 部分中参数的值，否则所有单个应用程序都使用该部分中的每个参数值。

在上面的 eapps.cfg 示例文件中，Siebel Partner Portal 使用 [/prmpportal_enu] 部分中的 AnonUserName 和 AnonPassword 值，而不是 [defaults] 部分中提供的值。

注释：您可以使用任何纯文本编辑器添加参数及其参数值，或者更改现有参数的值。在您编辑配置文件时，不要使用在文件中添加附加的非文本字符的文本编辑器。

在给定的 eapps.cfg 文件中，缺省情况下有些参数可能不会出现。在您重新启动 Siebel 服务器和 Web 服务器之前，对 eapps.cfg 文件所做的更改不会生效。

与验证有关的参数

eapps.cfg 文件中的以下参数与验证有关。它们可以在 [defaults] 部分或用于单个应用程序的部分中定义。

- **AnonUserName**。该参数是存储在目录以及 Siebel 数据库中的匿名用户的用户名。
匿名用户提供了目录与 AOM 之间的绑定，从而允许向尚未登录的用户显示 Siebel 应用程序主页。同样，该匿名用户还要提供登录才能看到允许匿名浏览的其它页面。显示的主页可能提供了供用户登录的界面。
- **AnonPassword**。该参数是与 AnonUserName 配对的已验证的口令。
- **ClientCertificate**。如果在 Web SSO 实施中将该参数设置为 TRUE，则通过数字认证验证此用户。
另请参阅第 137 页的“数字认证验证”。
- **DoCompression**。指定 SWSE 是否将压缩 HTTP 信息流量。
如果压缩 HTTP 信息流量切实可行，这样做可以大大降低带宽消耗。HTTP 1.1 支持该功能，HTTP 1.0 不支持。
 - 如果将该参数设置为 FALSE，则不压缩 HTTP 信息流量。如果从不压缩 HTTP 信息流量，请使用该设置。例如，您的代理服务器只支持 HTTP 1.0，或者与带宽约束相比，压缩/解压缩的管理成本更让您关注，则可能使用该设置。
 - 如果将该参数设置为 TRUE，并且未检测到代理服务器，则压缩 HTTP 信息流量。但是，在检测到任何一个代理服务器时，将首先假定它不支持 HTTP 1.1，并且不压缩 HTTP 信息流量。如果您要在切实可行的情况下压缩 HTTP 信息流量，但是不能确信是否可能使用了不支持 HTTP 1.1 的代理服务器，请使用该设置。
 - 如果将该参数设置为 CompressProxyTraffic，则始终压缩 HTTP 信息流量。只有在您确信 Siebel 应用程序用户前面的任何代理服务器支持 HTTP 1.1 时，才对 Siebel 应用程序使用该设置。

您可以为单个 Siebel 应用程序设置该参数，或者通过在 [defaults] 部分中定义该参数，为多个应用程序设置该参数。例如，对于在 Intranet 上访问的雇员应用程序，如果您知道所部署的任何代理服务器都支持 HTTP 1.1，则可能将该参数设置为 CompressProxyTraffic。否则，请将该参数设置为 FALSE 或 TRUE（例如，在 [defaults] 部分中）。

注释：由于不可能知道外部用户（即合作者或客户）在使用哪一种代理服务器，因此应该只将 CompressProxyTraffic 设置用于雇员应用程序，而不适用于客户或合作者应用程序。

- **EncryptedPassword.** 如果该参数设置为 TRUE，匿名用户口令和 Web 更新口令被解释成加密口令。在您使用 SWSE 配置实用程序时，该参数被添加到 eapps.cfg 文件中（值为 TRUE）。然而，如果未在此文件中定义该参数，其效果等同于 FALSE 值。

有关详细信息，请参阅第 33 页的“管理 eapps.cfg 文件中的加密口令”。

- **EncryptSessionId.** 如果将该参数设置为 TRUE（缺省值），会话 ID 被加密。如果参数值为 FALSE，则不对会话 ID 进行加密。对于 Siebel Web 客户机，会话 ID 用于会话 cookie（基于 cookie 模式下）或应用程序 URL 中（cookieless 模式下）。

有关 cookie 的详细信息，请参阅第 143 页的“Cookie 和 Siebel 应用程序”。

- **GuestSessionTimeout.** 来宾用户的会话超时。缺省值为 300 秒（5 分钟）。有关会话超时的详细信息，请参阅 SessionTimeout 参数的说明。

- **SessionTimeout.** 从用户的上一个浏览器请求至用户连接超时的时间（以秒计）。缺省值为 900 秒（15 分钟）。标准会话是指用户使用其注册用户名和口令进行登录的会话。

注释：以上提及的所有会话超时都会使会话处于不活动状态。也就是说，如果将它们设置为 3600 秒，则需要会话保持不活动的时间达到一小时，才能使该会话超时。会话不活动表示未对该会话上的服务器提出任何请求。任何 ping 服务器的行为（包括消息栏更新和日程表警报功能），都会重置会话超时期间。如果更新间隔时间小于 SessionTimeout 值，会话将从不会超时。

- **SingleSignIn.** 如果该参数为 TRUE，SWSE 则在 Web SSO 模式下工作。

有关详细信息，请参阅第 7 章“Web 单一登录验证”。

- **SubUserSpec.** 在实施数字认证验证的 Web SSO 环境下，CN 值将指定应该从认证的 CN（公共名称）属性中提取 Siebel 用户 ID。

有关详细信息，请参阅第 138 页的“用户身份的来源”。

- **TrustToken.** 在 Web SSO 环境下，该标记字符串是 SWSE 与安全适配器之间的共享密钥。它是一种防止电子欺骗袭击的措施。此设置在 SWSE 和安全适配器上必须相同。

有关详细信息，请参阅第 7 章“Web 单一登录验证”。

- **UserSpec.** 在 Web SSO 实施中，该变量名指定 SWSE 在 UserSpecSource 所指定来源中的哪个位置查找用户的用户名。缺省情况下，值 REMOTE_USER 由验证筛选器填入。

如果在 Windows 或 AIX 上实施数字认证验证，请使用值 CERT_SUBJECT，它是包含认证名称的变量。例如，UserSpec/SubUserSpec 将成为 "CERT_SUBJECT"/"CN"。对于其它 UNIX 平台，UserSpec 使用 "REMOTE_USER"。SubUserSpec 设置将被忽略。

有关详细信息，请参阅第 138 页的“用户身份的来源”。

- **UserSpecSource.** 在 Web SSO 实施中，该参数指定 SWSE 从中导出用户证书的来源：如果从常用的 Web 服务器用户名字段中得到用户证书，则来源是服务器；如果变量位于 HTTP 请求标题中，则来源是标题。

有关详细信息，请参阅第 138 页的“用户身份的来源”。

以下参数可以在用于各 Siebel 应用程序的部分中进行定义：不要在 [defaults] 部分中定义该参数。

- **ProtectedVirtualDirectory**。该参数为 Siebel 应用程序指定受保护的虚拟目录。该参数指定 Web 服务器的虚拟目录，它表示 Siebel 应用程序的受保护位置。在 Web SSO 实施中该参数必须具有值，而在其它实施中则为可选。

该受保护的目录让您可以将 Web 服务器或第三方验证软件配置为在访问特定的 Siebel 应用程序视图时需要进行用户验证。如果请求需要显式登录的视图，此请求将被重定向到该虚拟目录。

有关详细信息，请参阅第 128 页的“创建被保护的虚拟目录”。

例如，如果您对 Siebel eService 受保护的虚拟目录使用了建议的名称，请输入：

```
[/eservice]
ProtectedVirtualDirectory = /p_eservice
```

如果没有为匿名浏览配置 Web SSO 实施，请将该值设置为与应用程序相同的目录。例如：

```
[/eservice]
ProtectedVirtualDirectory = /eservice
```

否则，应用程序的日志文件中可能出现 Web 验证失败的消息。

注释：您可以使用上述类似示例保护整个应用程序。然而，如果应用程序的某些部分不需要验证，您必须可以在用户访问应用程序的受保护部分时对这些用户进行验证。在此情况下，将该参数设置为传送 Web SSO 证书的别名。Siebel 应用程序将重定向验证请求。

eapps.cfg 文件中的以下参数可以在此文件的 [swe] 部分中定义。

- **IntegratedDomainAuth**。要对 Web SSO 支持 Windows 集成身份验证，请将该参数设置为 TRUE。该设置导致 SWSE 从 HTTP 标题中删除此域名，从而允许应用程序与 Windows 集成身份验证相集成。

SSL 相关参数

如果要使用 SSL 对 Web 服务器与 Siebel 服务器之间的 SISNAPI 通讯进行加密，则可以将以下参数包括在 eapps.cfg 文件的 [connmgmt] 部分中。有关详细信息，请参阅第 52 页的“为 SWSE 配置 SSL 加密”。

- **CACertFileName**。确定发行认证的信任机构。
- **CertFileName**。指定 ASN/PEM 认证文件的名称。
- **KeyFileName**。指定 PEM 私有密钥文件的名称。
- **KeyFilePassword**。指定用于对私有密钥文件进行解密的口令。
- **PeerAuth**。在 SSL 信息交换期间启用同级验证。
- **PeerCertValidation**。独立地验证 SWSE 机器的主机名与认证中出现的主机名匹配。

Siebel 网关名称服务器参数

Siebel 网关名称服务器的参数可以在一个或多个 Enterprise、Siebel 服务器或组件级别设置。它们在 Siebel 雇员应用程序（例如，Siebel Call Center）的“管理 - 服务器配置”屏幕中设置。

- 您在 Enterprise 级别设置的参数将配置整个 Enterprise 的所有 Siebel 服务器。
- 您在 Siebel 服务器级别设置的参数将配置特定 Siebel 服务器上的所有适用组件。
- 您在组件级别设置的参数将配置特定组件的所有任务或实例。
- 您为企业资料（指定子系统）配置的参数将配置适用的安全适配器。

为进行验证，大多数感兴趣的组件都是 AOM，例如，Call Center 对象管理器或 eService 对象管理器。同步管理器组件也支持验证。

在更低级别设置的特定参数将覆盖在更高级别设置的相同参数。例如，eService 对象管理器组件在 Enterprise 级别的设置是安全适配器模式 = LDAP，在组件级别的设置是安全适配器模式 = ADSI，则 Siebel eService 将使用 ADSI 安全适配器。

如果为 Siebel 安全适配器配置参数，则同时也是为企业资料（适用于 GUI Server Manager）或指定子系统（适用于命令行 Server Manager）配置参数。

有关配置安全适配器的详细信息，请参阅第 6 章“安全适配器验证”。

注释：有关如何使用 Siebel Server Manager 在 Siebel 网关名称服务器上设置参数的详细信息，请参阅 *Siebel System Administration Guide*。

数据库验证的参数

以下参数适用于数据库验证，并且为 InfraSecAdpt_DB 类型的指定子系统进行定义（也就是说，可能为 DBSecAdpt 指定子系统或具有非缺省名称的类似安全适配器设置这些参数）：

- **CRC（别名是 DBSecAdpt_CRC）**。使用该参数实施 checksum 验证，以验证每位用户通过正确的安全适配器获得对数据库的访问权限。该参数包含 checksum 实用程序为适用的安全适配器 DLL 计算的值。如果您将该值留空，系统则不执行检查。如果您升级系统，则必须重新计算并替换该参数中的值。

有关详细信息，请参阅第 115 页的“配置 Checksum 验证”。

- **数据来源名称（别名是 DataSourceName）**。确定要为其指定口令散列处理参数的数据来源。
- **传播更改（别名是 DBSecAdpt_PropagateChange）**。将该参数设置为 TRUE，以允许通过 Siebel 应用程序管理数据库中的证书。然后，如果管理员在 Siebel 应用程序中添加用户或更改口令，或者用户更改口令或自行注册，所做的更改将传播到数据库中。
- **安全适配器 DLL 名称（别名是 DBSecAdpt_SecAdptDllName）**。指定用于实施与 Siebel eBusiness Applications 集成所需的安全适配器 API 的 DLL。不需要明确指定文件扩展名。例如，sscfsadb.dll 在 Windows 实施中实施 Siebel 数据库安全适配器，sscfsadb.so 在 UNIX 实施中也实施 Siebel 数据库安全适配器。如果适配器的 DLL 名称用于 UNIX 实施中，则在内部将其转换为实际的 DLL 文件名。

以下参数也适用于数据库验证环境，并且为 InfraDataSource 类型的指定子系统进行定义（也就是说，可能为 ServerDataSrc 指定子系统或其它数据来源设置这些参数）。指定子系统被确定为数据库安全适配器的 DataSourceName 参数值。

- **散列用户口令（别名是 DSHashUserPwd）**。为用户口令指定口令散列处理。请使用通过 DSHashAlgorithm 参数指定的散列算法。有关详细信息，请参阅第 109 页的“配置口令散列处理”。
- **用户口令散列算法（别名是 DSHashAlgorithm）**。如果 DSHashUserPwd 是 TRUE，则指定要使用的口令散列算法。缺省值是 RSASHA1，它使用 RSA SHA-1 算法提供口令散列处理。SIEBELHASH 值指定由 Siebel Systems 的杂乱算法提供的口令散列机制（只对现有客户支持）。有关详细信息，请参阅第 109 页的“配置口令散列处理”。

LDAP/ADSI 验证的参数

以下参数适用于 LDAP/ADSI 验证，并且为 InfraSecAdpt_LDAP 类型的指定子系统进行定义（也就是说，可能为 LDAPSecAdpt 或 ADSISecAdpt 指定子系统或具有非缺省名称的类似安全适配器设置这些参数）：

- **应用程序口令（别名是 ApplicationPassword）**。在目录中为 ApplicationUser 参数定义的用户指定口令。
 - 在 LDAP 目录中，口令存储在属性中。
 - 在 ADS 中，口令通过 ADS 用户管理工具进行存储，它不存储在属性中。
- **应用程序用户（别名是 ApplicationUser）**。在目录中指定记录的用户名，该用户名具有足够权限读取任何用户的信息并执行任何必要的管理任务。

在某个用户请求登录页时，该用户提供了 LDAP 或 ADS 与 AOM 的初始绑定，否则需要匿名浏览目录。

如果是 LDAP，您输入该参数作为完整的识别名 (DN)，例如 "uid=APPUSER, ou=People, o=companyname.com"，包括引号在内。安全适配器使用该名称来绑定。

注释：您必须实施应用程序用户。

- **基本 DN（别名是 BaseDN）**。指定基本的识别名，它是树的根目录，该 Siebel 应用程序的用户存储在该根目录下面的目录中。在该目录下面可以直接或间接地添加用户。LDAP 服务器的典型录入值可能是 BaseDN = "ou=People, o=domain_name"。“o”表示“组织”，并且通常是 Web 站点的域名。“ou”表示“组织单位”，并且是存储用户的子目录。

ADS 服务器的典型录入值可能是 BaseDN = "CN=Users, DC=qatest, DC=siebel, DC=com"。域组件 (DC) 录入值是用于确定该服务器位置的嵌入域。公共名称 (CN) 录入值是目录中用户对象的特定路径。因此，请调整 CN 和 DC 录入值数量以代表您的体系结构。

- **CRC（别名是 CRC）**。使用该参数实施 checksum 验证，以验证每位用户通过正确的安全适配器获得对数据库的访问权限。该参数包含 checksum 实用程序为适用的安全适配器 DLL 计算的值。如果您将该值留空，系统则不执行检查。如果您升级系统，则必须重新计算并替换该参数中的值。

有关详细信息，请参阅第 115 页的“配置 Checksum 验证”。

- **证书属性类型（别名是 `CredentialsAttributeType`）**。指定存储数据库帐户的属性类型。例如，如果 `CredentialsAttributeType = dbaccount`，在验证用户名为 HKIM 的用户时，安全适配器从 HKIM 的 `dbaccount` 属性中检索数据库帐户。

该属性值必须采用 `username=U password=P` 的形式，其中 `U` 和 `P` 是数据库帐户的证书。在两个密钥值对之间可以有任意空白，但是在每个密钥值对内部不能有空白。关键字 `username` 和 `password` 必须是小写。

注释：如果您实施 LDAP 或 ADSI 安全适配器验证以通过 Siebel 客户机管理目录中的用户，则从创建新用户的用户处为新用户继承数据库帐户属性的值。此继承与您是否实施共享数据库帐户无关，但是不会覆盖共享数据库帐户的使用。有关共享数据库帐户的信息，请参阅第 116 页的“配置共享数据库帐户”。
- **散列数据库证书（别名是 `HashDBPwd`）**。为数据库证书口令指定口令散列处理。有关详细信息，请参阅第 109 页的“配置口令散列处理”。
- **散列用户口令（别名是 `HashUserPwd`）**。为用户口令指定口令散列处理。请使用通过 `HashAlgorithm` 参数指定的散列算法。有关详细信息，请参阅第 109 页的“配置口令散列处理”。
- **口令属性类型（别名是 `PasswordAttributeType`）**。指定属性类型，用户的登录口令将以该属性类型存储在目录中。

`PasswordAttributeType = userPassword` 是 LDAP 唯一支持的值。在用户名为 HKIM 的用户尝试登录时，安全适配器将 HKIM 的 `userPassword` 属性中的值与用户输入的口令进行比较。

该参数仅用于 LDAP 安全适配器。（ADS 不在属性中存储口令，因此该参数不适用于 ADSI 安全适配器。）
- **口令过期警告天数（仅限于 ADSI）（别名是 `PasswordExpireWarnDays`）**。指定在口令过期之前显示警告消息的天数。

该参数仅用于 ADSI 安全适配器。
- **端口（别名是 `Port`）**。指定服务器机器上用于访问 LDAP 服务器的端口。通常，标准传输使用缺省值 389，安全传输使用端口 636。

该参数仅用于 LDAP 安全适配器。（如果是 ADS，则在目录级别设置端口，以便不将该参数用于 ADSI 安全适配器。）
- **传播更改（别名是 `PropagateChange`）**。将该参数设置为 `TRUE`，以允许通过 Siebel 应用程序管理目录。然后，如果管理员在 Siebel 应用程序中添加用户或更改口令，或者用户更改口令或自行注册，所做的更改将传播到目录中。

注释：非 Siebel 安全适配器必须支持 `SetUserInfo` 和 `ChangePassword` 方法，以允许动态管理目录。
- **角色属性类型（别名是 `RolesAttributeType`）**。指定存储在目录中的角色的属性类型。例如，如果 `RolesAttributeType = roles`，在验证用户名为 HKIM 的用户时，安全适配器从 HKIM 的角色属性中检索用户的 Siebel 职责。

职责通常与 Siebel 数据库中的用户关联，但是它们可以存储在数据库或目录中，或者在两个地点同时存储。用户有权访问在这两个来源中指定的所有职责中的所有视图。然而，建议您在数据库或目录中定义职责，而不要同时在两个地点定义职责。

有关详细信息，请参阅第 119 页的“配置在目录中定义的角色”。
- **安全适配器 DLL 名称（别名是 `SecAdptDllName`）**。指定用于实施与 Siebel eBusiness Applications 集成所需的安全适配器 API 的 DLL。不需要明确指定文件扩展名。例如，`sscfdap.dll` 在 Windows 实施中实施 LDAP 安全适配器。在支持的 UNIX 平台上，文件名可能是 `libsscfdap.so` 或 `libsscfdap.sl`。如果 LDAP 安全适配器的 DLL 名称用于 UNIX 实施中，则在内部将其转换为实际的文件名。

- **服务器名称**（别名是 **ServerName**）。指定运行 LDAP 或 ADS 服务器的机器名称，例如 `ldapserversiebel.com`。

注释：如果是 ADSI，则必须在此参数中填入 ADS 服务器的完整机器名称，而不是填入其 IP 地址，否则，用户将无法通过 Siebel 应用程序更改自己的口令。此限制的产生是因为对 ADSI 安全适配器使用的 ADSI 客户机库进行限制。

- **共享证书 DN**（别名是 **SharedCredentialsDN**）。指定目录中对象的绝对路径（不是相对于 BaseDN 的路径），并且该对象具有共享的应用程序数据库帐户。如果该参数为空，则可以照常在用户的 DN 中查找数据库帐户。如果该参数不为空，则在共享证书 DN 中查找所有用户的数据库帐户。属性类型仍然由 `CredentialsAttributeType` 决定。

例如，如果 `SharedCredentialsDN = "uid=HKIM, ou=People, o=siebel.com"`，在验证用户时，安全适配器将从 HKIM 记录的相应属性中检索数据库帐户。该参数的缺省值是一个空白字符串。

- **Siebel 用户名属性类型**（别名是 **SiebelUsernameAttributeType**）。如果 `UseAdapterUsername = TRUE`，该参数是指安全适配器检索已验证用户的 Siebel 用户 ID 所依据的属性。如果该参数留空，则假定传入的用户名是 Siebel 用户 ID。
- **单一登录**（别名是 **SingleSignOn**）。(TRUE 或 FALSE) 如果是 TRUE，则在 Web SSO 模式下使用安全适配器，而不是使用安全适配器验证。
- **SSL 数据库**（别名是 **SslDatabase**）。指定 LDAP 安全适配器与目录之间的通讯是否使用安全套接层 (SSL)。如果该参数留空，则不使用 SSL。如果该参数不为空，其值必须是 `ldapkey.kdb` 文件的绝对路径。该文件由 IBM GSK iKeyMan 生成，它包含 LDAP 服务器使用的认证机构发行的认证。
- **信任标记**（别名是 **TrustToken**）。仅适用于 Web SSO 环境。适配器将请求中提供的 `TrustToken` 值与应用程序配置文件中存储的值进行比较。如果两个值相匹配，AOM 则承认请求来自 SWSE（即信任的 Web 服务器）。该参数的缺省值是一个空白字符串。
- **使用适配器定义的用户名**（别名是 **UseAdapterUsername**）。(TRUE 或 FALSE) 如果是 TRUE，该参数表示在传递给安全适配器的用户密钥不是 Siebel 用户 ID 时，安全适配器从 `SiebelUsernameAttributeType` 参数定义的属性中检索已验证用户的 Siebel 用户 ID。`UseAdapterUsername` 的缺省值是 FALSE。
- **用户口令散列算法**（别名是 **HashAlgorithm**）。如果 `HashUserPwd` 是 TRUE，或者 `HashDBPwd` 是 TRUE，请指定要使用的口令散列算法。缺省值是 RSASHA1，它使用 RSA SHA-1 算法提供口令散列处理。SIEBELHASH 值指定由 Siebel Systems 的杂乱算法提供的口令散列机制（只对现有客户支持）。有关详细信息，请参阅第 109 页的“配置口令散列处理”。
- **用户名属性类型**（别名是 **UsernameAttributeType**）。指定属性类型，用户的登录名将以该属性类型存储在目录中。例如，如果 `UsernameAttributeType = uid`，在用户名为 HKIM 的用户尝试登录时，安全适配器将搜索 uid 属性包含 HKIM 值的记录。除非 `UseAdapterUsername` 参数为 TRUE，否则该属性是 Siebel 用户 ID。

注释：如果您实施适配器定义的用户名 (`UseAdapterUsername = TRUE`)，则必须相应地设置 OM - 用户名 BC 字段参数，以允许从 Siebel 客户机更新 `UsernameAttributeType` 定义的目录属性。有关实施适配器定义的用户名的详细信息，请参阅第 117 页的“配置适配器定义的用户名”。

定制的安全适配器验证的参数

以下参数只适用于定制的安全适配器验证，并且为指定子系统 InfraSecAdpt_Custom 进行定义：

- **配置文件名**（别名是 **ConfigFileName**）。指定包含定制的安全适配器配置参数的文件名。这些设置不同于在本节中定义的那些设置。
- **Config 部分名称**（别名是 **ConfigSectionName**）。在使用 ConfigFileName 参数指定的文件中，指定包含定制的安全适配器配置设置的部分名称。

以下参数适用于定制的安全适配器验证，并且为指定子系统 InfraSecAdpt_Custom 进行定义。有关这些参数的详细信息，请参阅适用于 LDAP/ADSI 安全适配器的类似参数的说明，这在第 251 页的“Siebel 网关名称服务器参数”中有介绍。

- **CRC**（别名是 **CustomSecAdpt_CRC**）
- **散列数据库证书**（别名是 **CustomSecAdpt_HashDBPwd**）
- **散列用户口令**（别名是 **CustomSecAdpt_HashUserPwd**）
- **传播更改**（别名是 **CustomSecAdpt_PropagateChange**）
- **安全适配器 DII 名称**（别名是 **CustomSecAdpt_SecAdptDIName**）
- **单一登录**（别名是 **CustomSecAdpt_SingleSignOn**）
- **信任标记**（别名是 **CustomSecAdpt_TrustToken**）
- **使用适配器定义的用户名**（别名是 **CustomSecAdpt_UseAdapterUsername**）
- **用户口令散列算法**（别名是 **CustomSecAdpt_HashAlgorithm**）

AOM 的参数

以下是为 Enterprise、Siebel 服务器或 AOM 组件定义的参数：

- **OM - 代理雇员**（别名是 **ProxyEmployee**）。代理雇员的用户 ID。
有关代理雇员的信息，请参阅第 261 页的“Seed 数据”。
- **OM - 用户名 BC 字段**（别名是 **UsernameBCField**）。只有实施适配器定义的用户名才能使用该参数。它指定用户业务组件的字段，并在由应用程序配置文件的 UsernameAttributeType 参数定义的目录中填入属性。也就是说，在用户 ID（用户业务组件中的登录名字段）不是识别密钥时，该字段就是。如果该参数没有出现在参数列表中，您必须进行添加。
有关信息，请参阅第 117 页的“配置适配器定义的用户名”。

Siebel 应用程序配置文件参数

每种语言的每个 Siebel eBusiness Applications 都有一个配置文件。此文件中的参数确定用户如何与 AOM 以及安全适配器进行交互。

控制特定用户会话的配置文件取决于用户连接的客户机。

- **Siebel 服务器上的配置文件。**如果用户通过标准 Siebel Web 客户机进行连接，应用程序配置文件位于 `SIEBSVR_ROOT\bin\LANGUAGE` 子目录中。例如，`SIEBSVR_ROOT\bin\ENU` 目录中提供的 `eservice.cfg` 文件是为了实施美国英语的 Siebel eService。

注释：大多数适用于 Siebel 服务器（因而也适用于 Siebel Web 客户机）并且与安全有关的参数存储在名称服务器中。配置文件的 [SWE] 部分中的参数适用于 Siebel 服务器。然而，本节介绍的其它大多数参数不适用于 Siebel 服务器。

- **Siebel 移动 Web 客户机或专用 Web 客户机上的配置文件。**如果用户通过 Siebel 移动 Web 客户机或专用 Web 客户机进行连接，配置文件则位于客户机的 `SIEBEL_CLIENT_ROOT\bin\LANGUAGE` 子目录中。例如，`SIEBEL_CLIENT_ROOT\bin\ENU` 目录中提供的 `eservice.cfg` 是为了实施美国英语的 Siebel eService。

- Siebel 移动 Web 客户机直接连接至本地数据库；它绕过 Siebel 服务器。
- Siebel 专用 Web 客户机直接连接至服务器数据库；它绕过 Siebel 服务器。

注释：LDAP/ADSI 安全适配器配置不适用于 Siebel 移动 Web 客户机。

有关处理配置文件的详细信息，请参阅 *Siebel System Administration Guide*。

在提供的配置文件中，缺省情况下有些参数可能不会出现。其它参数在出现时前面可能带有分号 (;)，表示该参数是注释，不会进行解释。您必须删除分号才能使参数生效。在您重新启动 Siebel 服务器或 Siebel 客户机之前，对应用程序配置文件所做的更改不会生效。

警告：您为 Siebel LDAP 和 ADSI 安全适配器提供的参考目录属性的参数值区分大小写。该值必须与目录中的属性名称相匹配。

以下参数是与验证有关的参数，这些参数在缺省情况下显示，并且可以添加到每个应用程序的配置文件中。它们按出现时所在的标记部分分组。该列表不包括应用程序配置文件中与验证无关的参数。

[SWE] 部分中的参数

以下参数位于应用程序配置文件的 [SWE] 部分中。这些参数适用于所有 Siebel 客户机类型。

- **AllowAnonUsers。**(TRUE 或 FALSE) 如果该参数值是 FALSE，则不允许未注册的用户访问该 Siebel 应用程序。
- **SecureLogin。**(TRUE 或 FALSE) 如果是 TRUE，用户填写的登录表单将通过安全套接层 (SSL) 传输。这要求在安装 Siebel Web 引擎的 Web 服务器上具有认证机构发行的认证。
- **SecureBrowse。**如果 SecureBrowse 设置为 TRUE，则通过 SSL 导航应用程序中的所有视图。如果 SecureBrowse 设置为 FALSE，则通过 SSL 导航应用程序中安全属性设置为 TRUE 的视图。

警告：Siebel 客户应用程序支持在安全视图与非安全视图之间切换，但是雇员应用程序（例如 Siebel Call Center）不支持这种切换。有关详细信息，请参阅第 139 页的“配置安全视图”。

有关视图安全属性的信息，请参阅 *Configuring Siebel eBusiness Applications*。

[InfraSecMgr] 部分中的参数

以下参数位于应用程序配置文件的 [InfraSecMgr] 部分中。

注释： 这些参数只适用于 Siebel 移动 Web 客户机和专用 Web 客户机。如果是 SecAdptMode 和 SecAdptName，请参阅第 251 页的“Siebel 网关名称服务器参数”中等效参数的说明。

■ SecAdptMode。指定安全适配器模式。

- 如果是数据库验证，请指定 DB。（DB 是 SecAdptMode 的缺省值。）
- 如果是 LDAP 验证，请指定 LDAP。
- 如果是 ADSI 验证，请指定 ADSI。
- 如果是定制的安全适配器，请指定 CUSTOM。

■ SecAdptName。指定安全适配器的名称。

- 如果是数据库验证，请指定 DBSecAdpt。如果是移动或专用 Web 客户机配置，请在配置文件中创建 [DBSecAdpt] 部分。（DBSecAdpt 是 SecAdptName 的缺省值。）
- 如果是 LDAP 验证，请指定 LDAPSecAdpt（或者您选择的其它名称）。如果是专用 Web 客户机配置，并且您使用 LDAP/ADSI 配置实用程序配置了 LDAP，缺省情况下在配置文件中创建 [LDAPSecAdpt] 部分。
- 如果是 ADSI 验证，请指定 ADSISecAdpt（或者您选择的其它名称）。如果是专用 Web 客户机配置，并且您使用 LDAP/ADSI 配置实用程序配置了 ADSI，缺省情况下在配置文件中创建 [ADSIAdpt] 部分。
- 如果是定制的安全适配器，请指定一个名称，例如 SecAdpt_Custom。（您必须在文件中添加适用部分。）

注释： 如果您实施定制的非 Siebel 安全适配器，并且要使用这些参数，则必须将您的适配器配置为解释 Siebel 适配器使用的参数。

以下参数只适用于 Siebel 专用 Web 客户机：

■ UseRemoteConfig。指定只包含安全适配器参数的配置文件路径，也就是说，它包含参数的方式就仿佛这些参数包括在应用程序配置文件的 [LDAPSecAdpt] 等部分中将要格式化一样。

您必须提供以通用命名惯例 (UNC) 格式表示的路径，例如，类似于 \\server\vol\path\ldap_remote.cfg 的形式。

有关使用该参数的详细信息，请参阅第 120 页的“安全适配器和 Siebel 专用 Web 客户机”。

[DBSecAdpt] 部分中的参数

如果您要配置数据库安全适配器，以下参数位于应用程序配置文件的 [DBSecAdpt] 部分（或等效部分）中。应用程序配置文件中与验证有关的每个参数由用于执行数据库验证的安全适配器进行解释。

注释：这些参数只适用于 Siebel 移动 Web 客户机和专用 Web 客户机。有关详细信息，请参阅适用于 Siebel Web 客户机和其它验证上下文的等效参数的说明，这在第 251 页的“Siebel 网关名称服务器参数”中有介绍。

- **DBSecAdpt_CRC**。使用该参数实施 checksum 验证，以验证每位用户通过正确的安全适配器获得对数据库的访问权限。该参数包含 checksum 实用程序为适用的安全适配器 DLL 计算的值。如果您将该值留空，系统则不执行检查。如果您升级系统，则必须重新计算并替换该参数中的值。

有关详细信息，请参阅第 115 页的“配置 Checksum 验证”。

- **DBSecAdpt_PropagateChange**。将该参数设置为 TRUE，以允许通过 Siebel 应用程序管理数据库中的证书。然后，如果管理员在 Siebel 应用程序中添加用户或更改口令，或者用户更改口令或自行注册，所做的更改将传播到数据库中。

对于 Siebel 专用 Web 客户机，系统首选项 SecThickClientExtAuthent 也必须设置为 TRUE。有关详细信息，请参阅第 260 页的“系统首选项”。

- **DBSecAdpt_SecAdptDllName**。指定用于实施与 Siebel eBusiness Applications 集成所需的安全适配器 API 的 DLL。不需要明确指定文件扩展名。例如，sscsadb.dll 在 Windows 实施中实施数据库安全适配器。
- **DataSourceName**。指定适用于所指定数据库安全适配器的数据来源。

数据来源部分中的参数

以下参数位于应用程序配置文件的数据来源部分中，例如，[ServerDataSrc]（适用于 Siebel 专用 Web 客户机）或 [Local]（适用于 Siebel 移动 Web 客户机）。

- **DSHashAlgorithm**。如果 DSHashUserPwd 是 TRUE，则指定要使用的口令散列算法。缺省值是 RSASHA1，它使用 RSA SHA-1 算法提供口令散列处理。SIEBELHASH 值指定由 Siebel Systems 的杂乱算法提供的口令散列机制（只对现有客户支持）。有关详细信息，请参阅第 109 页的“配置口令散列处理”。
- **DSHashUserPwd**。为用户口令指定口令散列处理。请使用通过 DSHashAlgorithm 参数指定的散列算法。有关详细信息，请参阅第 109 页的“配置口令散列处理”。
- **IntegratedSecurity**。只适用于使用 Oracle 或 Microsoft SQL Server 数据库的 Siebel 专用 Web 客户机。有关详细信息，请参阅第 120 页的“安全适配器和 Siebel 专用 Web 客户机”。

[LDAPSecAdpt] 或 [ADSISecAdpt] 节中的参数

根据您是要配置 LDAP 安全适配器还是 ADSI 安全适配器，以下参数位于应用程序配置文件的 [LDAPSecAdpt] 或 [ADSISecAdpt] 部分（或等效部分）中。应用程序配置文件中每个与验证相关的参数均通过安全适配器进行解释（适用于 LDAP 或 ADSI 验证）。

有些参数仅适用于 LDAP 实施，或者仅适用于 ADSI 实施。有些参数仅适用于 Web SSO 验证环境。

LDAP 和 ADSI 验证不适用于 Siebel 移动 Web 客户机。

以下参数还适用于 Siebel 专用 Web 客户机。有关详细信息，请参阅适用于 Siebel Web 客户机和其它验证上下文的等效参数的说明，这在第 251 页的“[Siebel 网关名称服务器参数](#)”中有介绍。

- **ApplicationPassword**
- **ApplicationUser**
- **BaseDN**
- **CRC**
- **CredentialsAttributeType**
- **HashAlgorithm**
- **HashDBPwd**
- **HashUserPwd**
- **PasswordAttributeType**
- **PasswordExpireWarnDays**
- **Port**
- **PropagateChange**
- **RolesAttributeType**
- **SecAdptDllName**
- **ServerName**
- **SharedCredentialsDN**
- **SiebelUsernameAttributeType**
- **SingleSignOn**
- **SslDatabase**
- **TrustToken**
- **UseAdapterUsername**
- **UsernameAttributeType**

系统首选项

在“管理 - 应用程序”屏幕中，您可以为 Siebel 应用程序设置与验证有关的系统首选项。系统首选项是在整个 Enterprise 使用的设置。

下面是与验证有关的系统首选项：

- **SecThickClientExtAuthent**。（TRUE 或 FALSE）为了允许对通过 Siebel 专用 Web 客户机登录的用户执行安全适配器验证，您必须将 SecThickClientExtAuthent 系统首选项设置为 TRUE。该系统首选项对通过 Siebel Web 客户机登录的用户执行安全适配器验证没有任何影响。

要编辑系统首选项

- 1 以管理员身份登录到 Siebel 雇员应用程序。
- 2 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 应用程序”>“系统首选项”。
- 3 在“系统首选项”列表中，选择要编辑的系统首选项。
- 4 编辑“系统首选项值”列中的录入值，然后提交记录。
- 5 重新启动 Siebel 服务器。



Seed 数据

本附录介绍了为 Siebel eBusiness Applications 提供并与本指南中的内容相关的 seed 数据，并且提供了有关如何使用该数据的信息。它包括以下主题：

- 第 261 页的 “Seed 雇员”
- 第 262 页的 “Seed 用户”
- 第 262 页的 “Seed 职责”
- 第 263 页的 “Seed 职位和组织”
- 第 263 页的 “Seed 数据库登录”

注释：在本附录的表中，术语“客户应用程序”表示 Siebel eSales、Siebel eService、Siebel eCustomer、Siebel Training、Siebel Events 和 Siebel eMarketing 的组合。

Seed 雇员

雇员记录在安装时作为 seed 数据提供，这在第 261 页的表 24 中有介绍。该记录没有数据库登录或职责，但是与其他雇员一样，它具有职位和组织。

客户用户（例如 Siebel eService 用户）没有分配到自己的职位或组织。在客户用户登录时，应用程序会按照编程将代理雇员与该用户关联。代理雇员将提供下列功能：

- 将用户随后创建的数据与代理雇员的组织关联，从而允许这些数据显示在实施组织访问控制的视图中。
- 用户可以在实施组织访问控制的视图中看到自己以及其他用户创建的数据。

代理雇员在应用程序级别作为一个名称服务器参数指定。

有关将代理雇员与应用程序关联的信息，请参阅第 251 页的“Siebel 网关名称服务器参数”。

有关组织访问控制的信息，请参阅第 185 页的“访问控制机制”。

表 24. 代理雇员 seed 数据字段值

姓氏	名字	用户 ID	职责	职位	组织
代理	雇员	PROXYE	无	代理雇员	缺省组织

Seed 用户

第 262 页的表 25 介绍了作为 seed 数据提供的非雇员用户记录。

表 25. 用户 seed 数据字段值

姓氏	名字	用户 ID	职责	新职责	供这些应用程序使用
客户	来宾	GUESTCST	Web 匿名用户	Web 注册用户	客户应用程序
渠道合作者	来宾	GUESTCP	未注册的合作者代理	自行注册的合作者代理	Siebel Partner Portal

Seed 职责

职责记录作为 seed 数据提供，这在第 262 页的表 26 中有介绍。为 seed 数据“用户”记录提供的职责允许用户查看供匿名浏览的视图，包括用户可从中执行自行注册或登录的视图。其它职责则按照编程分配给自行注册的用户，或者由内部管理员或授权管理员手动分配给用户。

注释：有关 seed 数据中提供的所有职责，请参阅 Siebel 应用程序中列出的那些职责。

表 26. 职责 Seed 数据

名称	组织	说明	供这些应用程序使用
Web 匿名用户	缺省组织	为匿名浏览提供的视图	客户应用程序
Web 注册用户	缺省组织	为典型的注册用户提供的视图	客户应用程序
Web 授权客户管理员	缺省组织	包括 Web 注册用户职责中的视图以及用于管理用户的视图	客户应用程序
Web 公司用户	缺省组织	eSales 公司用户的视图	eSales
Web 采购经理	缺省组织	eSales 采购经理的视图	eSales
未注册的合作者代理	缺省组织	为匿名浏览提供的视图	Siebel Partner Portal
自行注册的合作者代理	缺省组织	为自行注册的用户提供的一组数量有限的视图	Siebel Partner Portal
合作者关系经理	缺省组织	Siebel Partner Portal 的合作者关系经理的视图	Siebel Partner Portal
合作者操作经理	缺省组织	Siebel Partner Portal 的合作者操作经理的视图，包括用于管理用户的视图	Siebel Partner Portal
合作者销售经理	缺省组织	Siebel Partner Portal 的合作者销售经理的视图	Siebel Partner Portal
合作者销售代表	缺省组织	Siebel Partner Portal 的合作者销售代表的视图	Siebel Partner Portal

表 26. 职责 Seed 数据

名称	组织	说明	供这些应用程序使用
合作者服务经理	缺省组织	Siebel Partner Portal 的合作者服务经理的视图	Siebel Partner Portal
合作者服务代表	缺省组织	Siebel Partner Portal 的合作者服务代表的视图	Siebel Partner Portal
注册的客户 - 无线	缺省组织	为使用无线设备的已注册 eService 用户提供的视图	eService
Web 培训经理	缺省组织	允许管理员查看他或她的直属下司的课程和课程表注册信息的视图	Training
培训管理员	缺省组织	用于允许管理课程和注册人的视图	Training

要查看职责中包括的视图

- 1 从应用程序级菜单中，选择“导航”>“场地图”>“管理 - 应用程序”>“职责”。
- 2 在“职责”列表中，选择一个职责。

此时职责的视图出现在“视图”列表中。

Seed 职位和组织

代理雇员职位和缺省组织部门记录作为 seed 数据提供。该职位位于部门中，而部门是它本身的组织。职位和部门都被分配给 seed 数据“雇员”记录。

Seed 数据库登录

数据库登录作为 seed 数据提供。它专门用于通过外部验证系统登录的所有用户，并且您不应该将其分配给任何个人用户。登录证书为登录 = LDAPUSER，口令 = LDAPUSER。

警告：强烈建议管理员更改此口令。

D

Siebel Financial Services 的附录

本附录介绍了在 Siebel Financial Services 应用程序中实施用户验证、用户管理和基本访问控制与本手册其它章节中介绍的实施有何不同。它包括以下主题：

- 第 265 页的 “Siebel Financial Services 应用程序”
- 第 266 页的 “Siebel Financial Services 的用户验证”
- 第 268 页的 “注册和管理 Siebel Financial Services 的用户”
- 第 271 页的 “Siebel Financial Services 的基本访问控制”
- 第 273 页的 “Siebel Financial Services 应用程序的配置文件名”
- 第 274 页的 “Siebel Financial Services 的 seed 数据”

Siebel Financial Services 应用程序

在第 265 页的表 27 中列出的应用程序是特定于 Siebel Financial Services 应用程序的应用程序，或者是其功能适用于 Siebel Financial Services 的应用程序。应用程序按照它们在 Siebel Tools 中使用的名称列出。

对于一些应用程序，表中还列出了一些选项，这些选项与功能模块一起，共同决定了为您授权的屏幕和视图。某个应用程序可能被一个或多个产品名称引用，引用此应用程序的产品列在“产品”列中。信息被分成雇员、合作者和客户应用程序三大类。

表 27. Siebel Financial Services 应用程序

Tools 应用程序对象名称	用户	选项	产品
Siebel Financial Services	雇员	Siebel Sales	Siebel Finance
		Siebel Service	Siebel Insurance
		Siebel Call Center	Siebel Healthcare
		Siebel 合作者管理器	
Siebel Financial Services ERM	雇员		Siebel 雇员关系管理
Siebel Financial Services Marketing	雇员	仅限于 Siebel Marketing	Siebel Finance
			Siebel Insurance
			Siebel Healthcare

表 27. Siebel Financial Services 应用程序

Tools 应用程序对象名称	用户	选项	产品
Siebel Financial Partner Relationship Management (PRM)	合作者		Siebel PRM for Finance Siebel Agent Portal Siebel Healthcare Group Portal Siebel Healthcare Provider Portal
Siebel eBanking	客户		Siebel eBanking
Siebel Financial eBrokerage	客户		Siebel eBrokerage
Siebel Financial eService	客户		Siebel Insurance/Healthcare eService Siebel Healthcare Member Portal
Siebel Financial eEnrollment	客户		Siebel Healthcare Enrollment Portal
Siebel FINS eSales	客户		Siebel eSales
Siebel Financial eCustomer	客户		Siebel eCustomer
Siebel eEvents Management	客户		Siebel Events Manager for Finance

注释： Siebel Healthcare Group Portal 用作一个客户产品；也就是说，用户通常是您的客户。从技术角度来看，Siebel Healthcare Group Portal 是 Siebel Financial 合作者应用程序的一个产品标签。与客户应用程序的用户不同的是，您向用户提供他们自己的职位和组织。

Siebel Financial Services 的用户验证

本节包含了 Siebel Financial Services 应用程序的信息，这些信息不同于本指南其它章节中的信息或其它证明中提到的信息。

LDAP 和 ADSI 安全适配器验证

如果您要实施用户的自行注册或外部管理，安全适配器验证是先决条件。然而，并非所有的 Siebel 应用程序都将用户的自行注册和外部管理作为缺省功能提供。

有关该组中将用户的自行注册和外部管理作为缺省功能提供的应用程序的信息，请参阅第 268 页的“注册和管理 Siebel Financial Services 的用户”。

实施 LDAP 和 ADSI 安全适配器验证

为 Siebel Financial Services 应用程序实施 LDAP/ADSI 安全适配器验证与在本指南其它章节中介绍的信息相同，但存在以下例外。

Siebel Financial Services 应用程序的参数主要列在 eapps_fins.cfg 文件中，而按照本指南其它章节中的介绍，eapps.cfg 文件也包括在内。eapps.cfg 文件具有一个包括行，它指向 eapps_fins.cfg 文件。本节中所有提到 eapps.cfg 文件之处都应该替换为 eapps.cfg 文件和 eapps_fins.cfg 文件。

设置安全适配器验证：方案

分配给 seed 匿名用户 GUESTCST 的此职责和新职责专门用于 Siebel Financial Services 客户应用程序。这些职责不同于为非特定于财务服务的 Siebel 客户应用程序用户 GUESTCST 分配的职责，这些应用程序在本指南其它章节中也有介绍。

如果您在部署任何其它 Siebel Financial Services 客户应用程序的同时还部署了 Siebel Events Manager for Finance 或非特定于财务服务的 Siebel 客户应用程序，则必须创建单独的匿名用户。

该新匿名用户用于 Siebel Events Manager for Finance 以及非特定于财务服务的 Siebel 客户应用程序，即在本指南其它章节中介绍的应用程序。请按照第 261 页的“Seed 数据”中介绍的 GUESTCST 职责，为该匿名用户分配职责。

如果在数据库中添加 TESTUSER，则应当在“职责”和“新职责”字段中，为所设置应用程序的典型注册用户输入相应的职责。有关为特定规范提供的 seed 职责的信息，请参阅第 274 页的“Siebel Financial Services 的 seed 数据”和第 261 页的“Seed 数据”。

实施 Web SSO 验证

为 Siebel Financial Services 应用程序实施 Web SSO 验证与在本指南其它章节中介绍的信息相同，但存在以下例外。

Siebel Financial Services 应用程序的参数主要列在 eapps_fins.cfg 文件中，而按照本指南其它章节中的介绍，eapps.cfg 文件也包括在内。eapps.cfg 文件具有一个包括行，它指向 eapps_fins.cfg 文件。本节中所有提到 eapps.cfg 文件之处都应该替换为 eapps.cfg 文件和 eapps_fins.cfg 文件。

设置 Web SSO：方案

分配给 seed 匿名用户 GUESTCST 的此职责和新职责专门用于 Siebel Financial Services 客户应用程序。这些职责不同于为非特定于财务服务的 Siebel 客户应用程序用户 GUESTCST 分配的职责，这些应用程序在本指南其它章节中也有介绍。

如果您在部署任何其它 Siebel Financial Services 客户应用程序的同时还部署了 Siebel Events Manager for Finance 或非特定于财务服务的 Siebel 客户应用程序，则必须创建单独的匿名用户。

该新匿名用户用于 Siebel Events Manager for Finance 以及非特定于财务服务的 Siebel 客户应用程序，即在本指南其它章节中介绍的应用程序。请按照第 261 页的“Seed 数据”中介绍的 GUESTCST 职责，为该匿名用户分配职责。

如果在数据库中添加 TESTUSER，则应当在“职责”和“新职责”字段中，为所设置应用程序的典型注册用户输入相应的职责。有关为特定规范提供的 seed 职责的信息，请参阅第 274 页的“Siebel Financial Services 的 seed 数据”和第 261 页的“Seed 数据”。

eapps.cfg 和 eapps_fins.cfg 文件中的参数

除 eapps.cfg 文件之外，Siebel Web 引擎还使用 eapps_fins.cfg 文件控制 Siebel Financial Services 应用程序与 Siebel Web 引擎之间的交互。用于定义应用程序对象管理器 (AOM) 和应用程序验证参数的部分只出现一次，它可能出现在 eapps.cfg 文件或 eapps_fins.cfg 文件中。

第 268 页的表 28 列出了 eapps.cfg 文件和 eapps_fins.cfg 文件中的部分，它们适用于 Siebel Financial Services 应用程序。

表 28. eapps.cfg 文件和 eapps_fins.cfg 文件中的部分

Tools 应用程序对象名称	eapps.cfg 中的部分	eapps_fins.cfg 中的部分
Siebel Financial Services		[/fins]
Siebel Financial Services ERM		[/finserm]
Siebel Marketing	[/marketing]	
Siebel Financial PRM		[/finsechannel]
Siebel eBanking		[/finsebanking]
Siebel Financial eBrokerage		[/finsebrokerage]
Siebel Financial eService		[/finseservice]
Siebel Financial eEnrollment		[/finseenrollment]
Siebel FINS eSales		[/finsesales]
Siebel Financial eCustomer		[/finsecustomer]
Siebel eEvents for Finance	[/eevents]	

Siebel 应用程序配置文件参数

有关特定应用程序的应用程序配置文件名称，请参阅第 273 页的“Siebel Financial Services 应用程序的配置文件名”。

注册和管理 Siebel Financial Services 的用户

本节包含 Siebel Financial Services 应用程序的信息，这些信息不同于本指南其它章节中有关注册和管理用户的小节中的信息，也不同于其它证明中提到的信息。

Seed 数据

分配给 seed 用户 GUESTCST 的此职责和新职责专门用于 Siebel Financial Services 客户应用程序。这些职责不同于为非特定于财务服务的 Siebel 客户应用程序用户 GUESTCST 分配的职责，这些应用程序在本指南其它章节中也有介绍。

如果您在部署任何其它 Siebel Financial Services 客户应用程序的同时还部署了 Siebel Events Manager for Finance 或非特定于财务服务的 Siebel 客户应用程序，则必须创建单独的匿名用户。该新匿名用户用于 Siebel Events Manager for Finance 以及非特定于财务服务的 Siebel 客户应用程序，即在本指南其它章节中介绍的应用程序。请按照第 261 页的“Seed 数据”中介绍的 GUESTCST 职责，为该匿名用户分配职责。

有关特定于 Siebel Financial Services 应用程序的 seed 数据的信息，请参阅第 274 页的“Siebel Financial Services 的 seed 数据”。

未注册的用户和匿名浏览

匿名浏览是以下 Siebel Financial Services 应用程序的缺省功能：

- Siebel 雇员关系管理
- Siebel Events Manager for Finance
- Siebel Finance PRM
- Siebel eBanking
- Siebel eBrokerage
- Siebel Finance eSales
- Siebel Healthcare Enrollment Portal

除作为匿名用户提供的 GUESTCST 和 GUESTCP seed 用户记录之外，还提供了用户 ID 为 GUESTERM 的 seed 用户记录作为 Siebel Financial Services ERM 的匿名用户。

有关特定于 Siebel Financial Services 应用程序的 seed 数据的信息，请参阅第 274 页的“Siebel Financial Services 的 seed 数据”。

自行注册

用户自行注册是以下所列 Siebel Financial Services 应用程序的缺省功能。

注释：尽管自行注册是作为一些 Siebel Financial Services 应用程序的缺省功能提供，但是，在行业中由用户自行注册财务服务并不常见。更为常见的是，内部管理员使用 Siebel Financial Services 应用程序注册用户。

- Siebel Finance PRM
- Siebel Events Manager for Finance
- Siebel eBanking
- Siebel eBrokerage
- Siebel Finance eSales

用户可以在 Siebel Finance PRM 中作为公司或个人自行注册。通过自行注册，用户请求成为一个合作者或者成为一个潜在合作者。

内部管理员使用 Siebel Finance 中的“管理 - 合作者”屏幕，将潜在合作者提升为批准合作者，然后提升为注册合作者。

有关使用“管理 - 合作者”屏幕的信息，请参阅 *Siebel Partner Relationship Management Administration Guide*。

内部管理用户

Siebel Financial Services 应用程序的用户内部管理与本指南其它章节中介绍的信息相同，但存在以下例外。

添加新的合作者用户

您可以在 Siebel Financial Services 的“管理 - 合作者”屏幕中管理合作者用户。

有关使用“管理 - 合作者”屏幕的信息，请参阅 *Siebel Partner Relationship Management Administration Guide*。

用户的外部管理

授权管理是 Siebel Financial PRM 的缺省功能。

注释：尽管授权管理是作为 Siebel Financial PRM 的缺省功能提供，但是，在财务行业中由外部管理员注册客户或合作者用户并不常见。更为常见的是，内部管理员使用 Siebel Financial Services 应用程序注册用户。

访问注意事项

在第 261 页的“Seed 数据”中介绍了为授权管理员提供用户管理视图的 seed 职责。授权管理员的 seed 职责未包括特定于 Siebel Financial Services 应用程序的视图。要使授权管理员可以访问适当的财务服务视图和用户管理视图，则必须通过以下方式之一为授权管理员分配职责：

- 至少为授权管理员分配两个 seed 职责 — 一个适用于 Siebel 应用程序的普通用户，另一个则为适用于应用程序的授权管理员的适当职责。
- 创建单一职责，此职责包括您希望授权管理员拥有的所有视图，然后将该职责分配给授权管理员。

有关为用户分配职责的信息，请参阅本指南其它章节中有关用户内部管理和外部管理的小节。

维护用户资料

为 Siebel Financial Services 应用程序维护用户资料与在本指南其它章节中介绍的信息相同，但存在以下例外。

编辑个人信息

用户可以单击“我的资料”或“我的客户”以访问“用户资料”表单，具体视 Siebel 客户应用程序而定。

Siebel Financial Services 的基本访问控制

Siebel Financial Services 应用程序实施基本访问控制的情况与本指南其它章节中介绍的信息相同，但存在以下例外。

访问控制机制

以下注释会影响对使用个人、职位或组织访问控制的任何视图中的“商机”的访问控制。

注释：如果核选商机的“安全”字段，对于应用个人、职位或组织访问控制的任何视图，只有该销售团队中的职位才具有对这些视图中商机的可视性。例如，在“全部商机”视图中，销售团队中的用户可以看到安全商机，但是同一个组织中的其他用户则无法看到。在“我的团队的商机”视图中，除非经理也在销售团队中，否则该经理无法看到其直属上司是主要项的安全商机。与安全商机相关的任何活动或事件同样也对不在该销售团队中的任何用户隐藏。

安全商机访问控制通过商机业务组件上的以下搜索规范提供：

```
[Secure Flag] = 'N' OR EXISTS([Sales Rep Id] = LoginId())
```

访问组访问控制

家庭也可以与其他当事方类型结合使用，以形成一个访问组。在所有访问控制上下文中，家庭应该包括在可作为访问组成员的当事方类型列表中。

管理访问组访问控制

访问组访问控制的管理与在本指南其它章节中介绍的信息相同，但存在以下例外。下面的小节是对关于管理各种当事方类型小节的补充。

将访问组与数据关联

将访问组与目录或类别关联的过程与本指南其它章节中介绍的信息不同。

将访问组与目录关联

通过将访问组与主数据的目录关联，您可以为访问组中的个人用户授予对此目录中数据的访问权限。

注释：要使目录及其所有子类别仅对与其关联的访问组可视，则必须设置目录的“私有”标志。

要将访问组与目录关联

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 目录” > “目录”。
此时将显示“目录”列表。
- 2 选择一个目录。
- 3 单击“访问组”视图选项卡。
此时将出现“访问组”列表，其中显示了与该目录关联的访问组。
- 4 在“访问组”列表中添加新记录。
此时将显示一个弹出列表，其中包含访问组。
- 5 选择访问组，然后单击“添加”。
此访问组将显示在“访问组”列表中。
- 6 请按照下表中提供的准则，为要添加的访问组填写以下字段，然后退出访问组记录以保存记录。

字段	准则
管理	设置该标志，以允许该访问组中的用户管理目录。
级联	设置该标志，以自动将该访问组与目录的后代类别（子类别、孙类别等等）关联。结果是该访问组中的用户有权访问后代类别中的数据。

您可以按此类似方式断开访问组与目录的关联。

将访问组与类别关联

通过将访问组与主数据的类别关联，您可以为访问组中的个人用户授予对此类别中数据的访问权限。

注释：要使类别及其所有子类别仅对与其关联的访问组可视，则必须设置类别的“私有”标志，或者必须设置作为此类别祖先的目录或类别的“私有”标志。

要将访问组与类别关联

- 1 从应用程序级菜单中，选择“导航” > “场地图” > “管理 - 目录” > “目录”。
此时将显示“目录”列表。
- 2 向下搜索到目录名称。
此时将显示目录的类别列表。
- 3 单击“访问组”视图选项卡。
- 4 在“访问组”列表中添加新记录。
此时将出现一个列出了访问组的多值组。

5 选择访问组，然后单击“添加”。

此访问组将显示在“访问组”列表中。

6 请按照提供的准则，为要添加的访问组填写以下字段，然后退出访问组记录以保存记录。

字段	准则
管理	设置该标志，以允许该访问组中的用户管理此类别。
级联	设置该标志，以自动将该访问组与此类别的后代类别（子类别、孙类别等等）关联。结果是该访问组中的用户有权访问后代类别中的数据。

您可以按此类似方式断开访问组与类别的关联。如果断开访问组与类别的关联，系统会自动断开该访问组与此类别的所有后代类别的关联。

Siebel Financial Services 应用程序的配置文件名

本节包含有关 Siebel Financial Services 应用程序的信息，这些信息不同于附录中包含本指南其它章节的 Siebel 应用程序配置文件名的信息，也不同于其它证明中提到的信息。

第 273 页的表 29 包含 Siebel Financial Services 应用程序使用的应用程序配置文件的名称。

表 29. Siebel Financial Services 应用程序配置文件名

Tools 应用程序对象名称	配置文件名
Siebel Financial Services	fins.cfg
Siebel Financial Services ERM	finserm.cfg
Siebel Financial Services Marketing	finsmarket.cfg
Siebel Financial PRM	finscw.cfg
Siebel eBanking	finsebanking.cfg
Siebel Financial eBrokerage	finsebrokerage.cfg
Siebel Financial eService	finseservice.cfg
Siebel Financial eEnrollment	finseenrollment.cfg
Siebel FINS eSales	finsesales.cfg
Siebel Financial eCustomer	finsecustomer.cfg
Siebel eEvents Management	eevents.cfg

Siebel Financial Services 的 seed 数据

本节包含 Siebel Financial Services 应用程序的信息，这些信息不同于第 261 页的“Seed 数据”中的信息或其它证明中提到的信息。

Siebel Financial Services 应用程序也提供了与用户访问有关的 seed 数据。

在本节中，术语“Siebel Financial Services 客户应用程序”代表的是第 265 页的表 27 中表示为客户应用程序的一个组。

Seed 用户

第 274 页的表 30 显示了对 Siebel Financial Services 应用程序提供的 seed 非雇员用户记录所做的修改。

GUESTCP seed 用户记录在第 261 页的“Seed 数据”中有介绍，它用作 Siebel Financial PRM 的匿名用户，Siebel Financial PRM 是 Siebel Financial Services 中的合作者应用程序。其职责是提供用于匿名浏览的视图，而其“新职责”字段中的职责则为自行注册的用户提供视图。

表 30. 用户 seed 数据字段值

姓氏	名字	用户 ID	职责	新职责	供这些应用程序使用
客户	来宾	GUESTCST	未注册的客户	注册的客户	Siebel Financial Services 客户应用程序
来宾	ERM	GUESTERM	ERM AnonUser		Siebel Financial Services ERM

Seed 职责

第 275 页的表 31 列出了 Siebel Financial Services 应用程序提供的附加 seed 职责。尽管 Siebel Financial Services 应用程序也提供了这些 seed 职责，但是，这些职责不包括特定于 Siebel Financial Services 应用程序的视图。

不存在为 Siebel Financial PRM 的注册合作者用户提供的附加 seed 职责。您必须根据注册合作者用户的各种业务角色为他们建立职责。您可以为合作者用户创建新职责，也可以复制并修改 seed 职责。

表 31. seed 职责

名称	组织	说明和注释	供这些应用程序使用
未注册的客户	缺省组织	为匿名浏览提供的视图。	Siebel Financial Services 客户应用程序，但不包括 Siebel Events Manager for Finance。 如果是 Siebel Events Manager for Finance，请改为使用 Web 匿名用户。
注册的客户		典型注册用户的视图。 请首先将缺省组织与该职责关联，然后将该职责分配给用户。	Siebel Financial Services 客户应用程序，但不包括 Siebel Events Manager for Finance。 如果是 Siebel Events Manager for Finance，请改为使用 Web 注册用户。
ERM AnonUser	缺省组织	为匿名浏览提供的视图。	Siebel Financial Services ERM。
ERM 用户	缺省组织	典型注册用户的视图。	Siebel Financial Services ERM。
ERM 经理	缺省组织	雇员管理视图。 除包含普通用户视图的职责之外，还应该为经理分配该职责。	Siebel Financial Services ERM。

有关创建和修改职责的信息，请参阅第 10 章“配置访问控制”。

索引

英文字母

Active Directory Server

请参阅 ADS

ADS

- ADS 服务器, 口令分配 130
- ADS 服务器, 设置 130
- ADS 服务器, 作为目录配置 130
- 口令存储和使用 70
- 目录, 用户管理建议 71

ADSI 安全适配器和 DNS 服务器 72

ADSI 标准, 安全适配器验证 69

ADSI 适配器

- ADSI 客户机的要求 72
- ApplicationPassword 参数 252
- Siebel Financial Services, 关于 266
- Siebel Financial Services, 实施 267
- 安全适配器流程概述 67
- 安全适配器验证, 实施 90
- 部署选项 113
- 部署选项, 列出 113
- 口令 70
- 授权的管理员, 可用性 172

ADSI 适配器, 设置方案

- 安装的先决条件 97
- 测试 106
- 重新启动服务器 106
- 关于实施 97
- 流程概述 97
- 名称服务器参数, 编辑 101
- 目录记录, 关于 99
- 配置文件参数, 使用准则 105
- 配置文件参数值, 表 101
- 数据库登录, 创建 98
- 验证目录, 创建 98
- 用户, 创建 99
- 用户记录, 添加 100

AllowAnonUsers 参数

- 关于 256
- 匿名浏览, 设置 149
- 为 LDAP 或 ADSI 设置 105
- 为 Web SSO 设置 136

AnonPassword 参数

- 关于 248
- 匿名浏览, 设置 149
- 为 LDAP 或 ADSI 设置 101
- 为 Web SSO 设置 133

AnonUserName 参数

- 关于 248
- 匿名浏览, 设置 149
- 为 LDAP 或 ADSI 设置 101
- 为 Web SSO 设置 133

ApplicationPassword 参数

- 关于 252
- 为 LDAP 或 ADSI 设置 104

ApplicationUser 参数

- 关于 252
- 为 LDAP 或 ADSI 设置 104

APPUSER 99

APPUSERPW 99

BaseDN 参数

- 关于 252
- 为 LDAP 或 ADSI 设置 103

CA 认证文件名参数 (CACertFileName) 51

CACertFileName 参数 51, 53, 250

CERT_SUBJECT 变量 249

CertFileName 参数 51, 53, 250

checksum 实用程序 115

- 验证, 设置 115

ClientCertificate 参数, 关于 248

cookie

- Siebel QuickStart 143, 145
- 会话 143
- 启用 146
- 自动登录 cookie 和 “记住我的用户 ID 和口令”
功能 141
- 自动登录证书 143

CRC 参数

- 关于 252

CredentialsAttributeType 参数

- 关于 253
- 为 LDAP 或 ADSI 设置 104

Crypto

请参阅 Microsoft Crypto 加密

CSSSWEFrameListVisibilityAssoc 类 229

CSSSWEFrameListVisibilityPick class 229

CSSSWEFrameUserRegistration 类 156, 158

DBO 口令, 更改 30

DBSecAdpt_CRC 参数, 关于 258

DBSecAdpt_SecAdptDllName 参数

- 关于 258

DoCompression 参数 38

- 关于 248

- eapps.cfg 文件**
 - 请参阅配置文件
- EncryptedPassword 参数** 32
- EncryptedPassword 参数, 关于** 33, 249
- EncryptSessionId 参数**
 - 关于 249
- EncryptSessionId 参数 (eapps.cfg 文件)** 144, 145
- encryptstring.exe** 33
- eservice.cfg 文件, LDAP 示例** 119
- FindContact 方法**
 - 输入字段, 添加或删除 165
 - 忘记口令, 修改 163
- GUESTCP 用户 ID** 262
- GUESTCST 用户 ID** 262
- GUESTPW** 99
- GuestSessionTimeout 参数**
 - 关于 249
- HTTP 1.1 协议** 38
- IBM Directory Server** 19
- IBM GSK iKeyMan, 安装** 72
- IBM GSKit, 安装** 72
- IBM HTTP Server** 19
- IBM LDAP Client, 安装** 72
- IIS Web 服务器, 配置** 131
- IIS 管理服务, 重新启动** 136
- IntegratedDomainAuth 参数**
 - 关于 250
 - 为 Web SSO 设置 134
- IntegratedSecurity 参数** 120
- keyfile 口令, 更改** 60
- KeyFileName 参数** 51, 54
- KeyFilePassword 参数** 51, 54, 250
- LDAP 适配器**
 - ApplicationPassword 参数 252
 - Siebel Financial Services, 关于 266
 - Siebel Financial Services, 实施 267
 - SsIDatabase 参数 254
 - 安全适配器流程概述 67
 - 安全适配器验证 69
 - 安全适配器验证, 实施 90
 - 部署选项 113
 - 授权的管理员, 可用性 172
- LDAP 适配器, 设置方案**
 - 安装的先决条件 97
 - 测试 106
 - 重新启动服务器 106
 - 关于 97
 - 流程概述 97
 - 名称服务器参数, 编辑 101
 - 目录记录, 关于 99
 - 配置文件参数, 使用准则 105
 - 配置文件参数值, 表 101
 - 数据库登录, 创建 98
 - 验证目录, 创建 98
 - 用户, 创建 99
 - 用户记录, 添加 100
- LDAP/ADSI 配置实用程序** 91
- LDAPUSER** 98
- libsscldap.sl** 253
- libsscldap.so** 253
- Microsoft Active Directory** 19
- Microsoft Crypto 或 RSA 加密的密钥交换** 49
- Microsoft Crypto 加密**
 - 密钥交换 49
 - 配置 48
- Microsoft IIS** 17
- Microsoft Windows, 更改 SADMIN 口令** 28
- Novell NDS eDirectory** 19
- NULL 字段, 处理** 163
- PasswordAttributeType 参数**
 - 关于 253
 - 为 LDAP 或 ADSI 设置 104
- PeerAuth 参数** 51, 54, 250
- PeerCertValidation 参数** 52, 54, 250
- PortName 参数**
 - 关于 253
- ProtectedVirtualDirectory 参数**
 - 不用于 LDAP 或 ADSI 101
 - 关于 250
 - 为 Web SSO 设置 134
- PROXYE 用户 ID** 261
- RC2 加密管理**
 - 关于 57
 - 密钥数据库管理器, 使用 58
 - 升级 61
- REMOTE_USER 变量** 249
- RolesAttributeType 参数**
 - 关于 253
 - 示例设置, eservice.cfg 119
- RSA 加密** 16
 - 密钥交换 49
 - 配置 48
- S_BU 表** 238, 239
- S_CONTACT 表** 232, 233, 234
- S_EMP_PER 表** 234
- S_ORG_EXT 表** 236, 237, 238, 239
- S_ORG_GROUP 表** 240
- S_ORG_PRTNR 表** 239
- S_PARTY 表**
 - 部门数据模型 237
 - 访问组数据模型 242
 - 雇员数据模型 234
 - 关于和图表 230
 - 合作者组织数据模型 239
 - 家庭数据模型 240
 - 客户数据模型 236
 - 人员 (联系人) 数据模型 232

- 用户列表数据模型 241
- 用户数据模型 233
- 职位数据模型 235
- 组织数据模型 238
- S_PARTY_GROUP 表** 242
- S_PARTY_PER 表** 231
- S_PARTY_REL 表** 231
- S_PER_RESP 交集表** 233
- S_POSTN 表** 234, 235
- S_USER 表** 233, 234
- S_USERLIST 表** 241
- SADMIN 口令**
 - Microsoft Windows, 更改 28
 - UNIX, 更改 29
- SecAdptDllName 参数**
 - 关于 253
 - 为 LDAP 或 ADSI 设置 103
- SecThickClientExtAuthent 系统首选项** 260
- SecureBrowse 参数, 关于** 256
- SecureLogin 参数**
 - 关于 256
 - 为 LDAP 或 ADSI 设置 105
 - 为 Web SSO 设置 136
- seed 数据**
 - GUESTCST 用户 149
 - Siebel Financial Services, 注册和管理 268
 - Siebel Financial Service, 关于 seed 用户和表 274
 - Siebel Financial Service, 关于 seed 职责和表 275
 - 代理雇员 261
 - 代理雇员职位, 关于 263
 - 非雇员用户记录 (表) 262
 - 工作流程过程, 关于修改 154
 - 雇员记录 261
 - 匿名用户, 关于 100
 - 匿名用户, 使用 149
 - 缺省组织部门记录, 关于 263
 - 数据库登录 263
 - 用户 ID, 匿名用户 152
 - 职位结构 187
 - 职责 seed 数据图表 (表) 262
 - 职责, 修改 149
 - 自行注册工作流程过程, 修改 155
- ServerName 参数**
 - 关于 254
 - 为 LDAP 或 ADSI 设置 103
- SessionTimeout 参数**
 - 关于 249
- SessionTracking 参数** 144
- SharedCredentialsDN 参数**
 - 为 LDAP 或 ADSI 设置 104
- SharedCredentialsDN 参数, 关于** 254
- Siebel Financial Services**
 - eapps.cfg 文件和 eapps_fins.cfg, 关于和表 268
 - LDAP 和 ADSI 安全适配器验证 266
 - LDAP 和 ADSI 安全适配器验证, 实施 267
 - seed 数据, 注册和管理 268
 - seed 用户, 关于和表 274
 - seed 职责, 关于和表 275
 - Web SSO 验证, 实施 267
 - 匿名浏览, 注册和管理 269
 - 配置文件名, 关于和表 273
 - 未注册的用户, 注册和管理 269
 - 应用程序 (表) 265
 - 用户的内部管理 270
 - 用户的外部管理 270
 - 用户资料, 关于维护 270
 - 自行注册, 注册和管理 269
- Siebel Financial Services, 基本访问控制**
 - 访问控制机制 271
 - 访问组访问控制, 管理 271
- Siebel QuickStart cookie** 143, 145
- Siebel Strong Encryption Pack** 61
- Siebel Web Server Extension**
 - SSL 加密, 配置 52
 - Web 服务器通讯 DLL 129
 - 数据库验证中的角色 68
- Siebel Web 客户机, 管理安全适配器验证** 153
- Siebel Web 引擎**
 - 配置参数, 示例 247
- Siebel 安全适配器软件开发人员套件 (SDK), 关于** 19
- Siebel 报表服务器, 保护**
 - 报表组件 42, 43
 - 为安全配置 42
- Siebel 服务器**
 - SSL 配置实用程序, 运行 50
 - SSL, 设置附加名称服务器参数 52
 - 重新启动 136
 - 配置文件 256
 - 数据库的数据保密性 21
- Siebel 服务器负载均衡, 关于和功能** 39
- Siebel 数据库**
 - “新职责”字段, 填写 171
 - 雇员, 禁用 168
 - 雇员设置, 关于完成 168
 - 合作者用户, 添加 169
 - 联系人用户, 添加新用户 169
 - 新雇员, 添加 167
 - 用户记录, 添加 100, 132
 - 职位, 角色 167
- Siebel 网关, 名称服务器参数 (表)** 251
- Siebel 文件系统, 访问** 41

Siebel 专用 Web 客户机

- 安全适配器系统首选项 260
- 配置文件 256
- 与标准 Web 客户机比较 120

siebel.local.client cookie

请参阅 Siebel QuickStart cookie

SiebelAdapterUsername 参数, 关于 254**SingleSignOn 参数** 254

- 不用于 LDAP 或 ADSI 101
- 关于 249
- 为 Web SSO 设置 133

SISNAPI (Siebel Internet 会话 API) 21**sscfldap.dll** 253**sscsadb.dll** 258**SsIDatabase 参数**

- 关于 254

SSL 加密

- Siebel Web Server Extension, 配置 52
- Siebel 服务器, 设置其附加名称服务器参数 52
- 配置 49

SSL 配置实用程序

- Siebel 服务器, 运行 50
- SWSE, 运行 53

SSL 通讯 16**SubUserSpec 参数**

- 关于 249

Sun ONE Directory Server 19**Sun ONE Web Server** 22**TESTPW** 99**TESTUSER** 99**TrustToken 参数**

- 不用于 LDAP 或 ADSI 101
- 关于 249, 254
- 为 Web SSO 设置 133

Unicode 支持 64**UNIX, 更改 SADMIN 口令** 29**URL 参数, 输入证书作为** 143**URL 登录, 输入证书作为** 143**UseAdapterUsername 参数**

- 关于 254

UseRemoteConfig 参数 121

- 关于 257

UserNameAttributeType 参数

- 关于 254

UsernameAttributeType 参数

- 为 LDAP 或 ADSI 设置 104

UserSpec 参数

- 不用于 LDAP 或 ADSI 101
- 关于 249
- 为 Web SSO 设置 134

UserSpecSource 参数

- 不用于 LDAP 或 ADSI 101
- 关于 249
- 为 Web SSO 设置 134

Web 服务器

另请参阅 Siebel Web Server Extension

Web SSO

- checksum 验证 115
- Siebel Financial Services, 实施 267
- 安全套接层, 实施 116
- 共享数据库帐户, 实施 116
- 关于 19
- 匿名用户, 实施 118
- 匿名浏览, 实施 118
- 视图, 保护 139
- 数字认证验证 137
- 虚拟目录 250
- 应用程序用户, 关于 114
- 用户身份的来源, 实施 138
- 用户证书来源指定 248, 249
- 证书口令散列处理 109

Web SSO 适配器

- ApplicationUser 参数 252
- BaseDN 参数 252
- CredentialsAttributeType 参数 253
- PasswordAttributeType 参数 253
- PortName 参数 253
- RolesAttributeType 参数 253
- SecAdptDllName 参数 253
- ServerName 参数 254
- SingleSignOn 参数 254
- SsIDatabase 参数 254
- TrustToken 参数 254
- UserNameAttributeType 参数 254
- 安全适配器流程概述 67
- 部署选项, 列出 113
- 角色, 使用 119
- 适配器定义的用户名, 实施 117
- 远程配置选项, 关于 121

Web SSO 验证

- 关于 125
- 设置方案 127
- 实施, 关于 126
- 实施的注意事项 126
- 实施设置任务, 列出 128
- 数字认证验证 127
- 验证流程, 概述 125
- 用户身份来源选项 127
- 与其它方法比较 66
- 远程验证 122
- 自行注册 150

Web SSO, 设置方案

- Active Directory Server 服务器, 口令分配 130
- Active Directory Server, 设置 130
- Active Directory Server, 作为目录配置 130
- CFG 文件参数值, 使用准则 133
- IIS Web 服务器, 配置 131

- 安装要求 127
 - 测试 136
 - 服务器, 重新启动 136
 - 名称服务器参数, 设置准则 134
 - 配置参数, 使用准则 135
 - 设置任务 128
 - 示例配置 127
 - 数据库登录, 创建 130
 - 虚拟目录, 创建 128
 - 用户记录, 添加到 Siebel 数据库 132
 - 在目录中创建用户 131
 - 注释, 更改文件 135
 - Web 服务器**
 - IBM HTTP Server 19
 - Microsoft IIS 17
 - Siebel 服务器的数据保密性 21
 - Sun ONE Web Server 22
 - Web 服务器图像, 添加用于执行更新的口令** 32
 - Web 更新保护密钥** 32
 - Web 客户机, 配置加密** 54
 - Web 客户机用户, 验证兼容性** 91
 - Web 站点, 安全性参考** 25
 - Web 浏览器, 安全设置** 24
 - WebUpdatePassword 参数** 32
 - Windows**
 - ADSI 客户机的要求 72
 - SADMIN 口令, 更改 28
 - Windows 集成身份验证** 250
 - X.509 验证** 16
- ## A
- 安全登录**
 - 部署选项 141
 - 实施 141
 - 安全适配器**
 - 另请参阅 LDAP 适配器
 - ASSI 适配器的要求 71
 - LDAP 和 ADSI 安全适配器验证 69
 - LDAP 和 ADSI 安全适配器验证, 实施 90
 - SharedCredentialsDN 参数 254
 - Siebel 专用 Web 客户机, 和 120
 - 安全适配器验证方案 97
 - 部署选项, 列出 113
 - 操作模式 67
 - 单一应用程序访问 69
 - 概述 67
 - 管理登录要求 166
 - 目录要求 70
 - 外部安全适配器, 关于实施 67
 - 安全适配器通讯部署选项** 113
 - 安全适配器验证**
 - checksum 验证 115
 - 安全套接层, 实施 116
 - 登录口令存储 70
 - 共享数据库帐户, 实施 116
 - 角色, 使用 119
 - 口令散列处理 109
 - 匿名用户, 实施 118
 - 匿名浏览, 实施 118
 - 设置, 流程概述 91
 - 适配器定义的用户名, 实施 117
 - 视图, 保护 139
 - 数字认证验证 137
 - 通过 Web 客户机管理 153
 - 应用程序用户, 设置 114
 - 用户身份的来源, 实施 138
 - 优点 69
 - 与其它方法比较 66
 - 远程配置选项, 关于 121
 - 证书口令散列处理 109
 - 作为验证服务 69
 - 安全套接层 (SSL)**
 - ADS 目录建议 71
 - SsIDatabase 参数 254
 - 安全视图 256
 - 部署选项 113, 141
 - 登录表单传输参数 256
 - 实施 116
 - 安全套接层 (SSL)**
 - 数据库验证选项 69
 - 安全系统访问, 用户验证**
 - Web 单一登录 (SSO) 19
 - 关于 17
 - 数据库验证 18
 - 外部验证, 安全适配器 19
 - 安全性**
 - 概述 15
 - 体系结构, 组件 17
 - 行业标准, 使用 16
 - 安全性参考, 参考书目** 24
- ## B
- 本地访问标志** 201
 - 标准 Web 客户机和专用 Web 客户机, 比较** 120
 - 标准加密器** 64
 - 标准交互, 自行注册** 150
 - 表所有者 (DBO), 更改和口令** 30
 - 部门**
 - 部门记录, 删除 194
 - 基本表和扩展表, 图示 237
 - 角色 194
 - 设置 (过程) 198
 - 与组织有关 238
 - 组织当事方类型, 位于 231
 - 部署**
 - 请参阅物理部署
 - 部署选项, LDAP 和 ADSI 适配器** 113

C

- 参考数据, 访问控制策略 192
- 测试外部验证系统 106
- 测试用户
 - Siebel 数据库, 添加记录 100
 - Web SSO 验证 131
 - 关于 99
- 查询用户参数 163
- 重复用户
 - 清除重复项字段, 修改 160
 - 自行注册清除重复项检查, 禁用 161

D

- 代理雇员 188
- 代理雇员职位, **seed** 数据 263
- 单一登录
 - 参阅 *Web SSO 条目*
- 单一登录 (SSO), 关于 19
- 单一应用程序访问 69
- 单一职位访问控制 186, 209
- 单一组织访问控制 189
- 当事方
 - 请参阅 *当事方类型*
- 当事方基本表和扩展表, 关于和图表 230
- 当事方类型
 - 当事方, 定义 181
 - 当事方类型之间的关系 231
 - 访问控制, 分类的主数据 191
 - 关于和表 181
 - 确定用户访问 204
 - 用户列表, 创建 219
 - 用户列表, 添加用户 220
- 当事方数据模型
 - 部门数据模型 237
 - 访问组数据模型 242
 - 雇员数据模型 234
 - 关于 230
 - 合作者组织数据模型 239
 - 家庭数据模型 240
 - 客户数据模型 236
 - 人员 (联系人) 数据模型 232
 - 用户列表数据模型 241
 - 用户数据模型 233
 - 职位数据模型 235
 - 组织数据模型 238
- 导出选项卡布局 225
- 导入选项卡布局 225
- 登录
 - seed** 数据库登录 263
 - 口令, 存储 70
 - 示例页 140
 - 视图的要求, 设置或删除 150

- 数据库验证概述 68
- 帐户策略, 关于实施 141

登录表单

- 附加功能 140
- 口令过期, 关于和实施 142
- 示例 140

电子欺骗袭击, 防止 249

动态端口号, 使用 39

端口参数

- 为 LDAP 或 ADSI 设置 103

端口号, 使用动态端口号 39

多组织

- 访问控制 189
- 优点 193
- 原因 193

F

防火墙 38

防火墙支持

- 布局, 建议 37
- 功能, 列表 37
- 关于 37

访问, 限制

- Siebel 文件系统访问 41
- 客户机设备, 实体安全 40
- 数据库服务器访问 41

访问控制

- Siebel Financial Services 中的商机 271
- 部门, 设置 194
- 策略, 列表 192
- 单一职位访问控制, 关于 186
- 单一职位访问控制, 经理视图 209
- 当事方类型, 关系 231
- 当事方类型, 关于和表 181
- 当事方数据模型, **S_PARTY** 表 230
- 定义 179
- 访问组, 关于 191
- 个人 209
- 个人访问控制 185
- 基本访问控制, 关于 180
- 记录级别 22
- 经理访问控制 187, 210
- 可访问的数据, 子组织视图 210
- 可视性全部自动属性, 使用 228
- 可视性子视图类型 209
- 客户数据 183
- 目录, 概述 184
- 目录访问控制视图 210
- 全部访问控制 191
- 视图级别 21
- 视图级别机制 180
- 视图属性, 显示 209
- 特殊框架类, 使用 229

- 团队 209
- 团队访问控制, 关于 187
- 问题疑难解答 246
- 向下搜索可视性, 配置 229
- 许可证密钥, 角色 198
- 选取列表对象, 设置可视性 228
- 选项卡布局, 通过职责管理 224
- 选择子视图, 配置可视性 227
- 业务环境结构, 关于和元素 (表) 192
- 职位 186
- 职位, 设置 195
- 职责, 定义和添加视图及用户 196
- 职责, 角色 119
- 主数据 183
- 子组织访问控制 190
- 组织 188, 210
- 组织, 设置 194
- 访问控制, 实施**
 - 可视性 MVField 205
 - 可视性 MVLink 205
 - 可视性属性, 角色 197
 - 可视性子视图, 角色 197
 - 可视性字段 204
 - 视图访问控制属性 208
 - 视图结构示例 211
 - 私有和公共记录, 标志设置 204
 - 所有者当事方类型 204
 - 业务组件视图模式 203
 - 业务组件视图模式字段 204
 - 应用程序, 角色 197
 - 应用程序级别访问控制 197
 - 职责, 关于 197
 - 职责, 与用户关联 200
 - 子视图访问控制属性 206
- 访问控制, 业务组件视图**
 - 单一或多组织 190
 - 单一职位视图模式 186
 - 角色 197
 - 经理设置 188
 - 团队设置 187
 - 子组织设置 191
- 访问组**
 - 成员, 添加 221
 - 创建 220
 - 结构, 修改 221
 - 类别, 断开关联 223
 - 类别, 关联 223
 - 目录访问控制 192
 - 数据, 关联 222
 - 职责, 关联任务 226
 - 主数据目录, 关联 222
- 访问组访问控制**
 - 另请参阅访问控制
 - 访问组, 与财务应用程序中的数据关联 271
- 关于 191
- 管理任务, 列出 218
- 基本原则 212
- 继承规则 212, 213
- 家庭, 财务应用程序中的管理 271
- 目录, 将访问组与财务应用程序关联 272
- 业务方案 213
- 用户的体验 216
- 访问组基本表和扩展表, 图示** 242
- 访问组数据模型, 关于和图表** 242
- 分类数据**
 - 另请参阅目录
 - 关于用户体验 216
 - 在信息中心中查看 217
- G**
- 高交互客户机, 自行注册** 150
- 个人访问控制** 185, 209
- 个人可视性** 185
- “更改职位”按钮** 177, 195
- 工作流程过程**
 - seed 流程, 关于修改 154
 - seed 数据, 修改 155
 - 查看 153
 - 定制业务服务, 关于 156
 - 激活 (过程) 153
 - 修改 155
 - 许可协议文本, 替换 155
 - 自行注册, 激活流程 153
 - 自行注册工作流程视图, 表 154
- 公司结构**
 - 类别, 介绍 193
 - 设置 193
- 公司网络安全, 概述** 15
- 共享数据库帐户, 实施** 116
- 共享数据库帐户部署选项** 113
- 雇员, 禁用** 168
- 雇员基本表和扩展表, 图示** 234
- 雇员用户**
 - seed 数据记录 261
 - 定义 234
 - 雇员, 禁用 168
 - 雇员设置, 关于完成 168
 - 雇员数据模型 234
 - 合作者用户, 添加 169
 - 活动职位, 更改 177
 - 联系人用户, 添加新用户 169
 - 新记录, 添加 167
 - “新职责”字段, 填写 171
 - 职位, 活动 177
 - 职位访问控制 186
 - 职责, 分配 202
 - 主要职位, 更改 177
 - 最低要求 167

“管理 - 服务器配置” 屏幕, 无法工作 243

管理模式, 可视性 191, 211

管理任务, 雇员

禁用 168

管理任务, 职位和职责

职位, 设置 199

职责, 定义 200

管理任务, 组织

部门, 设置 198

公司结构, 设置 193

组织, 设置 199

H

行业标准, 使用 16

合作者应用程序

重复项字段 160

授权的管理员, 角色 174

职责, 分配 202

主要职位, 更改 177

自行注册 151, 152

自行注册工作流程视图 154

合作者用户

添加 169

新建用户, 注册 175

职位访问控制 186

职责, 分配 202

合作者组织基本表和扩展表, 图示 239

合作者组织数据模型 239

会话 cookie 143

关于 55

活动目录服务接口适配器

请参阅 ADSI 适配器

J

“级联” 按钮 213

“记住我的用户 ID 和口令” 功能 141

加密

Microsoft Crypto, 配置 48

RC2 加密管理 57

RC2 加密管理, 升级 61

RSA 配置 48

Siebel Web Server Extension, 为 SSL 加密

配置 52

Siebel 服务器, 配置 Microsoft Crypto

或 RSA 48

SSL 加密, 配置 Siebel Enterprise 或

Siebel 服务器 49, 52

Unicode 支持 64

Web 客户机, 配置 54

采用 SSL 加密的 Siebel 服务器, 配置 49

端对端数据保密性 20

类型 45

密钥数据库管理器, 使用 58

新加密密钥, 添加 59

业务组件加密, 启用和禁用 62

移动 Web 客户机, 为同步加密 55

加密客户机数据库口令参数 111

家庭

管理任务 219

基本表和扩展表, 图示 240

交易数据, 访问控制策略 192

经理 - 下属关系, 关于 187

经理访问控制, 关于 187

经理可视性 187, 191, 210

经理列表模式用户属性 188

角色

存储在目录中 71, 119

分配 119

配置文件设置 119

适用的验证策略 119

K

可视性

另请参阅访问控制条目和职责

个人 185

经理 187

可视性字段 204

全部 209

视图可视性属性 197

职位, 角色 195

职责, 角色 196

可视性 MVField 205

可视性 MVLink 205

可视性类型属性 228, 229

可视性全部自动属性, 使用 228

可视性子视图

访问控制, 类型 209

视图结构示例 211

业务组件和视图连接 197

字段显示, 角色 209

可视性子视图类型属性 229

客户基本表和扩展表, 图示 236

客户机浏览器, Web 服务器的数据保密性 20

客户数据, 访问控制中的角色 183

客户数据模型 236

口令

另请参阅“忘记口令?” 问题

SADMIN, 在 Windows 上更改 28

UNIX, 更改 29

Web 服务器图像, 添加用于执行更新的口令 32

表所有者 (DBO) 和口令, 更改 30

更改缺省口令 27

过期, 关于和实施 142

散列处理 109

散列处理选项, 数据库验证 69

失败的任务, 检查 31

- “忘记口令”链接 161
- “忘记口令”体系结构 162
- “忘记口令？”问题 141
- 新口令，重新找回 162
- 用户资料，更改 176

框架类 229

L

类别

- 访问组，断开关联 223
- 访问组，关联 223
- 访问组，与数据关联 222
- 公司结构，介绍 193
- 管理任务，列出 218
- 继承规则 212, 213
- 控制访问权限 212
- 与目录有关 184

联系人用户

- 添加新用户 169
- 现有联系人，提升 171
- 组织关联 188

M

密钥数据库管理器

- keyfile 口令，更改 60
- 新加密密钥，添加 59
- 运行 58

名称服务器参数

- 编辑 101, 106
- 关于和表 251
- 设置，准则 134

目录

- 另请参阅访问组访问控制
- 创建，流程概述 98
- 创建用户 131
- 导航 216
- 访问控制，类型 192
- 访问控制策略 192
- 访问组，与数据关联 222
- 访问组访问控制原则 212
- 共享数据库帐户部署选项 113
- 关联的访问组和数据 222
- 关于 184
- 关于访问 184
- 管理任务，列出 218
- 检查证书 69
- 角色 67
- 控制类别的访问权限 212
- 类别，角色 184
- 目录记录，关于 99
- 权限记录参数 252
- 实施和测试，流程概述 97
- 授权访问 192

- 属性 184
- 要求 70
- 应用程序用户，角色 114
- 应用程序用户，设置 114
- 用户，创建 99
- 用户记录，添加 100
- 用户权限，关于 71
- 用户体验，关于 216
- 主数据中的角色 184

目录访问控制视图 210

N

内部管理员，修改“新职责”字段 171

匿名用户

- seed 数据用户 ID 152
- seed 数据职责，关于使用 149
- Siebel 数据库中的用户记录 100
- Web SSO 验证 131
- 参数控制 256
- 关于 99, 148
- 匿名用户记录，修改 149
- 实施 118
- 自动填写字段 152
- 自行注册，修改 152

匿名浏览

- AllowAnonUsers 参数 149
- Siebel Financial Services，注册和管理 269
- 关于 148
- 匿名用户，角色 149
- 配置参数，设置 149
- 实施 118, 148
- 视图，设置或删除显式登录 150

P

配置

- SADMIN 口令，在 UNIX 上更改 29
- SADMIN 口令，在 Windows 上更改 28
- Web 服务器图像，添加用于执行更新的口令 32
- Web 浏览器，安全设置 24
- 安全性指示，任务列表 25
- 口令，更改缺省值 27

配置文件

- AllowAnonUsers 参数 256
- ApplicationUser 参数 252
- BaseDN 参数 252
- CredentialsAttributeType 参数 253
- DBSecAdpt_SecAdptDllName 参数 258
- eapps.cfg 示例参数 247
- eapps.cfg 文件参数值，使用准则 133
- eservice.cfg 示例 119
- PasswordAttributeType 参数 253
- PortName 参数 253
- RolesAttributeType 参数 253

SecAdptDllName 参数 253
 SecureBrowse 参数 256
 SecureLogin 参数 256
 ServerName 参数 254
 SharedCredentialsDN 参数 254
 SiebelAdapterUsername 参数 254
 SingleSignIn 参数 254
 SsIDatabase 参数 254
 SSL 相关参数 250
 TrustToken 参数 254
 UseAdapterUsername 参数 254
 UseRemoteConfig 参数 257
 UserNameAttributeType 参数 254
 编辑, 关于 256
 参数值, 表 101
 参数值, 使用准则 105, 135
 激活应用程序配置文件中的更改 256
 角色, 设置 119
 名称服务器参数, 关于和表 251
 系统首选项, 关于设置 260
 验证参数 256
 与客户机有关 256
 与验证有关的参数 248
 远程配置文件的要求 122
 注释, 更改文件 135
 注释, 指定 256

屏幕, 定义 180

Q

轻型目录访问协议适配器

请参阅 LDAP 适配器

清除用户重复项, 关于 158

清除重复项

关于 158
 清除重复项检查, 禁用 161
 字段, 修改 160

权限, 验证目录参数 252

全部访问控制

关于 191, 209
 移动用户限制 202

缺省组织部门记录, seed 数据 263

R

人员

与用户对比 233
 职责, 分配 202

人员基本表和扩展表, 图示 233

人员数据类型, 定义 232

认证文件名参数 (CertFileName) 51

S

散列处理

口令 109

审计追踪 22

适配器定义的用户名

部署选项 113

实施 117

视图

保护 139

视图, 定义 180

视图结构, 示例 211

添加字段 158

显式登录的要求, 设置或删除 150

显示视图属性 209

限制访问 196

新子视图, 包括 158

许可证密钥和可视性 197

职责, 访问中的角色 200

自行注册工作流程视图, 表 154

自行注册视图, 相关的业务组件 155

组访问控制 210

视图可访问性, 未注册的用户 148

授权的管理员

另请参阅 授权管理

“新职责”字段, 编辑 171

关于 172

授权管理, 管理员访问 172

用户验证要求 172

职责继承 171

授权管理

另请参阅 授权的管理员

合作者应用程序, 关于 174

合作者用户, 注册 175

授权的管理员职责, 限制 201

写权限, 用户目录 172

新客户, 注册 173

验证要求 172

注册用户, 关于 173

属性, 口令存储 70

数据, 分类 216

数据保密性, 端对端加密 20

数据可视性, 授权控制

访问控制, 记录级别 22

访问控制, 视图级别 21

关于 21

入侵, 通过安全物理部署防止 23

数据库存储, 数据保密性 21

数据库登录, 创建 98, 130

数据库服务器, 访问 41

数据库验证

安全套接层 (SSL) 选项 69

概述 68

口令散列处理 109

口令散列处理选项 69

- 流程概述 68
- 实施 68
- 授权的管理员, 可用性 172
- 限制 68
- 与其它方法比较 66
- 自行注册 150
- 数据库验证, 关于** 18
- 数据连续性**
 - 审计 41
 - 审计, 程度 22
- 数字认证验证** 137
 - 关于 127
- 私有密钥文件口令参数 (KeyFilePassword)** 51
- 私有密钥文件名参数 (KeyFileName)** 51
- 私有字段标志** 204
- 所有者当事方类型** 204
- 所有者类型为“职位”的视图模式** 210

T

- 弹出可视性类型属性** 228
- 体系结构, Siebel 安全性**
 - 安全系统访问, 用户验证 17
 - 入侵, 通过安全物理部署防止 23
 - 数据保密性, 端对端加密 20
 - 数据可视性, 授权控制 21
 - 数据连续性, 审计 22
 - 移动解决方案, 安全 23
- 同级验证参数 (PeerAuth)** 51
- 团队访问控制** 187, 209

W

- 外部验证**
 - 测试 Web SSO 136
 - 登录证书 147
 - 口令存储的要求 70
 - 匿名用户记录 148
 - 系统测试 106
 - 远程安全配置文件的要求 122
 - 远程配置选项, 关于 120
 - 专用 Web 客户机, 包括 120
- 外部验证, 安全适配器** 19
- 万维网 (WWW) 发布服务, 重新启动** 136
 - “忘记口令?” 问题 141
 - NULL 字段, 处理 163
 - 比较字段, 关于修改 164
 - 比较字段, 修改 164
 - 查询用户步骤参数 163
 - 工作流程过程, 关于修改 163
 - 使用链接, 关于 161
 - 输入字段, 添加或删除 165
 - 体系结构 162
 - 新口令, 重新找回 162

未注册的用户

- 另请参阅匿名用户
- seed 匿名用户, 关于 149
- Siebel Financial Services, 注册和管理 269
- 参数控制 256
- 匿名用户记录 148
- 配置参数, 设置 149
- 视图, 设置或删除显式登录 150
- 授予视图可访问性 148

文档

- 安全性参考, 参考书目 24

文件

- cookie 143

无线通讯, 安全实时

物理部署

- Siebel 报表服务器, 保护 42, 43
- Siebel 服务器负载均衡 39
- 端口号 39
- 防火墙支持 37
- 访问, 限制 40
- 数据连续性, 审计 41
- 网络, 基本组件 (图表) 35

X

系统首选项

- 编辑 260
- 列出 260

向下搜索可视性, 配置

“新职责”字段

- 关于 152
- 填写 171
- 修改 171

信息中心

- 分类数据, 查看 217
- 浏览器, 关于 216

虚拟目录

- ProtectedVirtualDirectory 参数 250
- 创建 128

虚拟字段

- 自行注册流程, 角色 155

许可协议, 替换缺省文本

许可证密钥, 视图可视性中的角色

选取列表对象, 设置可视性

选项卡布局

- 导入和导出 225
- 管理选项卡布局 224
- 通过职责管理, 关于 224
- 主要职责, 分配 225

选择子视图

- 可视性 227
- 特殊框架类, 用于可视性 229

Y

验证

另请参阅验证管理器

标准 Web 客户机与专用 Web 客户机之间的体系结构差别 120

方法, 比较表 66

方法, 概述 65

数据库验证 68

数据库验证, 实施 68

验证方法参数 123

验证管理器

另请参阅验证; 数据库验证; Web SSO 验证

验证同级认证参数 (PeerCertValidation) 52

验证选项

checksum 验证 115

安全登录 141

安全套接层, 实施 116

共享数据库帐户, 实施 116

角色 119

口令散列处理 109

匿名用户, 实施 118

匿名浏览, 实施 118

适配器定义的用户名, 实施 117

视图, 保护 139

数字认证验证 137

应用程序用户, 设置 114

用户身份的来源, 实施 138

远程配置 121

证书口令散列处理 109

业务服务, 定制 156

业务环境结构

多组织, 优点 193

多组织, 原因 193

关于和元素 (表) 192

业务组件

覆盖可视性 228

可视性属性, 访问控制中的角色 197

可视性子视图, 访问控制中的角色 197

可视性子视图, 关于 209

控制属性, 显示 209

全部访问控制 191

视图结构示例 211

自行注册 152

自行注册视图 155

业务组件加密

启用和禁用 62

业务组件视图模式

单一或多组织设置 190

单一职位设置 186

访问控制中的角色 197

关于数据访问 203

经理设置 188

可视性字段 204

模式和可视性字段, 查看 203

团队设置 187

子组织设置 191

移动 Web 客户机, 为同步加密 55

移动应用程序

安全, 关于 23

设备用户验证 24

无线通讯, 安全实时 24

移动用户

可访问的视图 202

验证, 限制 91

职位和可视性规则 196

疑难解答

“管理 - 服务器配置”屏幕, 无法工作 243

访问控制问题 246

用户注册问题 244

应用程序

访问控制, 影响 197

许可证密钥和视图可视性 197

应用程序对象管理器, ADSI 适配器的要求 72

应用程序级别访问控制, 关于和视图可视性 197

应用程序用户

Web SSO 验证 131

关于 99

设置 114

特点 114

写权限 166, 172

应用的可视性规则链接属性 229

“用户”业务组件, 基础表 167

“用户注册”业务服务 163

“用户注册”业务组件

“忘记口令”体系结构 162

比较字段, 修改 164

查询用户步骤参数 163

清除重复项字段, 排除 159

清除重复项字段, 修改 160

新子视图 158

自行注册视图 155

用户

另请参阅未注册的用户

Siebel 数据库, 添加 167

定义 233

用户数据模型 233

与雇员对比 234

职责, 分配 202

用户管理

Siebel 数据库, 添加用户 167

授权的管理员 172

用户验证要求 166

用户资料, 维护 176

用户记录

seed 数据, 提供为 (表) 262

数据收集, 流程概述 157

添加到 Siebel 数据库 100

用户列表

- 创建 219
- 用户, 添加 220

用户列表基本表和扩展表, 图示 241

用户列表数据模型, 关于和图表 241

用户目录

- 写权限 166, 172
- 自行注册参数 153

用户身份的来源

- 关于 127
- 实施 138

用户数据模型 233

用户验证

请参阅验证

用户证书, 来源指定参数 249

用户注册

- seed 数据 148
- 问题疑难解答 244
- 要求 148
- 注册, 关于 147

用户资料

- 个人信息, 编辑 176
- 关于更新 176
- 活动职位, 更改 177
- 口令, 更改 176

远程配置选项

- 实施准则 122
- 适用的验证策略 121
- 外部验证, 关于实施 120

远程验证 122

Z

帐户策略, 关于实施 141

证书

- ADSI 验证中的角色 67
- CredentialsAttributeType 参数 253
- LDAP 验证中的角色 67
- URL 参数 143
- 安全适配器验证流程 70
- 登录页 140
- 根据目录验证 69

证书口令散列处理 109

职位

- 重命名, 警告 195
- 多位雇员, 关于 195
- 父子关系 195
- 雇员定义中的角色 234
- 管理任务, 列出 218
- 合作者用户和授权的管理员 174
- 活动职位, 更改 177
- 活动职位, 关于 177
- 活动职位, 指定 186
- 联系人用户, 添加新用户 169

删除 195

设置 (过程) 199

设置, 关于 195

通过组织更改 195

职位, 定义 186

职位结构 187

职位数据模型 235

主要职位 186

主要职位, 更改 177

职位访问控制, 关于实施 186

职位基本表和扩展表, 图示 235

职责

另请参阅可视性

seed 数据, 关于和表 262

seed 数据, 修改 149

seed 职责, 修改或删除 196

“新职责” 字段 171

定义 200

访问控制, 影响 197

分配 119

分配给雇员用户 202

分配给合作者 202

分配给人员 202

关于 196

管理视图 196

继承 171

角色 119

匿名用户 149

任务, 关联 226

使用角色关联 71, 119

视图, 包括在职责中的视图 263

视图, 本地访问 201

系统首选项视图, 限制访问 196

用户, 分配到 202

由授权的管理员分配 173

与工作职能有关 196

与合作者组织关联 174

职责字段和自行注册 152

组织, 关联 201

主数据

访问控制 191

访问控制策略 192

访问控制中的角色 183

与访问组关联, 关联 222

组织 184

主要职责, 分配 225

注册, 用户注册问题疑难解答 244

专用 Web 客户机

请参阅 Siebel 专用 Web 客户机

资源

安全性参考, 参考书目 24

子视图

查看属性 207

定义 206

- 访问控制 209
- 可视性属性, 关于 206
- 可视性特殊框架类 229
- 显示名称和可视性 208
- 选择子视图可视性 227
- 业务组件和可视性 207
- 子组织访问控制**
 - 关于 190
 - 可访问的数据 210
- 自动登录 cookie**
 - “记住我的用户 ID 和口令” 功能 141
- 自动登录证书 cookie** 143
- 自行注册**
 - 另请参阅自行注册工作流程过程
 - Siebel Financial Services, 注册和管理 269
 - 工作流程过程, 查看 153
 - 工作流程过程, 激活 153
 - 关于 150
 - 激活 (过程) 153
 - 匿名用户记录, 修改 152
 - 配置参数 153
 - 清除用户重复项, 关于 158
 - 清除重复项检查, 禁用 161
 - 视图, 关于修改 154
 - 许可协议, 替换缺省值 155
 - 业务组件 152
 - 与应用程序有关的示例 150
 - 注册, 用户角度 151
 - 自行注册的组件 152
 - 字段, 重新定义必需字段 156
- 自行注册定制业务服务, 关于** 156
- 自行注册工作流程过程**
 - 另请参阅自行注册
 - seed 数据, 修改 155
 - 重复用户更新, 防止 159
 - 清除重复项检查, 禁用 161
 - 清除重复项字段, 修改 160
 - 视图, 表 154
 - 数据收集概述 157
 - 新子视图, 包括 158
 - 字段, 添加到视图中 158
- 自行注册字段**
 - 必需, 指定为 156
 - 必需属性, 删除 157
 - 重复用户更新, 防止 159
 - 将字段添加到视图中 158
 - 类规范 156
 - 清除重复项字段, 修改 160
 - 数据收集流程概述 157
 - 虚拟字段, 使用 155
 - 自动填写 152
- 字段, 自行注册**
 - 必需属性, 删除 157
 - 查找 156
 - 指定为必需 156
- 组访问控制视图** 210
- 组织**
 - 部门, 角色 194
 - 多组织, 原因 193
 - 管理任务 219
 - 设置 (过程) 199
 - 设置, 关于 194
 - 优点 193
 - 职位, 更改 195
- 组织当事方类型**
 - 部门, 关于 231
 - 定义 238
 - 关系规则 231
- 组织访问控制**
 - 单一和多组织 189
 - 单一组织访问控制 189
 - 多组织访问, 确定视图 190
 - 多组织访问控制 189
 - 关联的职责 201
 - 关于 188
 - 活动组织和视图访问 201
 - 可定制产品可视性 190
 - 子组织访问控制 190
- 组织基本表和扩展表, 图示** 238
- 组织可视性** 210
- 组织数据模型, 关于** 238
- 组织组类型, 管理任务** 219