Sterling B2B Integrator

安全性（V5.2.3 或更高版本）

V 5.2.3

Sterling B2B Integrator

安全性（V5.2.3 或更高版本）

V 5.2.3

注

在使用本资料及其支持的产品之前，请阅读第 127 页的『声明』中的信息。

目录

安全性（V5.2.3 或更高版本）

Sterling B2B Integrator 使用各种安全机制，包括用于管理功能的系统密码，基于贵公司安全策略的密码规则，以及基于角色的安全性（用于为组织内的不同用户提供不同级别的访问）。

以下安全功能随附于 Sterling B2B Integrator：

- 基于角色的安全性根据与用户帐户关联的许可权，向该用户提供对文件、业务流程、Web 模板、服务和产品功能的访问。
- 密码规则是您根据贵公司的安全策略制定并应用于不同用户帐户的安全性决策的集合。这些选项包括诸如密码有效天数以及密码最大和最短长度等等。
- LDAP 认证可用于向 LDAP 目录委派外部用户帐户的认证，并使用贵公司内其他应用程序使用的相同安全信息提供认证。如果贵公司已经采用了 LDAP，那么您可以将现有 LDAP 目录用于应用程序。
- 系统安装口令 - 在安装期间，您可以为 Sterling B2B Integrator 安装创建系统口令。该口令是长度超过 16 个字符的高度复杂的字符串。系统口令是启动系统和访问受保护系统信息所必需的。
- 支持 x.509 证书，以实现加密、签名和传输层安全性。
- 联邦信息处理标准 (FIPS) 140-2 认证的软件模块以及对 FIPS 140-2 认证的 nCipher 和 Safenet 硬件的支持。
- 安全套接字层 (SSL) 和传输层安全性 (TLS)。

此外，还可配置以下安全功能：

- 安全超时功能为您提供配置用户会话超时的能力。
- 定制密码规则功能允许您添加额外的密码规则规则。这些额外的密码规则可以帮助您防止使用较弱且易受入侵的密码以及拒绝不符合规定的密码。
- 单点登录 (SSO) 功能是一个认证流程，支持用户访问若干应用程序并只需输入一个用户名和密码。
- 文档加密功能允许在传统文件和数据库许可权之外配置额外的安全层。

基于角色的安全性

基于角色的安全性概述

基于角色的安全性根据与用户帐户关联的许可权，向该用户提供了对特定文件、业务流程、Web 模板、服务以及产品功能的访问权。

为理解如何管理基于角色的安全性，您需要理解组、许可权和用户帐户是如何协作的。

- 许可权提供对用户界面页面以及页面提供的功能的访问权。
- 组是许可权的集合。
- 用户帐户分配给许可权和密码规则。

管理基于角色的安全性包括以下任务：

- 创建许可权
- 创建组
- 创建密码规则
- 创建用户帐户

组

组是许可权的集合。通过组，可以在一个位置维护多个用户的访问许可权。组有助于使维护帐户的工作量降至最低，尤其是在多个用户执行相同作业功能的情况下。

通过为每个作业功能（而非每个用户）创建组，可以将许多许可权与不同的用户相关联。还可以将组指定为另一个组的子组。

例如，采购部门有五名全部执行相同作业的采购专员。可以创建一个采购组并维护一个组中所有采购专员的访问许可权，以代替对每个采购专员用户帐户应用许可权。在该采购组中，您可以指定子组，从而根据专员负责的采购类型来进一步优化访问许可权。您可以为该采购组指定名为办公类用品、机械类用品、常规设备或交通工具的子组，从而优化访问许可权。

要避免在应用升级或补丁时发生覆盖，请勿修改系统预配置的组。

组任务包括：

- 创建组
- 搜索组
- 编辑组
- 删除组

预配置组

要向用户分配许可权，可以分配预配置组。用户将继承与组关联的所有许可权。如果为某用户帐户定义了"辅助功能选项"和"主题"，那么可以向该用户分配预配置组。

要创建组，必须具有针对"帐户"模块的许可权。

组命名约定

组命名有一系列约定。

对组使用以下命名约定：

- 组标识必须不同。
- 名称区分大小写。
- 包含不同大小写的两个组名将视为不同名称。
- 如果某组名已使用，那么不能将其用作新组的名称。否则将显示错误消息。

搜索组

您可以通过**管理**菜单搜索组。

关于此任务

要搜索组：

过程

1. 在**管理菜单**中，选择**帐户** > **组**。
2. 请完成以下操作之一：
   - 在"搜索"下，输入要搜索的部分**组名**或完整**组名**，然后单击**执行！** "组"页面将列出与您的搜索标准相匹配的所有组。
   - 在"列出"下的**按字母顺序排列**字段中，选择"全部"或要搜索的组名的开头字母，然后单击**执行！** "组"页面将列出与您的搜索标准相匹配的所有组。

创建组

您可以通过**管理**菜单创建组。

关于此任务

在开始之前，您需要知道：

- 要创建的组的组标识。
- 要创建的组的组名。
- 组的所有者的名称。
- 要与组关联的贸易伙伴的身份。只能有一个贸易伙伴与组关联，但一个用户帐户可以与许多组关联。这样，一个用户帐户便可以与多个贸易伙伴相关联。身份字段用于路由 Mailbox 中的消息。

要创建组：

过程

1. 在**管理菜单**中，选择**帐户** > **组**。
2. 单击**创建新组**旁边的**执行！**。
3. 在"新建组"页面中，输入**组标识**。
4. 输入**组名**。
5. 输入**所有者**。
6. 选择**身份**。
7. 单击**下一步**。
8. 在"分配子组"页面中，如果要按名称过滤组，请在"过滤数据"下的**按名称**字段中，输入要过滤的组的部分名称或完整名称，然后单击过滤按钮。
9. 选择要分配给此组的组。将这些组从"可用"窗格移动到"已分配"窗格。
10. 单击**下一步**。
11. 在"分配许可权"页面中，是否希望过滤许可权？
    - 要按名称过滤，请在"过滤数据"下的**按名称**字段中，输入要过滤的许可权的部分名称或完整名称，然后单击**按类型**字段右侧的过滤按钮。
    - 要按类型过滤，请在"过滤数据"下，从"按类型"列表中选择要过滤的许可权类型，然后单击**按类型**字段右侧的过滤按钮。

12. 选择要分配给此组的许可权。将这些许可权从"可用"窗格移动到"已分配"窗格。 缺省情况下，已选中与分配给此组的子组相关联的许可权。关联的许可权不显示在"可用"列中；但显示在确认页面中。
13. 单击**下一步**。
14. 复审组信息。
15. 单击**完成**。

编辑组

您可以编辑组以更新设置、子组和许可权。

关于此任务

编辑组时，可以更新：

- 设置
- 子组
- 许可权

不能更改组标识。如果需要更改组标识，那么必须创建新组。

要编辑组：

过程

1. 在**管理菜单**中，选择**帐户 > 组**。
2. 通过使用"组名称搜索"或"按字母顺序列出"来搜索要编辑的组，然后单击**执行！**。
3. 针对要更新的组，选择**编辑**。
4. 更新任意组设置并单击**下一步**。
5. 更新已分配的任意子组并单击**下一步**。
6. 更新已分配的任意许可权并单击**下一步**。
7. 单击**下一步**。
8. 复审组信息。
9. 单击**完成**。

删除组

您可以通过**管理**菜单删除组。

关于此任务

您不能从管理员用户除去 Sterling B2B Integrator 管理员组或 UI 帐户许可权。这些项允许系统管理员对系统进行管理。

要删除组：

过程

1. 在**管理菜单**中，选择**帐户 > 组**。
2. 在"组"页面中，通过使用"搜索"或"列出"选项查找要删除的组。
3. 在"组"页面中，单击要删除的组旁边的**删除**。

系统将删除组并显示以下消息：

系统更新已成功完成。

复审组名和标识

您可以通过**管理**菜单复审组名和标识。

关于此任务

要复审组名和标识：

过程

1. 在**管理菜单**中，选择**帐户** > **组**。
2. 在"组"页面中，通过使用"搜索"或"列出"选项查找要复审的组。
3. 选择组。 此时将显示组名和标识。

许可权

许可权提供对 Sterling B2B Integrator 中不同模块的访问，是基于角色的安全性的基础。用户许可权包括组许可权以及单独分配的任何许可权。

使用许可权可以：

- 从一个地方管理若干用户的访问权。
- 通过最少工作量来管理用户帐户，尤其是管理执行相同作业功能的多个用户。

许可权任务包括：

- 创建许可权
- 搜索许可权
- 编辑许可权名称
- 删除许可权

在创建、编辑或删除许可权之前，决定该组中的用户需要或不需要访问哪些模块，以执行其分配的功能。必须向您分配对"帐户"模块的许可权以创建许可权。

要避免在应用升级或补丁时发生覆盖，请勿修改系统预配置的许可权。如果需要定制的许可权分组，请创建新组。

许可权命名约定

许可权名称区分大小写，并且不能重复。

许可权命名约定包括：

- 名称区分大小写，包含不同大小写的两个名称将视为不同的名称。例如，"Any document"和"Any Document"是两个不同的许可权名称。
- 如果某名称已用于现有许可权，那么不能将其用作新许可权的名称。否则将显示错误消息。

不建议两个许可权采用大小写不同的相同名称，但允许存在此种情况。

从组继承的许可权

这些是预安装的组，以及在将许可权组分配给用户帐户时继承的许可权。如果将某组分配为子组，那么将继承相同的许可权。

每个组包含菜单项许可权以及用来授予页面访问权的对应 UI 许可权。例如，EBXML 包含 UI EBXML。

组名	组标识	从组继承的许可权
ACCOUNTS	ACCOUNTS	PasswordPolicy、Permissions、UI Accounts 和 UserNews
ADAPTER_UTILITIES	ADAPTER_UTILITIES	BEATuxedo、CDNetmaps、CDNetmapXref、CDNodes、SAPRoutes、SAPRouteXREF、 SAPSuiteBuilder 和 UI Adapter Utilities
ADVANCED_SETUP	ADVANCED_SETUP	DeliveryChannels、DocumentExchange、Identities、Packaging、Profiles、Transports 和 UI Advanced Trading Profile Setup
AS2 Edition	as2admin	子组 BPMONITOR 的所有许可权，以及 AS2 UI、TestNow、UI AS2 Trading Profile Setup、UI BP Manager、UI Ca Certs、UI Delete Trading Partner Data、UI Logs、UI Scheduler、UI System Certs 和 UI trading Parners
异常事件通知	eventAbnormal	无
帐户	acctadmin	子组 ACCOUNTS 的所有许可权以及 UI Groups 和 UI User Accounts。
警报通知	notifications	无
BPMONITOR	BPMONITOR	BPSSCorrelation、BusinessProcesses、CentralSearch、CommunicationSessions、Correlation、CurrentActivities、CurrentDocuments、CurrentProcesses、DataFlows、Documents、EBXMLCorrelation、EDICorrelation、EDIINT、GentranServerforUnix、Message Entry Workstation Home、SWIFTNETCorrelation、 UI BP Monitor 和 RosettaNet
业务流程	bpadmin	BPMONITOR 和 SERVICES 子组的所有许可权以及 UI BP Manager、UI Business Process 和 UI Delete BP。
CD 服务器代理管理员	cdsp_admin	子组 ACCOUNTS、BPMONITOR、CD 服务器代理用户、OPERATIONS 和 SERVICES 的所有许可权以及 UI Groups、UI Licenses、UI Password Policy、UI SQL Tool 和 UI User Accounts。
CD 服务器代理用户	cdsp_user	缺省情况下，使用 CDSP 辅助功能选项创建用户帐户时分配此组。 ACCOUNTS、BPMONITOR、OPERATIONS 和 SERVICES 子组的所有许可权以及 CDSP Services、UI CA Certs、UI Import/Export、UI Lock Manager、UI Logs、UI Perimeter Servers、UI Reports、UI Support Case Tool、UI System Certs 和 UI Trusted Certs。
命令行用户	commandlineuser	eInvoicing、eInvoicing ALL BUYERS、eInvoicing ALL SUPPLIERS、eInvoicing Archive、eInvoicing Configuration、eInvoicing CREATE/EDIT AGREEMENT、eInvoicing DELETE AGREEMENT 和 VIEW AGREEMENT

组名	组标识	从组继承的许可权
DEPLOYMENT	DEPLOYMENT	UI Deployment 和 Resource Tags
仪表板用户	dashboardUsers	缺省情况下，使用仪表板 UI 辅助功能选项以及以下任意仪表板主题创建用户帐户时将分配此组： • AFT • 缺省值 • 社区管理操作员、参与者、参与者发起方或发起方 Administration Management Console、Business Process Search Portlet、Cache Statistics Portlet、Cache Usage Portlet、Community Management Portlet、Community Statistics Portlet、Database Pool Usage Portlet、Database Status Portlet、Database Usage Portlet、Document Search Portlet、Document Tracking Portlet、Documents Processed Bar Chart Portlet、Documents Processed Time Series Portlet、Event Viewer Portlet、IFrame Portlet、Log File Viewer Portlet、Log File Viewer Portlet 2、ParticipatingCommunities Portlet、Peers Portlet、Queue Priority Statistics Portlet、Quick Links Portlet、RSS Feed Portlet、Sponsored Communities Portlet、System Alerts Portlet、Web Search Portlet 和 Web View Plus Portlet
部署	deploymentadmin	ADAPTER_UTILITIES、DEPLOYMENT、EBXML、MAILBOX、MAPS、 SERVICES、WEB_EXTENSIONS 和 WEB_SERVICES 子组的所有许可权以及 UI Connect:Direct、UI Delete CPA and CPSS Schema/Extension、UI Delete Map、UI Delete PGP Profile、UI Delete SAP Routes、UI Delete Schema、UI Delete Service Instance、UI Delete SWIFTNet Routing Rule、UI Delete Web Resource、UI Delete Web Templates、UI Delete WSDL、UI Delete XSLT Template、UI Generate/Download WAR Files、UI Import/Export、UI Scheduler、UI Schemas、UI SSH Local Identity Key、UI SWIFTNet Routing Rule 和 UI XSLT
EBICS 管理员	EBICS_ADM	UI EBICS Bank Profile Configuration、UI EBICS Contract Configuration、UI EBICS File Format Configuration、UI EBICS Offer Configuration、UI EBICS Order Type Configuration、UI EBICS Partner Profile Configuration、UI EBICS User Permission Configuration、UI EBICS User Profile Configuration、UI EBICS Bank Profile Configuration、UI EBICS Contract Configuration 和 UI EBICS Subscriber Key Validation
EBICS 操作员	EBICS_OPERATOR	UI EBICS Bank Profile Configuration、UI EBICS Contract Configuration、UI EBICS File Format Configuration、UI EBICS Offer Configuration、UI EBICS Order Type Configuration、UI EBICS Partner Profile Configuration、UI EBICS Subscriber Key Validation、UI EBICS User Permission Configuration 和 UI EBICS User Profile Configuration
EBXML	EBXML	BPSS、BPSSExtension、CPA 和 UI EBXML
ENVELOPES	ENVELOPES	ControlNumberHistory、ControlNumbers、EDISequenceCheckQueue、Envelopes、 TransactionRegister 和 UI Envelopes

组名	组标识	从组继承的许可权
异常事件通知	eventExceptional	无
MAILBOX	MAILBOX	Configuration、Messages、Routing Rules、UI Mailbox 和 VirtualRoots
MAPS	MAPS	ExtendedRuleLibraries、Maps、Standards 和 UI Maps
Mailbox 管理员	mboxadmins	MAILBOX 和 Mailbox 浏览器界面用户组的所有许可权以及 DeadLetter Mailbox、Mailbox Global Delete、Mailbox Global Query 和 EBICS_DEADLETTER Mailbox
Mailbox 浏览器界面用户	mbiusers	Mailbox Add Business Process、Mailbox Extract Business Process、Mailbox Path List Process、Mailbox Query Business Process、Mailbox Search Business Process、Mailbox Self Registration Business Process、Mailbox View Business Process 和 MBISearch JSP
OPERATIONS	OPERATIONS	JDBCMonitor、MessageMonitor、Perfdumps、SequenceManager、Statistics、ThreadMonitor、Troubleshooter、Tuning、UI Federated Systems 和 UI Operations
临时贸易伙伴	provisionalpartners	无
SERVICES	SERVICES	Configuration、Installation/Setup 和 UI Services
SSH	SSH	AuthorizedUserKey、KnownHostKey、 RemoteProfiles、UI SSH 和 UserIdentityKey
会话演示 Web 套件买方	sd_buyer	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack Template、WebSuite PO Ack View Template、WebSuite Query Business Process、WebSuite RA Send Business Process、WebSuite Self Registration Business Process、WebSuite Session Demo Confirm Send Template、WebSuite Session Demo PO Send Business Process、WebSuite Session Demo PO Template、WebSuite Session Demo PO View Template 和 WebSuite Session Demo Query List Template

组名	组标识	从组继承的许可权
会话演示 Web 套件供应者	sd_supplier	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack Template、WebSuite PO Ack View Template、WebSuite PO to Advance Ship Notice Template、WebSuite PO to Invoice Template、WebSuite PO Turn Business Process、WebSuite Query Business Process、WebSuite RA Send Business Process、WebSuite Self Registration Business Process、WebSuite Session Demo Confirm Send Template、WebSuite SessionDemo PO Send Business Process、WebSuite Session Demo PO View Template 和 WebSuite Session Demo Query List Template
Sterling B2B Integrator 管理员	super	ACCOUNTS、ADAPTER_UTILITIES、ADVANCED_SETUP、BPMONITOR、DEPLOYMENT、EBXML、ENVELOPES、 MAILBOX、MAPS、邮箱管理员、 OPERATIONS、SERVICES、SSH、WEB_EXTENSIONS 和 WEB_SERVICES 子组的所有许可权以及 UI Archive、 UI AS2 Trading Profile Setup、 UI Basic Trading Profile Setup、 UI BP Manager、UI Business Process、UI CA Certs、UI CodeLists、 UI Connect:Direct、UI Contracts、 UI Delete BP、UI Delete CPA and CPSS Schema/Extension、UI Delete Map、UI Delete PGP Profile、UI Delete SAP Routes、 UI Delete Schema、UI Delete Service Instance、UI Delete SWIFTNet Routing Rule、 UI Delete Trading Partner Data、UI Delete Web Resource、UI Delete Web Templates、UI Delete WSDL、UI Delete XSLT Template、UI Federated、 UI Generate/Download WAR Files、UI Groups、UI Import/Export、UI Licenses、UI Lock Manager、 UI Logs、UI Notify、UI Perimeter Servers、UI PGP Profile Manager、UI Reports、UI Scheduler、 UI Schemas、UI SQL Tool、UI SSH Local Identity Key、UI Support Case Tool、UI SWIFTNet Routing Rule、UI System Certs、UI Trading Partners、UI Trusted Certs、UI User Accounts 和 UI XSLT
系统操作	operator	OPERATIONS 子组的所有许可权以及 UI Archive、UI Licenses、UI Lock Manager、 UI Logs、UI Notify、UI Perimeter Servers、UI Reports、UI Scheduler、UI SQL Tool 和 UI Support Case Tool
贸易概要文件	tpadmin	ADVANCED_SETUP、ENVELOPES 和 SSH 子组的所有许可权以及 UI AS2 Trading Profile Setup、UI Basic Trading Profile Setup、UI CA Certs、UI CodeLists、UI Contracts、UI Delete Trading Partner Data、UI System Certs、UI Trading Partners 和 UI Trusted Certs
WEB_EXTENSIONS	WEB_EXTENSIONS	Utilities、WebResources 和 WebTemplates
WEB_SERVICES	WEB_SERVICES	SchemaMappings、SecurityToken、UI Web Services、WebServicesManager 和 WSDLCheckin

组名	组标识	从组继承的许可权
Web 套件买方	wsbuyers	WebSuite ASN View Template、WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack View Template、WebSuite PO Send Business Process、WebSuite PO Template、WebSuite PO View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite RA Send Business Process、WebSuite Remittance Advice Template、WebSuite Remittance Advice View Template 和 WebSuite Self Registration Business Process
Web 套件员工	wsemployees	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite ER Send Business Process、WebSuite Expense Report Template、WebSuite Expense Report View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Purchase Req Send Business Process、WebSuite Purchase Req Template、Websuite Purchase Req View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process、WebSuite TimeSheet Template、WebSuite TimeSheet View Template 和 WebSuite TS Send Business Process
Web 套件财务	wsfinance	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Expense Report View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Query Business Process、WebSuite Query List Template 和 WebSuite Self Registration Business Process
Web 套件人力资源	wshr	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process 和 WebSuite TimeSheet View Template

组名	组标识	从组继承的许可权
Web 套件管理员	wsmanagers	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite ER Send Business Process、WebSuite Expense Report View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Purchase Req Send Business Process、WebSuite Purchase Req View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Self Registration Business Process、WebSuite TimeSheet View Template 和 WebSuite TS Send Business Process
Web 套件购买者	wspurchaser	WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite Purchase Req View Template、WebSuite Query Business Process、WebSuite Query List Template 和 WebSuite Self Registration Business Process
Web 套件供应者	wssupplier	WebSuite ASN Send Business Process、WebSuite ASN Template、WebSuite ASN View Template、WebSuite Change Password Confirm Template、WebSuite Change Password Template、WebSuite Confirm Send Template、WebSuite Draft Save Business Process、WebSuite Email Notification Business Process、WebSuite Email Notification Template、WebSuite Invoice Send Business Process、WebSuite Invoice Template、WebSuite Invoice View Template、WebSuite Load Business Process、WebSuite Menu Business Process、WebSuite PO Ack Send Business Process、WebSuite PO Ack Template、WebSuite PO Ack View Template、WebSuite PO to Advance Ship Notice Template、WebSuite PO to Invoice Template、WebSuite PO to PO Ack Template、WebSuite PO Turn Business Process、WebSuite PO View Template、WebSuite Query Business Process、WebSuite Query List Template、WebSuite Remittance Advice View Template 和 WebSuite Self Registration Business Process

访问 UI 资源所需的许可权

这是访问菜单项及其关联页面和功能所必需的最小许可权集合。分配最小许可权集合也可以使用户使用某些附加功能。如果不具有对菜单项及其关联功能的许可权，那么将不显示。

从管理菜单 > 业务流程，UI 资源	许可权名称 / 许可权标识
业务流程 > 管理器	UI BP Manager (BPMANAGE) 和 UI Business Process (BUSINESS_PROCESS)
业务流程 > 监控器 > 高级搜索 > 业务流程	BusinessProcesses (PLTADM2) 和 UI BP Monitor (BPMONITOR)

从管理菜单 > 业务流程，UI 资源	许可权名称 / 许可权标识
业务流程 > 监控器 > 高级搜索 > SWIFTNET 关联	SWIFTNETCorrelation (GISADM9) 和 UI BP Monitor (BPMONITOR) 以及 UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
业务流程 > 监控器 > 高级搜索 > 数据流	DataFlows (GISADM1) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > 文档	Documents (GISADM2) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > 通信会话	Communication Sessions (GISADM3) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > 关联	Correlation (GISADM4) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > BPSS 关联	BPSSCorrelations (GISADM5) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > EBXML 关联	EBXMLCorrelation (GISADM6) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > EDI 关联	EDICorrelation (GISADM7) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 高级搜索 > EDIINT	EDIINT (STDSADM6) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 中央搜索	CentralSearch (GISADM10) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 当前进程	CurrentProcesses (PLTADM3) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 当前文档	CurrentDocuments (GISADM11) 和 UI BP Monitor (BPMONITOR)
业务流程 > 监控器 > 当前活动	CurrentActivities (PLTADM4) 和 UI BP Monitor (BPMONITOR)
业务流程 > 消息条目工作站	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

从管理菜单 > 贸易伙伴，UI 资源	许可权名称 / 许可权标识
贸易伙伴 > 设置 > 基本	UI Basic Trading Profile Setup (BASIC_SETUP)
贸易伙伴 > 设置 > 高级 > 身份	Identities (GISADM12) 和 UI Advanced Trading Profile Setup (ADVANCED_SETUP) 删除还需要 UI Delete Trading Partner 许可权 (TP_DELETE)
贸易伙伴 > 设置 > 高级 > 传输	Transports (GISADM13) 和 UI Advanced Trading Profile Setup (ADVANCED_SETUP) 删除还需要 UI Delete Trading Partner 许可权 (TP_DELETE)

从管理菜单 > 贸易伙伴，UI 资源	许可权名称 / 许可权标识
贸易伙伴 > 设置 > 高级 > 文档交换	DocumentExchange (GISADM14) 和 UI Advanced Trading Profile Setup (ADVANCED_SETUP) 删除还需要 UI Delete Trading Partner 许可权 (TP_DELETE)
贸易伙伴 > 设置 > 高级 > 交货渠道	DeliveryChannels (GISADM15) 和 UI Advanced Trading Profile Setup (ADVANCED_SETUP) 删除还需要 UI Delete Trading Partner 许可权 (TP_DELETE)
贸易伙伴 > 设置 > 高级 > 打包	Packaging (GISADM16) 和 UI Advanced Trading Profile Setup (ADVANCED_SETUP) 删除还需要 UI Delete Trading Partner 许可权 (TP_DELETE)
贸易伙伴 > 设置 > 高级 > 概要文件	Profiles (GISADM17) 和 UI Advanced Trading Profile Setup (ADVANCED_SETUP) 删除还需要 UI Delete Trading Partner 许可权 (TP_DELETE)
贸易伙伴 > 数字证书 > CA	UI CA Certs (CA_CERTS) 和 UI System Certs (SYSTEM_CERTS) UI System Certs 添加系统选项。
贸易伙伴 > 数字证书 > 可信	UI Trusted Certs (TRUSTED_CERTS)
贸易伙伴 > 数字证书 > 系统	UI System Certs (SYSTEM_CERTS)
贸易伙伴 > 文档包络 > 包络	Envelopes (STDSADM1) 和 UI Envelope (ENVELOPE)
贸易伙伴 > 文档包络 > 控制号	ControlNumbers (STDSADM2) 和 UI Envelope (ENVELOPE)
贸易伙伴 > 文档包络 > 事务注册	TransactionRegister (STDSADM3) 和 UI Envelope (ENVELOPE)
贸易伙伴 > 文档包络 > 控制号历史记录	ControlNumberHistory (STDSADM4) 和 UI Envelope (ENVELOPE)
贸易伙伴 > 文档包络 > EDI 序列校验队列	EDISequenceCheckQueue (STDSADM5) 和 UI Envelope (ENVELOPE)
贸易伙伴 > 合同	UI Contracts (CONTRACTS) 和 UI Advanced Trading Partner Setup (ADVANCED_SETUP)
贸易伙伴 > 代码列表	UI CodeLists (CODELISTS)
贸易伙伴 > AS2	UI AS2 Trading Profile Setup (AS2_SETUP)
贸易伙伴 > SSH > 远程概要文件	RemoteProfiles (ASSETADM1) 和 UI SSH
贸易伙伴 > SSH > 已知主机密钥	KnownHostKey (ASSETADM2) 和 UI SSH

从管理菜单 > 贸易伙伴，UI 资源	许可权名称 / 许可权标识
贸易伙伴 > SSH > 用户身份密钥	UserIdentityKey (ASSETADM3) 和 UI SSH
贸易伙伴 > SSH > 授权用户密钥	AuthorizedUserKey (ASSETADM4) 和 UI SSH
贸易伙伴 > AS3	UI AS3 Trading Profile Setup (AS3_SETUP)
贸易伙伴 > Odette FTP 伙伴概要文件 > 实体伙伴	OftpPhysicalPartner (ASSETOFTP1) 和 UI Adapter Utilities (ADAPTER_UTILITIES)
贸易伙伴 > Odette FTP 伙伴概要文件 > 实体伙伴合同	OftpPhysicalPartnerContract (ASSETOFTP3) 和 UI Adapter Utilities (ADAPTER_UTILITIES)
贸易伙伴 > Odette FTP 伙伴概要文件 > 逻辑伙伴	OftpLogicalPartner (ASSETOFTP2) 和 UI Adapter Utilities (ADAPTER_UTILITIES)
贸易伙伴 > Odette FTP 伙伴概要文件 > 逻辑伙伴合同	OftpLogicalPartnerContract (ASSETOFTP4)
贸易伙伴 > PGP > 服务器管理器	PGP Server Manager (ASSETADM55) 和 UI PGP Profile Manager (PGP)
贸易伙伴 > PGP > 发起方管理器	PGP Sponsor Manager (ASSETADM56) 和 UI PGP Profile Manager (PGP)
贸易伙伴 > PGP > 伙伴管理器	PGP Partner Manager (ASSETADM57) 和 UI PGP Profile Manager (PGP)

从管理菜单 > 部署，UI 资源	许可权名称 / 许可权标识
部署 > 服务 > 安装/设置	Installation/Setup (PLTADM9) 和 UI Services (SERVICES)
部署 > 服务 > 配置	Configuration (PLTADM10) 和 UI Services (SERVICES)、UI BP Manager (BPMANAGE)。对于 V5.2.4.3 和更高版本，还需要 UI Adapters StartStop。
部署 > 调度	UI Scheduler (SCHEDULER)
部署 > 映射	Maps (ASSETADM5) 和 UI_Maps
部署 > 标准	Standards (STDSADM7) 和 UI_Maps
部署 > 扩展规则库	ExtendedRuleLibraries (ASSETADM6) 和 UI_Maps
部署 > XSLT	UI XSLT (XSLT)
部署 > Web 扩展 > Web 资源	WebResources (GISADM19) 和 UI Web Extensions 以及 UI Web Services (WEB_SERVICES) UI Web Services 允许用户检入新的 Web 资源文件。

从管理菜单 > 部署，UI 资源	许可权名称 / 许可权标识
部署 > Web 扩展 > 实用程序	Utilities (GISADM20) 和 UI Web Extensions。 仅在从较低版本进行升级时可视。
部署 > 模式	UI Schemas (SCHEMAS)
部署 > Mailbox > 配置	Configuration (MBXADM1) 和 UI Mailbox (MAILBOX)
部署 > Mailbox > 虚拟根	VirtualRoots (MBXADM2) 和 UI Mailbox (MAILBOX)
部署 > Mailbox > 路由规则	RoutingRules (MBXADM3) 和 UI Mailbox (MAILBOX)
部署 > Mailbox > 消息	Messages (MBXADM4) 和 UI Mailbox (MAILBOX)
部署 > EBXML > BPSS	BPSS (ASSETADM7) 和 UI EBXML (EBXML)
部署 > EBXML> BPSS 扩展	BPSSExtension (ASSETADM8) 和 UI EBXML (EBXML)
部署 > EBXML > CPA	CPA (ASSETADM9) 和 UI EBXM (EBXML)
部署 > 资源管理器 > 资源标记	Resource Tags (PLTADM1) 和 UI Deployment (DEPLOYMENT)
部署 > 资源管理器 > 导入/导出	UI Import/Export (IMPORT_EXPORT)
部署 > 适配器实用程序 > SAP 套件构建器	SAPSuiteBuilder (ASSETADM10) 和 UI Adapter Utilities
部署 > 适配器实用程序 > Sap 路径 > Sap 路径	SAPRoutes (ASSETADM11) 和 UI Adapter Utilities
部署 > 适配器实用程序 > Sap 路径 > SapRouteXRef	SAPRouteXREF (ASSETADM12) 和 UI Adapter Utilities
部署 > 适配器实用程序 > BEATuxedo	BEATuxedo (ASSETADM13) 和 UI Adapter Utilities 如果不安装 BEATuxedo jar，将不显示菜单项。
部署 > 适配器实用程序 > SWIFTNET 路由规则	UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
部署 > 适配器实用程序 > SWIFTNET 服务概要文件	UI SWIFTNet Service Profile (SWIFTNET_SVC_PROFILE)
部署 > 适配器实用程序 > SWIFTNET 复制服务概要文件	UI SWIFTNet Copy Profile (SWIFTNET_COPY_PROFILE)
部署 > 适配器实用程序 > 锁定策略管理器	LockoutPolicyManager (ASSETADM50)
部署 > 适配器实用程序 > C:D 网络映射 > C:D 节点	CDNetmaps (ASSETADM51) 和 UI Adapter Utilities (ADAPTER_UTILITIES)
部署 > 适配器实用程序 > C:D 网络映射 > C:D 网络映射	CDNodes (ASSETADM52) 和 UI Adapter Utilities (ADAPTER_UTILITIES)
部署 > 适配器实用程序 > C:D 网络映射 > C:D 网络映射 X-REF	CDNetmapXref (ASSETADM53) 和 UI Adapter Utilities (ADAPTER_UTILITIES)
部署 > 适配器实用程序 > 策略配置	Adapter Policies (ASSETADM54)

从管理菜单 > 部署，UI 资源	许可权名称 / 许可权标识
部署 > 适配器实用程序 > 文件系统虚拟根	File System Virtual Root (ASSETADM58)
部署 > SSH 主机身份密钥	UI SSH Local Identity Key (SSH_LCL_ID_KEY) 和 UI SSH (SSH)
部署 > Web Service > 管理器	WebServicesManager (ASSETADM16) 和 UI Web Services (WEB_SERVICES)
部署 > Web Service > 模式映射	SchemaMappings (ASSETADM17)、UI Web Services (WEB_SERVICES) 和 UI EBXML (EBXML)
部署 > Web Service > WSDL 检入	WSDLCheckIn (ASSETADM18) 和 UI Web Services (WEB_SERVICES)
部署 > Web Service > 安全性令牌	SecurityToken (ASSETADM18) 和 UI Web Service (WEB_SERVICES)

从管理菜单 > e-Invoicing，UI 资源	许可权名称 / 许可权标识
e-Invoicing > 协议	eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT) 删除还需要 eInvoicing DELETE AGREEMENT (EINV_DELETE_AGREEMENT) 许可权。
e-Invoicing > 集成归档	eInvoicing Archive (EINVOICING_ARCHIVE) 和 eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE)
e-Invoicing > 配置	eInvoicing Configuration (EINVOICING_CONFIGURATION)

从管理菜单 > 操作，UI 资源	许可权名称 / 许可权标识
系统 > 故障诊断器	Troubleshooter (PLTADM17) 和 UI Operations (OPERATIONS)
系统 > 性能 > 调优	Tuning (PLTADM18) 和 UI Operations (OPERATIONS)
系统 > 性能 > 统计信息	Statistics (PLTADM19) 和 UI Operations (OPERATIONS)
系统 > 性能 > JVM 监控器	Perfdumps (GISADMIN27) 和 UI Operations (OPERATIONS)
系统 > 支持工具 > SQL 管理器	UI SQL Tool (SQLMANAGER)
系统 > 支持工具 > 支持案例	UI Support Case Tool (SUPPORT_CASE)
系统 > 日志	UI Logs (SYSTEM_LOGS)
系统 > 许可证	UI Licenses (LICENSES)
报告	UI Reports (REPORTS)
线程监控器	ThreadMonitor (PLTADM24) 和 UI Operations (OPERATIONS)
JDBC 监控器	JDBCMonitor (PLTADM25) 和 UI Operations (OPERATIONS) 以及 UI SQL Tool (SQLMANAGER)

从管理菜单 > 操作，UI 资源	许可权名称 / 许可权标识
归档管理器	UI Archive (ARCHIVE-UI) 和 UI Operations (OPERATIONS)、UI BP Manage (BPMANAGE) 以及 UI Business Process (BUSINESS_PROCESS)
锁管理器	UI Lock Manager (LOCK_MANAGER)
消息监控器	MessageMonitor (GISADM24) 和 UI Operations (OPERATIONS)
外围服务	UI Perimeter Servers (PSERVERS)
代理服务器	UI Proxy Servers (PROXYSERVERS) 和 Sterling B2B Integrator Admin 组

从管理菜单 > 帐户，UI 资源	许可权名称 / 许可权标识
组	UI Groups (GROUPS) 和 UI Accounts (ACCOUNTS)
许可权	Permissions (PLTADM27) 和 UI Accounts (ACCOUNTS)
用户帐户	UI User Accounts (USER_ACCOUNTS) 和 UI Accounts (ACCOUNTS)
密码规则	PasswordPolicy (PLTADM29) 和 UI Accounts (ACCOUNTS)
用户新闻	UserNews (GISADM25) 和 UI Accounts (ACCOUNTS)
我的帐户	MyAccount (PLTADM30)

预配置的许可权

系统中包含预配置的许可权。与定制许可权一样，预配置的许可权提供对系统中不同模块的访问权。

搜索许可权名称

您可以通过**管理**菜单搜索许可权。

关于此任务

要搜索许可权：

过程

1. 在**管理菜单**中，选择**帐户** > **许可权**。
2. 在"许可权"页面上，完成以下操作之一：
   - 在"搜索"下的**许可权名称**字段中，输入要搜索的部分许可权名称或完整的许可权名称，然后单击**执行！** "许可权"页面将列出与您的搜索标准相匹配的所有许可权。
   - 在"列出"下的**按字母顺序排列**字段中，选择**全部**或要搜索的许可权名称的开头字母，然后单击**执行！** "许可权"页面将列出与您的搜索标准相匹配的所有许可权。

创建许可权

如果已从先前版本的系统进行升级，那么缺省情况下现有许可权将设置为"其他"。您可能需要编辑每个许可权以应用新的许可权类型。

关于此任务

在开始之前，您需要了解以下信息：

字段	描述
许可权标识	要创建的许可权的许可权标识。许可权标识是要为其设置许可权的业务流程、XSLT 文档、Web 模板或资源的名称。在标识后包含资源的扩展。必需。 许可权标识： • 必须唯一。 • 区分大小写。 • 许可权标识必须与业务流程、XSLT 文档、Web 模板或资源的名称相匹配。如果许可权标识与资源名称不完全匹配，那么将无法锁定资源。
许可权名称	要创建的许可权的名称。必需。 许可权名称必须唯一。许可权名称区分大小写，例如，"Any document"和"Any Document"是两个不同的许可权名称。
许可权类型	要创建的许可权的许可权类型。必需项。许可权类型包括： • UI – 允许访问界面中的特定菜单项。 • Mailbox – 允许访问系统中的特定邮箱。 • 模板 – 允许访问特定 Web 模板。 • BP – 允许访问特定业务流程。 • 跟踪 – 允许访问特定文档跟踪选项。 • 社区 – 允许访问特定社区管理选项。 • Web Service • 服务 • eInvoicing • 其他 – 允许访问上述某种类型无法识别的资源。

要创建许可权：

过程

1. 在**管理菜单**中，选择**帐户 > 许可权**。
2. 单击**创建新许可权**旁边的**执行！**。
3. 在"许可权"页面中，输入**许可权标识**。
4. 输入**许可权名称**。
5. 选择**许可权类型**。
6. 单击**下一步**。
7. 复审许可权设置。
8. 单击**完成**。

编辑许可权名称

如果您需要更改许可权名称以更准确地反映许可权，请编辑许可权名称。许可权名称必须唯一，且区分大小写。不能更改许可权标识。如果需要编辑许可权标识，那么必须创建新的许可权。

关于此任务

要编辑许可权名称：

过程

1. 在**管理菜单**中，选择**帐户** > **许可权**。
2. 通过使用"许可权名称搜索"或"按字母顺序列出"来搜索要编辑的许可权，然后单击**执行！**。
3. 单击要编辑的"许可权"旁边的**编辑**。
4. 输入新的**许可权名称**。
5. 如有需要，更新许可权类型，然后单击**下一步**。
6. 复审许可权设置信息。
7. 单击**完成**。

删除许可权

您可以删除与用户帐户关联的许可权。删除许可权后，所有用户帐户便不能再使用该许可权。

关于此任务

如果要删除的许可权是与用户帐户关联的唯一许可权，那么必须编辑该用户帐户以使其与另一种许可权关联。如果没有至少使一种新的许可权与该用户帐户关联，那么该用户可以登录，但不能访问任何菜单项。

要删除许可权：

过程

1. 在**管理菜单**中，选择**帐户** > **许可权**。
2. 通过使用"许可权名称搜索"或"按字母顺序列出"来搜索要删除的许可权，然后单击**执行！**。
3. 在"许可权"页面中，针对要删除的许可权，单击**删除**。
4. 验证许可权信息是否与要删除的许可权相匹配，然后单击**删除**。

   系统将删除许可权并显示以下消息：

   系统更新已成功完成。

复审许可权名称和标识

您可以通过**管理**菜单复审许可权名称和标识。

关于此任务

要复审许可权名称和标识：

过程

1. 在**管理菜单**中，选择**帐户 > 许可权**。
2. 使用"许可权名称搜索"或"按字母顺序排列的列表"并单击**执行！**，搜索要复审的许可权。
3. 选择许可权。 此时将显示许可权名称和标识。

用户帐户

用户帐户根据组、许可权和密码规则进行定义，以便有助于提供安全的环境。此类型用户帐户定义被定义为基于角色的安全性模型。

在创建任何新的用户帐户之前，需要确定您的业务环境需要什么样的组、许可权以及密码规则。组、许可权和密码规则的分配是可选的。

仅具有创建许可权的帐户才能创建新的用户帐户。用户帐户任务包括：

- 创建用户帐户
- 搜索用户帐户
- 编辑用户帐户
- 删除用户帐户

缺省用户帐户许可权

将自动向用户帐户分配"我的帐户"和"管理 Web 应用程序"许可权。

以下许可权将自动分配给用户帐户：

- 我的帐户（许可权标识 PLTADM30）– 允许访问"我的帐户"页面（帐户 > 我的帐户）。
- 管理 Web 应用程序许可权（许可权标识 WebAppAdminPermission）– 用于访问其他 Web 应用程序。

请勿从用户帐户除去这些许可权。如果意外除去了这些许可权，请编辑"用户帐户"并保存。这样将恢复缺失的许可权。

用户帐户认证

用户帐户认证可以是本地认证或外部认证。

用户帐户认证可以是以下任意一项：

- 本地 - 针对数据库完成认证。
- 外部 - 针对 LDAP 服务器完成认证。外部认证不需要 LDAP 适配器，该适配器用于业务流程并支持使用 Java 命名目录接口 (JNDI) 与本地或远程 LDAP 服务器进行通信。如果不具有单点登录或 LDAP 的许可证，那么您创建的所有用户均为本地用户，并针对应用程序的数据库进行认证。要创建外部用户帐户，您必须具有单点登录或 LDAP 的应用程序许可证。

用户帐户创建核对表

您可以创建用户帐户。

使用此核对表来创建用户帐户：

任务	基于角色的安全性核对表	注释
1	创建新的许可权或复审预安装的预配置许可权。	
2	创建新组或复审预安装的组。	
3	创建要分配给用户的定制密码规则。	
4	如果使用的是外部认证，请针对外部认证设置环境。	
5	创建用户帐户并分配许可权、组和密码规则。	

针对外部用户帐户认证设置环境

如果要创建外部用户，那么可以指定备用认证方法（通常为 LDAP）。

关于此任务

在创建外部用户帐户之前，您必须：

过程

1. 停止 Sterling B2B Integrator。
2. 通过在 authentication_policy.properties.in 文件中添加或修改认证配置来指定备用认证方法。 属性需要遵循以下格式：authentication_4.*xxx*=*xxx*_value。
3. 输入 `setupfiles.sh`。
4. 启动 Sterling B2B Integrator。

搜索用户帐户

您可以通过**管理**菜单搜索用户帐户。

关于此任务

要搜索用户帐户：

过程

1. 在**管理菜单**中，选择**帐户** > **用户帐户**。
2. 请完成以下操作之一：
   - 在"搜索"下的**帐户名称**字段中，输入要搜索用户帐户的部分名称或完整名称，然后单击**执行！** "帐户"页面将列出与您的搜索标准相匹配的所有用户帐户。
   - 在"列出"下的**按字母顺序排列**字段中，选择**全部**或要搜索的用户帐户名称的开头字母，然后单击**执行！** "帐户"页面将列出与您的搜索标准相匹配的所有用户帐户。

创建用户帐户

通过**管理**菜单创建新用户帐户。

关于此任务

在开始之前，您需要了解您使用的是本地认证还是外部认证：

- 本地 – 针对应用程序数据库完成认证。缺省值。
- 外部 - 针对 LDAP 服务器完成认证。外部认证并不需要 LDAP 适配器，该适配器用于业务流程并使系统可以使用 Java 命名目录接口 (JNDI) 与本地或远程 LDAP 服务器进行通信。

如果要向此帐户分配一个或多个授权用户密钥，那么必须从贸易伙伴处获取这些密钥，并在创建用户帐户之前检入这些密钥。

注：当支持多种外语时，一个用户帐户不应与多种特定语言一起使用，以避免用户界面显示问题。

您还需要了解以下信息：

字段	描述
用户标识	要创建的用户帐户的用户标识。用户标识长度必须至少为 5 个字母数字字符。不允许使用特殊字符或标点符号。必需。 只有 MySQL 数据库在登录时不区分大小写。您应始终使用在拼写上唯一的标识，这样，用户便不会意外地使用其他用户的标识。
密码（仅限本地认证）	要创建的用户帐户的密码。密码长度必须至少为 6 个字母数字字符。允许使用特殊字符。对于本地用户，这是必需的。对于外部用户，将不显示此字段。
确认密码（仅限本地认证）	再次输入密码。对于本地用户，这是必需的。对于外部用户，将不显示此字段。
策略（仅限本地认证）	要与此用户帐户关联的密码规则。从列表中选择要关联的策略。可选项。对于外部用户，将不显示此字段。 系统将从用户首次使用该密码登录的日期开始计算截止日期。
认证主机（仅限外部认证）	要在其上认证用户的轻量级目录访问协议 (LDAP) 服务器。此字段中列出的服务器是在 authentication_policy.properties.in 文件中指定的。
会话超时	在必须再次登录前，您可以保持不活动状态的合计时间（以分钟计）。该时间以分钟为单位。必需。
辅助功能选项	用户帐户可访问的仪表板用户界面部分。可选。 以下是辅助功能选项： • 管理 UI – 仅访问仪表板中的"管理控制台"窗格。 • AS2 UI – 仅访问 AS2 Edition 界面。 • 仪表板 UI – 访问仪表板界面。可通过选择一种仪表板主题来进行优化。

字段	描述
仪表板主题	用户帐户可访问的预定义仪表板。如果将辅助功能选项设置为"仪表板 UI"，那么这是必需的。 以下是仪表板主题选项： • 缺省值 • 操作员 • 参与者 • 参与者赞助商 • 赞助商 • AFT
名	用户的名字。必需。
姓	用户的姓氏。必需。
电子邮件	用户的电子邮件地址。
传呼机	用户的传呼机号码。
首选语言	将值设置为**使用客户机应用程序设置**。 **注：**此值将指示 Sterling B2B Integrator 使用用户浏览器和/或客户机操作系统语言环境中指定的语言。 **注：** 这是缺省值。
经理标识	用户经理的用户标识。
身份	要与用户帐户关联的贸易伙伴的身份。只能有一个贸易伙伴与用户帐户关联。一个用户帐户可以与许多组关联，每个组都具有自己的贸易伙伴身份关联。这样，一个用户帐户便可以与多个贸易伙伴相关联。"身份"字段用于路由 Mailbox 中的消息。从列表中选择贸易伙伴身份。 缺省值是"中心组织"。

要创建用户帐户：

过程

1. 在**管理菜单**中，选择**帐户 > 用户帐户**。
2. 单击**创建新帐户**旁边的**执行！**。
3. 在"新建帐户"页面中，选择**认证类型**。
4. 输入**用户标识**。
5. 输入**密码**。
6. 确认密码。
7. 选择**策略**。
8. 输入**会话超时**。
9. 选择**辅助功能选项**。
10. 选择**仪表板主题**。

11. 单击**下一步**。
12. 在"SSH 授权用户密钥"页面上，分配一个或多个公用密钥。将这些密钥从**可用**窗格移动到**已分配**窗格，然后单击**下一步**。
13. 在"组"页面上，分配许可权组。将这些组名从**可用**窗格移动到**已分配**窗格，然后单击**下一步**。
14. 在"许可权"页面上，分配个别许可权。将这些许可权从**可用**窗格移动到**已分配**窗格，然后单击**下一步**。 缺省情况下，已选中与此用户分配到的组相关联的许可权。必需许可权包括"管理 Web 应用程序许可权"和"我的帐户"。
15. 在"用户信息"页面上，输入**名**。
16. 输入**姓**。
17. 输入**电子邮件地址**。
18. 输入**传呼机号码**。
19. 选择**首选语言**。选择值**使用客户机应用程序设置**。

    注：此值将指示 Sterling B2B Integrator 使用用户浏览器和/或客户机操作系统语言环境中指定的语言。
20. 输入**经理标识**。
21. 选择**身份**。
22. 单击**下一步**
23. 复审用户帐户设置。
24. 单击**完成**。 这样会创建用户帐户并显示以下消息：

    系统更新已成功完成。

    如果已创建了外部用户，请从系统注销，然后使用外部用户标识或帐户重新登录。在外部 LDAP 服务器上，系统将认证外部用户标识。

编辑用户帐户

您可以通过**管理**菜单编辑用户帐户。

关于此任务

注：当支持多种外语时，一个用户帐户不应与多种特定语言一起使用，以避免用户界面显示问题。

要编辑用户帐户，请完成下列步骤：

过程

1. 在**管理菜单**中，选择**帐户 > 用户帐户**。
2. 通过使用"搜索"或"列出"选项查找要编辑的用户帐户。
3. 针对要编辑的用户帐户，单击**编辑**。
4. 对此用户的认证类型执行任意更改。

   如果将认证类型从外部更改为本地，那么需要为用户创建密码。如果将认证类型从本地更改为外部，那么将无法更改用户的密码或密码规则。
5. 对**新密码**执行任意更改并确认新密码。
6. 对**策略**执行任意更改。

7. 对**会话超时**执行任意更改并单击**下一步**。
8. 对 **SSH 授权用户密钥**执行任意更改并单击**下一步**。
9. 执行任意组更改并单击**下一步**。
10. 执行任意许可权更改并单击**下一步**。

    您不能除去"管理 Web 应用程序许可权"或"我的帐户"。
11. 对用户信息执行任意更改并单击**下一步**。

    注：对于以受支持的外语显示用户界面的用户帐户，请验证是否将"首选语言"值设置为**使用客户机应用程序设置**。此值将指示 Sterling B2B Integrator 使用用户浏览器和/或客户机操作系统语言环境中指定的语言。
12. 复审用户帐户设置。
13. 单击**完成**。

删除用户帐户

您可以通过**管理**菜单删除用户帐户。

关于此任务

要删除用户帐户：

过程

1. 在**管理菜单**中，选择**帐户 > 用户帐户**。
2. 通过使用"搜索"或"列出"选项查找要删除的用户帐户。
3. 针对要删除的用户帐户，单击**删除**。
4. 单击**确定**。
5. 复审用户帐户设置。
6. 单击**删除**。 这样会删除所选用户帐户，并显示以下消息：

   系统更新已成功完成。

更新"我的帐户"信息

"我的帐户"信息与您的用户名和密码关联，所以当您登录时，将在"我的帐户"页面中显示您的个人信息。您可以编辑自己的帐户信息并更改登录到系统时看到的初始页面。

关于此任务

很多种情况下，个人帐户信息发生更改时都要求您编辑帐户信息。此外，出于安全目的，您可能需要更改密码。

注：当支持多种外语时，一个用户帐户不应与一个以上特定语言一起使用，以避免用户界面显示问题。

要更新您的帐户信息：

过程

1. 在**管理菜单**中，选择**帐户 > 我的帐户**。
2. 如果要更新您的帐户密码，在**旧密码**字段中，输入当前密码，并在**新密码**字段中输入新的密码。在**确认新密码**字段中再次输入新密码。

3. 在**名**、**姓**、**电子邮件**或**寻呼机**字段中输入任意更改。
4. 要更改分配给此帐户的 **SSH 授权用户密钥**，请将密钥从"可用"移动到"已分配"窗格。
5. 要更改**首选语言**，选择语言。

   注：对于以受支持的外语显示用户界面的用户帐户，请验证是否将该值设置为**使用客户机应用程序设置**。该值将引导 Sterling B2B Integrator 使用用户浏览器和/或客户机操作系统语言环境中指定的语言。
6. 要更改登录时显示的**欢迎页面**（管理员控制台主页），请从列表中选择。
7. 要更改"当前进程"页面上一次显示的进程数，请为**当前进程页面大小**选择新值。
8. 要更改"当前文档"页面上一次显示的文档数，请为**当前文档页面大小**选择新值。
9. 如果要复用浏览器窗口来启动快捷方式，请选择**复用窗口以启动快捷方式**。
10. 如果希望系统基于您之前输入的字符串自动完成搜索，那么选择**自动完成搜索**。
11. 如果希望系统记住搜索依据值，请选择**记住搜索依据值**。 该选项将保存每个"搜索"字段中上次输入的值。
12. 单击**保存**。 新帐户信息将保存，并显示以下消息：

    ```
    Your update has completed successfully.
    ```

用于登录的用户帐户用户出口（V5.2.5 和更高版本）

Sterling B2B Integrator 提供了 Active Directory 同步用户出口，这些用户出口可用于通过 Active Directory 代替 Sterling B2B Integrator 用户界面来管理您的用户帐户。可以在 IBM 服务客户洽谈期间通过 IBM 服务来配置这些用户出口。请与您的 IBM 销售代表联系以获取更多信息。

用户出口	描述
IUserLoginUserExit_preAuthenticate	用于在认证之前插入定制代码。
IUserLoginUserExit_postAuthenticateFail	用于在成功认证之后插入定制代码。
IUserLoginUserExit_postAuthenticateSuccess	用于在认证失败之后插入定制代码。

用于注销的用户帐户用户出口（V5.2.6 和 更高版本）

Sterling B2B Integrator 提供了 Active Directory 同步用户出口，这些用户出口可用于通过 Active Directory 代替 Sterling B2B Integrator 用户界面来管理您的用户帐户。可以在 IBM 服务客户洽谈期间通过 IBM 服务来配置这些用户出口。请与您的 IBM 销售代表联系以获取更多信息。

用户出口	描述
ILogoutUserExit_OnSessionInvalidate	用于在会话失效之前插入定制代码。

单点登录

单点登录

单点登录 (SSO) 是一个认证流程，支持用户访问若干应用程序，并且必须仅输入一个用户名和密码。在此之前，登录到每个应用程序的用户必须管理若干用户名和密码。

SSO 的用户认证不需要 LDAP 适配器，该适配器与业务流程结合使用以通过 Java 命名目录接口 (JNDI) 与本地或远程 LDAP 服务器进行通信。

Sterling B2B Integrator 通过两种途径允许 SSO，一是与 Netegrity SiteMinder 集成，一是其他单点登录应用程序和服务器上的 SSL 插件的定制实施类。

单点登录限制于以下组件：

- 管理界面
- 邮箱界面
- 仪表板界面
- 高级文件传输 (AFT) 界面
- MyAFT 界面

单点登录提供者缺省类

除仪表板之外的所有其他接口的 SSO 登录 URL 类似于普通的登录接口。仪表板接口 URL 是 http:Host:port/dashboard/sso.jsp。仪表板接口的请求头必须具有值 SM_USER=SSO User Name（或可在 security.properties 文件的 SSO_USER_HEADER 下配置该值）。

SSOProviderDefault 接口允许单点登录 (SSO) 插件处理 Netegrity SiteMinder 的单点登录功能。

您可以配置 SSO 以在用户从 SSO 会话注销后重定向到外部 HTTP 页面（而非 Sterling B2B Integrator 注销页面）。SSO 服务器的外部页面可以是登录或注销页面。

以下示例显示了 SSOProviderDefault.java 类：

```
package com.sterlingcommerce.server_name.security.authentication;
import javax.servlet.*;
import javax.servlet.http.*;
import com.sterlingcommerce.server_name.security.SecurityManager;
import com.sterlingcommerce.server_name.util.frame.log.Logger;
import java.util.Properties;
import com.sterlingcommerce.server_name.util.frame.Manager;
import java.util.*;
/**
 * Default Single Sign On implementation for ISSOProvider that will use
* Request Header to get SSO_USER
 *
 * @author developer name
 */
public final class SSOProviderDefault implements ISSOProvider  {
    private static final String CLASS_NAME = "SSOProviderDefault";
    private static final Logger LOG = SecurityManager.getInstance().getLogger();
    private static final Logger AUTHLOG =
            SecurityManager.getInstance().getAuthenticationLogger();
/**
* Authenticate SSO processing (login)
*
* @param Request : The http request.
*
* @return String : The SSO User ID if the authentication is passed
*                : null if authentication is denied
* << No Exception thrown for the default SSO Provider - Either have value or null >>
*/
public String authenticate(HttpServletRequest request)
                        throws SSOAuthenticationException, SSOException
```

```
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (AUTHLOG.debug) {
          AUTHLOG.logDebug(CLASS_NAME + " Authenticate user tag : " +
              SecurityManager.getInstance().getSSOAuthenticationHeader() +
              " value : " + sso_user);
    }
    return sso_user;
}
/**
 * AuthenticatePage SSO processing (Page)
 *
 * @param Request : The http request.
*
 * @return boolean : True if the SSO authentication on the Page is passed or no Page
 *                   authentication is needed because not enable or not SSO User.
 *                 : False if authentication is denied
 *                   (Must throw SSOException if return false!!!!)
 */
public boolean authenticatePage(HttpServletRequest request)
                          throws SSOAuthenticationException, SSOException
{
    return true; // Always pass Page Validation for SSOProviderDefault
    /*****  Uncomment if want to do SSO_USER_HEADER (SM_USER) check on Page
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (sso_user != null) {
       passed = true;
    } else {
       passed = false;
       throw new
   SSOAuthenticationException(ISSOProvider.REASON_SSO_AUTHENTICATION_FAILURE);
    }
    return passed;   ******/
}
/**
 * When user logs out, calling this to do any extra actions
*
 * @param Response : The http response
 * @param Request : The http request.
 * @param int reason : An id to to tell where we called from
* @param String : The String identify the session type: WS, DASHBOARD, MAILBOX,
 *            AFT, MYAFT, or null if don't know
*
 * @return boolean : True if executes sucessfully,
 *           False if not & should use default logout logic
 *
 */
public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
{
    HttpSession session = request.getSession(false);
    String forward = "SSO_FORWARD_URL";
    if (sessionType != null)   {
       forward = forward + ".";
       forward = forward + sessionType;
    }
    if (reason == REASON_GIS_SESSION_EXPIRED) {
       forward = forward + ".GIS_TIMEOUT";
    }
    else if (reason == REASON_LOGOUT)  {
       forward = forward + ".LOGOUT";
    }
    else {  // Others reason : send all to VALIDATION_FAILED
       forward = forward + ".VALIDATION_FAILED";
    }
```

```
    String forwardUrl = getForwardURLParameter(forward);
    if (AUTHLOG.debug) {
       AUTHLOG.logDebug(CLASS_NAME + " Forward properties: " + forward +
" is forwardUrl: " + forwardUrl);
    }
    if (forwardUrl != null) {
       try {
           // Dashboard Timeout - Use JSP to kick outof IFrame
           if ((reason == REASON_GIS_SESSION_EXPIRED)&&
  (sessionType != null) &&
               (sessionType.equalsIgnoreCase(DASHBOARD_SESSION))) {
              if (AUTHLOG.debug) {
                   AUTHLOG.logDebug(CLASS_NAME + " Set ExternalSsoUrl = "
                                                 + forwardUrl);  }
              request.setAttribute("ExternalSsoUrl", forwardUrl);
              return false; // Set to false, we need to handle redirect in JSP
           } else {
              response.sendRedirect(response.encodeRedirectURL(forwardUrl));
           }
       } catch (Exception e) {
           return false;
       }
       return true;
   }
   return false;   // Use default logic (ie: GIS Logout/Login Page)
}
}
```

单点登录插件组件

Sterling B2B Integrator 允许其他单点登录应用程序和服务器上的单点登录 (SSO) 插件的定制实施类。您必须在 security.properties 文件中添加实施类 SSO_AUTHENTICATION_CLASS.<n>=<New class entry>，以实施 SSO 插件。

您可以基于以下 ISSOProvider.java 接口类编写 SSO 插件的定制实施类。

SSOProvider.java 接口类

```
import javax.servlet.*;
import javax.servlet.http.*;
public interface ISSOProvider {
public static final int REASON_UNKNOWN = -1;
public static final int REASON_SSO_SESSION_EXPIRED = 1
public static final int REASON_HTTP_SESSION_EXPIRED = 2;
public static final int REASON_LOGOUT = 3;
public static final int REASON_SSO_AUTHENTICATION_FAILURE = 4;
public static final int REASON_GIS_AUTHENTICATION_FAILURE = 5;
public String authenticate(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
public boolean invalidate(HttpServletRequest request,
HttpServletResponse response, int reason, String sessionType)
throws SSOAuthenticationException;
public boolean authenticatePage(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
}
```

SSOException 类

```
public class SSOException extends Exception {
private int reason = -1;
public int getReason() { return reason; }
public void setReason(int reason) { this.reason = reason; }
}
```

SSOAuthenticationException 类

```
public class SSOAuthenticationException extends SSOException { }
```

用户认证方法

认证方法在登录期间进行初始化。认证方法在成功认证后返回用户标识。针对不成功认证，将抛出 SSOAuthenticationException。异常应包含相应的原因码和重定向页面以处理是否存在 SSO 头。如果 SSO 头不存在，那么控件将传递回系统登录屏幕。

页面认证方法

authenticatePage 方法将在每个页面上初始化。此方法中将处理源自 SSO 服务器的页面转换期间发生的任何附加验证。例如，您可以 ping SSO 服务器以检查 SSO 会话是否已超时。对于不成功认证，应抛出异常，其中应包含相应的原因码和重定向页面。

无效的 SSO 请求

用户注销，用户未能认证登录或页面，或者会话到期时将初始化 invalidate 方法。应该针对无效的 SSO 请求执行 HTTP 重定向方法。对于不成功的认证，将初始化以下方法：

- 如果 SSO 服务器认证成功，但 Sterling B2B Integrator 认证不成功，那么将使用原因码初始化 REASON_GIS_AUTHENTICATION_FAILURE 方法。
- 如果 SSO 服务器认证不成功，那么将使用原因码初始化 REASON_SSO_AUTHENTICATION_FAILURE 方法。
- 如果用户注销，那么将使用原因码初始化 REASON_LOGOUT 方法。
- 如果 HTTP 会话到期，那么将使用原因码初始化 REASON_HTTP_SESSION_EXPIRED 方法。
- 如果用户的 SSO 会话到期，那么将使用原因码初始化 REASON_SSO_SESSION_EXPIRED 方法。

使用 Netegrity SiteMinder 进行单点登录的核对表

在配置单点登录 (SSO) 之前，必须了解 SSO 和 Netegrity SiteMinder。

通过本核对表以使用 Netegrity SiteMinder 配置 SSO：

任务	使用 Netegrity SiteMinder 进行单点登录的核对表	注：
1	安装 Netegrity SiteMinder 并使用逆向代理服务器进行配置。	
2	配置属性文件以用于 Netegrity SiteMinder。	
3	配置 Netegrity 安全代理服务器。	
4	创建 Netegrity 服务器安全域。	

有关其他单点登录应用程序和服务器的 SSO 插件定制实施，请参阅"单点登录插件组件"。

使用 IBM Global High Availability Mailbox 进行单点登录（V5.2.6 或更高版本）

具有相应许可权的 Sterling B2B Integrator 用户可以通过从 Sterling B2B Integrator 单点登录来直接访问 IBM® Global High Availability Mailbox 管理工具，以管理 Global Mailbox。

开始之前

Sterling B2B Integrator 用户必须属于以下某个组，才能从 Sterling B2B Integrator 直接访问 Global Mailbox 管理工具：

- *MAILBOX*
- 部署
- *Mailbox* 管理员
- *Sterling B2B Integrator* 管理员

关于此任务

选择通过单点登录访问 Global Mailbox 管理工具后，将在新的 Web 浏览器标签中打开 Global Mailbox 的新会话，而 Sterling B2B Integrator 会话仍可用。

您只能从 Sterling B2B Integrator 通过单点登录来访问 Global Mailbox。如果您从 Global Mailbox 管理工具注销，那么您并未从您的 Sterling B2B Integrator 会话中注销。

如果要更改您的 Global Mailbox 管理员密码，必须直接登录至 Global Mailbox 管理工具。

限制：如果通过单点登录方式登录至 Global Mailbox 管理工具，那么不能更改 Global Mailbox 管理员密码，并且**管理员**菜单中的**更改密码**不可用。

要通过单点登录访问 Global Mailbox 管理工具：

过程

1. 从"管理控制台"页面，展开"管理菜单"中的**部署**。
2. 展开 **Global Mailbox**。
3. 选择 **Mailbox 管理**。
4. 单击**启动 Global Mailbox 管理工具**超链接以在 Global Mailbox 管理工具中打开新会话。

   切记：单击**启动 Global Mailbox 管理工具**超链接后，将在新 Web 浏览器标签中打开 Global Mailbox 的新会话。

配置属性文件以使用 Netegrity SiteMinder 进行单点登录

您可以配置属性文件以使用 Netegrity SiteMinder 进行单点登录。

关于此任务

要编辑 neo-ui.properties 和 security.properties 文件：

过程

1. 停止 Sterling B2B Integrator。
2. 浏览至 /*install_dir*/install/properties。
3. 打开 neo-ui.properties 文件。
4. 为每个接口添加关联的 SSO 条目。以下代码样本显示了相同 HTTP 站点的关联条目：

```
url.host=%(host)
url.port=10200
url.cm=http://%(host):10200/communitymanagement/
url.cm.sso=http://%(host):10200/communitymanagement/
url.ob=http://%(host):10233/onboard/
url.ws=http://%(host):10200/ws/
url.ws.sso=http://%(host):10200/ws/
url.dash.sso=http://%(host):10233/dashboard/
url.ds=http://%(host):10200/datastore/
url.help=http://%(host):10200/help/index.htm?context=webhelplocal&single=true&topic=
url.help.ja=http://%(host):10200/help_ja/index.htm?context=webhelplocal&single=true& topic=
url.dash=http://%(host):10233/dashboard/
portlet.refresh.interval.seconds=60
url.aft=http://%(host):10200/aft/
url.aft.sso=http://%(host):10200/aft/
url.dmi=http://%(host):10200/dmi/
url.dmi.sso=http://%(host):10200/dmi/
```

5. 保存并关闭 neo-ui.properties 文件。
6. 在文本编辑器中打开 /*install_dir*/install/properties/security.properties 文件。
7. 在 security.properties 中，找到 ## SSO Authentication 配置参数，如以下代码样本所示：

```
## SSO Authentication configuration
## enable sso authentication  (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true
## enable sso authentication on each Page (true, false) default=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false
## http header variable that contains externally authenticated userid
SSO_USER_HEADER=SM_USER
## List of SSOProvider Classes that are supplied to use - If SSO Authentication is
## enable, should have at least one class, the following is the default one that we
## supplied.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Will try to use this first
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Will try to use this if first
## one failed
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Will try to use this if second ## one failed too
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Will try to use this if all
## first –1 classes failed
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS OProviderDefault
## External Page for SSO when Logout (Specify the SSO Server external page for each of
## the cases)
## Example: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## After SSO User logout from Mailbox, instead of display the Mailbox Login Screen
## display IBM Web page.
SSO_FORWARD_URL.AFT.LOGOUT=
SSO_FORWARD_URL.MYAFT.LOGOUT=
SSO_FORWARD_URL.MAILBOX.LOGOUT=
SSO_FORWARD_URL.WS.LOGOUT=
SSO_FORWARD_URL.DASHBOARD.LOGOUT=
## Default handling for LOGOUT if don't know source
SSO_FORWARD_URL.LOGOUT=
## External Page for SSO when Timeout (Specify the SSO Server External page for each ## of the case)
SSO_FORWARD_URL.AFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MYAFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MAILBOX.GIS_TIMEOUT=
SSO_FORWARD_URL.WS.GIS_TIMEOUT=
SSO_FORWARD_URL.DASHBOARD.GIS_TIMEOUT=
## Default handling for TIMEOUT if don't know source
SSO_FORWARD_URL.GIS_TIMEOUT=
## External Page for SSO on Validation/Authentication failure (SSO User Validation
## Failed - At login or Page Validation)
SSO_FORWARD_URL.AFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=
SSO_FORWARD_URL.WS.VALIDATION_FAILED=
SSO_FORWARD_URL.DASHBOARD.VALIDATION_FAILED=
##Default handling for VALIDATION FAILED if don't know source
SSO_FORWARD_URL.VALIDATION_FAILED=
```

8. 以下是 ##SSO Authentication 配置条目，请对 SSO 参数执行以下更改：

参数	描述	随附值	新值
SSO_AUTHENTICATION_启用	启用或禁用 SSO。	False	True
SSO_USER_HEADER	Netegrity SiteMinder 或您的 SSO 应用程序配置的用户头名称。	SM_USER 这是 Netegrity SiteMinder 中的值。	必须与 Netegrity SiteMinder 或您的 SSO 应用程序中的条目相匹配。
SSO_PAGE_AUTHENTICATION_启用	启用或禁用每个页面上的 SSO 认证	False	True–认证每个页面上的 SSO。 仅在提供了定制 SSO 提供者类的情况下才更改该值。

参数	描述	随附值	新值
SSO_AUTHENTICATION_CLASS.n	用于提供认证支持的实现类。	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	从提供的 SSOProvider 类列表中选择。
SSO_FORWARD_URL URL	显示从 Mailbox 注销后提供的 URL 页面。否则显示缺省页面。	已注释 显示缺省页面。	提供 URL。

9. 保存并关闭 security.properties 文件。
10. 启动 Sterling B2B Integrator。

配置 Netegrity 安全代理服务器

您可以通过向 proxyrules.xml 文件添加转发规则来配置 Netegrity 安全代理服务器。

关于此任务

在配置 Netegrity 安全代理服务器之前，必须：

- 在服务器（例如 acme.si.com）上安装 Sterling B2B Integrator。
- 知道 Mailbox 浏览器界面 (MBI) 安装到的端口号。在相应转发规则中必须使用此信息。
- 知道 Sterling B2B Integrator 仪表板用户界面安装到的端口号。在相应转发规则中必须使用此信息。

要配置 Netegrity 安全代理服务器：

过程

1. 将 Sterling B2B Integrator 必需的转发规则添加到 /opt/netegrity/proxy-engine/conf/proxyrules.xml 文件。

   以下示例显示在添加转发规则以访问 Sterling B2B Integrator 组件后，完成的 proxyrules.xml 文件的外观：

```
<?xml version="1.0"?>
<?cocoon-process type="xslt"?>
<!DOCTYPE nete:proxyrules SYSTEM "file:////home/netegrity/proxy-engine/conf/dtd/proxyrules.dtd">
<!-- Proxy Rules-->
<nete:proxyrules xmlns:nete="http://acme.com/">
   <nete:cond criteria="beginswith" type="uri">
<nete:case value="/gbm">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/help">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/webxtools">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/mailbox">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/dashboard">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/portlets">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/datastore">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:default>
   <nete:forward>http://acme.portalserver.com$0</nete:forward>
</nete:default>
</nete:cond>
</nete:proxyrules>
```

2. 向 proxyrules.xml 文件添加以下行，以关闭安全代理服务器中的"跨服务器脚本编制"检查，因为 Sterling B2B Integrator 不支持"Netegrity 跨服务器脚本编制"策略实施。

```
# Web Agent.conf
<WebAgent>
...." existing web agent configuration parameters"
badurlchars=""
badcsschars=""
CSSChecking="NO"
</WebAgent>
```

3. 保存并关闭 proxyrules.xml 文件。

创建 Netegrity 策略服务器安全域

Netegrity 策略服务器管理员必须针对安全代理服务器转发的每个 URL 模式创建安全域。这些安全域需要指定必要的规则以进行认证和授权。

关于此任务

此外，必须配置安全代理服务器中的 Web 代理以与策略服务器通信。

针对所列的每个 URL 模式创建安全域：

URL 模式	支持访问：
/mbi/*	应用程序 Mailbox 界面
/dashboard/*	应用程序仪表板界面，使用 http://host:port/dashboard 格式

URL 模式	支持访问：
/datastore/*	数据存储组件
/portlets/*	仪表板界面中的应用程序 portlet 组件
/help/*	上下文相关帮助组件
/webxtools/*	Web 扩展实用程序
/gbm/*	图形化流程建模器组件

密码

密码规则

密码规则是您根据贵公司的安全策略制定并应用于不同用户帐户的安全性决策的集合。这些选项包括诸如密码有效天数以及密码最大和最短长度等等。

您可以使用密码规则在添加新用户时简化安全性操作。不用为各个用户添加个别策略，您可以创建一个密码规则并将其应用于需要相同访问权的所有用户。

创建密码规则后，您可以仅将其应用于内部用户帐户。这样使您在维护安全策略方面具有最大的灵活性。如果使用的是 LDAP，那么无法将密码规则应用到外部帐户。

密码规则的缺省值有：

参数	缺省值
策略标识	default_user
策略名称	缺省用户策略
有效天数	60
最小长度	6
最大长度	28
历史记录中保存的密码数量	5
需要包含特殊字符的密码	已选
首次登录尝试要求更改密码	已选

密码规则任务包括：

- 创建密码规则
- 搜索密码规则
- 编辑密码规则
- 删除密码规则
- 编辑锁定参数
- 编辑密码到期消息

定制密码规则

Sterling B2B Integrator 定制密码规则是一种安全功能，可用于添加更多的密码规则规则。这些额外的密码规则可以帮助您防止使用较弱且易受入侵的密码以及拒绝不符合规定的密码。

要启用该功能，您需要：

- 通过插入点实现某些定制 Java 代码。一旦启用，该插入点将用于系统中与密码规则关联的所有用户（这是全局设置）。
- 将 passwordPolicyExtensionImpl 属性添加到 customer_overrides.properties 文件。
- 将定制密码规则应用于用户帐户。

在应用缺省密码规则前，先应用定制密码规则扩展。如果密码违反了多个策略需求（一个由扩展类执行，另一个由缺省实现执行），那么只会向用户显示从扩展类返回的错误消息。

示例：密码规则示例

此示例显示了密码规则的可能设置。

例如，名为"测试"的密码规则可具有以下密码设置：

- 10 天有效期
- 长度最短为 10 个字符
- 长度最长为 20 个字符
- 必须至少具有两个特殊字符
- 在初始登录期间用户必须更改缺省密码
- 要保存在历史记录中的密码数量

使用先前示例，系统管理员为用户分配用户名和密码。用户使用提供的用户名和密码登录，并且会提示用户更改密码。如果用户提供的密码不符合长度至少为 10 个字符、至多为 20 个字符或包含至少两个特殊字符的条件，系统将提示用户进行更正。一旦用户更改密码后满足了密码规则中设置的所有条件，系统将保存新密码并允许用户访问。每个用户帐户只能拥有一个与其关联的密码规则，但可以将一个密码规则应用于多个用户帐户。

除了在界面中执行密码规则更改外，您还可以更改在锁定尝试登录的用户的用户帐户之前，该用户可经历的登录失败次数。

例如，如果将失败前的连续登录尝试次数设置为 3，并且您输入三次错误密码，那么您将不能使用该特定计算机登录。您可以使用具有系统访问权的任何其他计算机登录。

安装密码或口令

在安装期间，创建 Sterling B2B Integrator 安装的系统口令。该口令是长度超过 16 个字符的高度复杂的字符串。系统口令是启动系统和访问受保护系统信息所必需的。

能够更新或更改口令的唯一人员是创建/安装软件的人员。如果丢失或忘记口令，那么将无法启动系统。能够更新系统口令的唯一用户是执行安装的用户。

系统口令不是由系统存储的，但在 Windows 安装上除外，它以模糊格式存储在 security.properties 中以促进系统作为非交互式服务运行。在其他平台上，它可以以清晰格式存储在 security.properties 中，这样您无需在启动系统时在命令行上输入系统口令。但是，系统口令仅受操作系统文件访问控制保护。

定制策略密码核对表

您可以实施定制策略密码。

使用以下核对表来实施定制密码规则：

任务	定制策略密码核对表
1	针对测试、策略和扩展，在 <SI_Install_Dir> 内创建目录结构。
2	在扩展目录内创建 Java 类。
3	在 customer_overrides.properties 文件中指定用于实施密码规则的 Java 类（passwordPolicyExtensionImpl 属性）。
4	向类路径添加实现类 jar。
5	定义错误消息。

示例 - 定制策略密码

此示例显示了定制策略密码扩展。

这是定制策略密码扩展的示例。

接口 com.sterlingcommerce.woodstock.security.PasswordPolicyExtension 已添加到系统，如下所示：

```
public interface IPasswordPolicyExtension {
    /**
     * Implements extended validation on passwords and
returns null if password
     * validation is successful. If validation fails,
an error message key
     * that may be looked up in Login_*.properties* should
be returned.
     * @param password - The password string to validate
     * @param policyId - The PWD_POLICY.POLICY_NAME of
the policy associated with the user in case the extension needs
it.
     * @return String Return null if password validation
was successful, the error message key if password validation fails
     */
    public String validateNewPassword (String password,
String policyName);
}
```

从方法返回 null 表明已接受密码。返回其他内容意味着密码无效。

实现示例

```
package test.policy.extension;
import java.util.regex.Pattern;
public class PwdPolExtnImpl implements com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension
{
   public String validateNewPassword(String
pwd,
                  String policyName) {
           // Additional password validation checks
                  boolean match=Pattern.matches(".*[a-z].*",
pwd) && Pattern.matches(".*[A-Z].*", pwd) && (Pattern.matches(".*[0-9].*",
pwd) || Pattern.matches(".*[^A-Za-z0-9].*",pwd));
                  if (match==true) return null;
                  else return "nogood";
      }

}
```

搜索密码规则

您可以通过**管理**菜单搜索密码规则。

关于此任务

要搜索密码规则：

过程

1. 在**管理菜单**中，选择**帐户** > **密码规则**。
2. 在"密码规则"页面中，完成以下操作之一：
   - 在"搜索"下的**密码规则名称**字段中，输入要搜索的密码规则的部分名称或完整名称，然后单击**执行！** "密码规则"页面将列出与您的搜索标准相匹配的所有许可权。
   - 在"列出"下的**按字母顺序排列**字段中，选择**全部**或要搜索的密码规则名称的开头字母，然后单击**执行！** "密码规则"页面将列出与您的搜索标准相匹配的所有许可权。

创建密码规则

您可以创建密码规则以向用户帐户分配策略。无需将密码规则与用户帐户关联，但如果使其关联，将确实有助于管理安全性。

关于此任务

在开始之前，您需要以下信息：

字段	描述
策略标识	用于在数据库中标识密码规则的标识。
策略名称	当引用密码规则时在用户界面中显示的策略名称。
有效天数	用户密码有效的天数。缺省值为 0，表示密码永不到期。 如果提供 1 到 999 之间的一个值，此时间段到期时将提示用户更改密码。到期倒计数从向某用户帐户分配密码后，该用户第一次登录时开始计算。

字段	描述
最小长度	密码必须具备的最小长度。必需项。有效值为任意数字。该数字必须至少设置为数字 6。缺省值是 6。如果没有应用策略，系统将强制采用最小长度 6。
最大长度	密码可以具备的最大长度。必需项。有效值为任意数字。该数字必须至少设置为与最小长度相同的数字。缺省值是 28。
历史记录中保存的密码数量	数据库的 PWD_HISTORY 表中要为用户保存的密码数量。超过此密码数量后，日期最早的密码将从该表中除去，并可供用户复用。缺省值是 0。
需要包含特殊字符的密码	指定密码必须包含至少一个特殊字符。有效值包括数字、大写字母、!、、#、$、%、^、& 或 *。
首次登录尝试时要求更改密码	指定用户必须在初始登录后更改缺省密码。这将提示用户在第一次登录后更改密码。

要创建密码规则：

过程

1. 在**管理菜单**中，选择**帐户** > **密码规则**。
2. 单击**创建新密码规则**旁边的**执行！**。
3. 在"密码规则"页面中，输入**策略标识**。
4. 输入**策略名称**。
5. 输入**有效天数**。
6. 输入**最小长度**。
7. 输入**最大长度**。
8. 输入**历史记录中保存的密码数量**。
9. 如果要求密码包含特殊字符，请选中该复选框。
10. 如果要求用户在首次登录尝试后更改密码，请选中该复选框。
11. 单击**下一步**。
12. 复审密码规则设置。
13. 单击**完成**。

编辑密码规则

您可以通过**管理**菜单编辑密码规则。

关于此任务

要编辑密码规则：

过程

1. 在**管理菜单**中，选择**帐户** > **密码规则**。
2. 通过使用"搜索"或"列出"选项查找要编辑的密码规则。
3. 针对要编辑的密码规则，单击**编辑**。
4. 在"密码规则设置"页面中，执行相应更改并单击**下一步**。
5. 复审密码规则设置。

6. 单击**完成**。

   这样会显示以下消息：

   系统更新已成功完成。

删除密码规则

如果删除某密码规则，与该特定密码规则关联的用户帐户仍可登录，但将不会强制该用户更改密码。如果该用户确实更改了密码，将不针对新密码完成验证。

关于此任务

要删除密码规则：

过程

1. 在**管理菜单**中，选择**帐户** > **密码规则**。
2. 通过使用"搜索"或"列出"选项查找要删除的密码规则。
3. 针对要删除的密码规则，单击**删除**。
4. 在"确认"页面上，单击**删除**。

   这样会显示以下消息：

   系统更新已成功完成。

更改用户密码到期的天数

系统通过在管理控制台主页的"系统警报"部分中放置消息来通知您密码即将到期。系统管理员可以针对要通知的用户更改到期前的天数。

关于此任务

该消息说明您的密码将在特定天数后到期。每过一天，该数字将减 1，直到密码到期当日为止，届时将提醒您更改密码。

系统管理员可以在 ui.properties.in 文件中更改到期前的天数。您应在 ui.properties.in 文件中执行所有更改，而不是在 ui.properties 文件中执行更改。如果对 ui.properties 文件执行更改并重新启动系统，那么对 ui.properties 文件所执行的更改将会被 ui.properties.in 文件覆盖。

要更改密码到期的天数：

过程

1. 停止 Sterling B2B Integrator。
2. 浏览至 */install_dir*/install/properties。
3. 打开 ui.properties.in 文件。
4. 找到 MsgPwdExpires= 15 条目。
5. 将 15 更改为用户密码到期的新天数。
6. 保存该文件。
7. 浏览至 */install_dir*/install/bin。
8. 输入 **setupfiles.sh**。

9. 重新启动 Sterling B2B Integrator。 您在 ui.properties.in 文件中所执行的更改将应用到 ui.properties 文件中，并对所有用户帐户有效。

锁定后重置您的密码

如果您被锁定，可以使用任何其他计算机登录，等候 30 分钟至锁定到期，或者联系系统管理员解除锁定。

关于此任务

如果您被锁定：

- 使用其他具有系统访问权的任意计算机登录。
- 等候 30 分钟，锁定到期，允许您重试使用锁定计算机登录。
- 联系系统管理员通过"锁管理器"页面解除锁定。这样将允许您重试使用锁定计算机登录。

定义定制密码规则的错误消息

您可以定义定制密码规则扩展的错误消息。

关于此任务

错误消息将向用户通知密码规则，并列出拒绝密码更改的原因。定制密码错误消息在 Login_*language_dir*.properties_*uniqueID*_ext 文件中进行定义。如果没有提供特定于定制的文本，那么会将缺省错误消息返回给用户。
Login_*language_dir*.properties_*uniqueID*_ext 文件不是缺省系统代码的一部分。必须在初始系统安装后创建该文件，然后根据您的环境来填充该文件。

要定义定制密码规则扩展的错误消息：

过程

1. 浏览到 */install_dir*/install/properties/lang/*language_dir* 目录。 其中 *language_dir* 是针对客户语言环境设置的语言（例如，en、ja、fr）。
2. 编辑 Login_*language_dir*.properties_*uniqueID*_ext 文件。 其中 language_dir 是针对客户语言环境设置的语言，<filename> 是新的定制密码扩展的唯一标识。例如：Login_en.properties_custompasswd_ext。
3. 针对定制扩展文件中设置的错误条件向该文件添加条目，并定义要返回给用户的描述性字符串。 例如，nogood 表示密码必须包含最少一个小写字符、一个大写字符和一个数字或特殊字符。
4. 保存并关闭该文件。

在 customer_overrides.property 文件中指定"定制密码规则扩展"

您可以指定用于实施密码规则扩展的 Java 类。

关于此任务

要插入定制实施，需要在 customer_overrides.properties 文件的 passwordPolicyExtensionImpl 属性中指定 Java 类名。

要指定用于实施密码规则扩展的 Java 类：

过程

1. 浏览到安装目录。
2. 浏览到属性目录。
3. 编辑 customer_overrides.properties 文件。
4. 在文件末尾添加 passwordPolicyExtensionImpl 属性并输入用于实施密码扩展验证的 Java 类的名称。例如，security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl。
5. 保存并关闭该文件。

向定制密码规则的类路径添加实现类 JAR

对于定制密码规则，您必须向类路径添加实现类 JAR。

关于此任务

必须按如下所示对扩展实现类进行编译和将其保存为 jar 文件：

过程

1. 浏览至 *SI_Install_Dir*。
2. 输入以下命令来编译定制类文件：

   ```
   javac -cp /SI_Install_Dir/jar/platform_ifcbase/1_3/platform_ifcbase.jar test/policy/extension/*.java
   ```

3. 在 *SI_Install_Dir* 中运行以下命令来创建 jar 文件：

   `jar cf any_filename.jar absolute_path_to_custom_class_file.class` 其中，*any_filename*.jar 是要创建的新 jar 文件的名称，*absolute_path_to_custom_class_file*.class 是定制实现 Java 类文件的名称。例如：`jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class`

4. 浏览至 *SI_Install_Dir*/bin 目录。
5. 输入以下命令来向 classpath 添加新创建的 jar：

   ```
   ./install3rdParty.sh userExit 1_0 -j path_to_jar_that_was_created_in_step3
   ```

   例如，`./install3rdParty.sh userExit 1_0 -j SI_Install_Dir/userExit.jar`

LDAP 认证

作为 Sterling B2B Integrator 认证工具的轻量级目录访问协议 (LDAP)

轻量级目录访问协议 (LDAP) 是一组用于访问信息目录（即 LDAP 目录）中所存储信息的协议。

LDAP 目录是数据库，但不是关系数据库，用于管理在网络上的多个服务器间传播的信息，并针对读操作性能进行优化。

您可以使用 LDAP 向 LDAP 目录委派外部用户帐户的认证，并使用贵公司内其他应用程序使用的相同安全信息提供认证。如果贵公司已经采用了 LDAP，那么您可以使用现有的 LDAP 目录。

用户帐户认证不需要 LDAP 适配器，该适配器与业务流程结合使用以通过 Java 命名目录接口 (JNDI) 与本地或远程 LDAP 服务器进行通信。

如果您的 LDAP 服务器未在运行，那么具有内部帐户的用户将保留访问权；但是，具有外部帐户的那些用户将不具有访问权，直到 LDAP 服务器运行为止。

在 Sterling B2B Integrator 中配置 LDAP 之前，您必须具备以下条件：

- 了解 LDAP
- 能够访问包含用户信息的已安装并已配置的 LDAP 服务器
- LDAP 服务器的位置
- （适用于 SSL）密钥库和信任库中已安装了安全证书
- 已为每个将通过您的 LDAP 服务器进行认证的用户创建了外部用户帐户
- （适用于 SSL）密钥库和信任库的位置

示例：LDAP 认证配置参数

此示例显示 LDAP 认证配置参数。

以下示例显示 LDAP 认证配置参数：

```
## GIS/LDAP Authentication configuration
## optional ssl (jsse) java system properties for locating and using
## the trustStore and the keyStore
## one set of keystore and truststore properties for all LDAP configuration.
# LDAP_SECURITY_TRUSTSTORE=/home/applications/properties/cacerts
# LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# LDAP_SECURITY_KEYSTORE=/home/applications/properties/keystore
# LDAP_SECURITY_KEYSTORE_PASSWORD=password
#########################################################################
#
# GIS Authentication Configuration
#
#########################################################################
authentication_0.className=com.sterlingcommerce.woodstock.security
.GISAuthentication
authentication_0.display_name=GIS Authentication
#########################################################################
#
# For additional LDAP Server Authentication Configuration,
# copy-paste the following set of properties and uncomment all properties
# that start with "authentication_<number>". Replace the <number>
# tag with the additional number for the authenticationmethod. For example,
# if the last authentication method is "authentication_0", then you should
# replace the <number> tag with "1" for your next new LDAP authentication
# method.
# Then you have to change each property with the properLDAP server information.
#
# You can comment out or leave blank the "authentication_<number>
# .security_protocol"
# property if you are not going to use SSL for the security protocol.
#
# The authentication_1 LDAP authentication propertieswould be replaced if
# the customer already used LDAP authentication as configuredin security
# .properties.
#
```

```
#########################################################################
#########################################################################
#
# LDAP Server <number> Authentication Configuration
#
#########################################################################
# authentication_<number>.className=com.sterlingcommerce.woodstock.security
# .LDAPAuthentication
# authentication_<number>.display_name=LDAP Serveragrona <number>
## enable ldap authentication  (true, false) default=false
# authentication_<number>.enabled=true
## jndi parameters for ldap connections
# authentication_<number>.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
# authentication_<number>.server=acme.inc.com
# authentication_<number>.port=636
# authentication_<number>.security_type=simple
# authentication_<number>.principle=cn=Manager,dc=acme,dc=inc,dc=com
# authentication_<number>.credentials=SecretPassword
## comment out or leave as blank on this property if the server is not
## going to use SSL for the security protocol.
# authentication_<number>.security_protocol=ssl
## search parameters for user password
# authentication_<number>.password_attribute=userPassword
# authentication_<number>.search_root=dc=acme,dc=inc,dc=com
# authentication_<number>.search_filter=(uid=<userid>)
# authentication_<number>.with_user_bind=falseBelow the ##LDAP Authentication
```

LDAP 认证配置核对表

您可以使用 Sterling B2B Integrator 配置 LDAP。

使用此核对表以在 Sterling B2B Integrator 中配置 LDAP：

任务	**LDAP 配置核对表**
1	通过以下某种方式配置 LDAP： • 密码比较方式 • 密码二进制方式
2	在 Sterling B2B Integrator 中配置 LDAP
3	验证 LDAP 配置
4	可选项。加密 LDAP 密码。

以密码绑定方式配置 LDAP

您可以通过输入外部帐户的**用户标识**和**密码**，以密码绑定方式配置 LDAP。

关于此任务

要以密码绑定方式配置 LDAP：

过程

输入外部用户帐户的**用户标识**和**密码**。 系统将：

- 尝试使用支持执行必要查询的凭证来绑定到 LDAP 存储库。
- 在 LDAP 目录中搜索具有适当用户标识的用户。
- 从 LDAP 目录中检索用户的专有名称 (DN)。
- 尝试使用用户的 DN 和密码来绑定到 LDAP 存储库。

- 成功 – 系统作为用户绑定到 LDAP 存储库。
- 失败 – 系统无法作为用户绑定到 LDAP 存储库。

以密码比较方式配置 LDAP

您可以密码比较方式配置 LDAP。

关于此任务

要以密码比较方式配置 LDAP：

过程

1. 输入外部用户帐户的**用户标识**和**密码**。
2. 系统尝试使用支持执行必要查询的凭证来绑定到 LDAP 存储库。
3. 系统在 LDAP 目录中搜索具有适当用户标识的用户。
4. 系统从 LDAP 目录中检索用户密码。
5. 系统将用户提供的密码与从 LDAP 目录中检索到的密码进行比较。如果密码匹配，那么您将通过认证并且允许您访问系统。如果密码不匹配，那么您将不能通过认证并且不允许您访问系统。

在 Sterling B2B Integrator 中配置 LDAP

要配置 Sterling B2B Integrator 以使用 LDAP，必须编辑 authentication_policy.properties.in 文件。您还可以使用 customer_overrides.properties 文件来设置不能被补丁安装覆盖的属性值。

关于此任务

要配置 LDAP 认证：

过程

1. 停止 Sterling B2B Integrator。
2. 浏览到安装目录。
3. 浏览到属性目录。
4. 打开 authentication_policy.properties.in 文件。
5. 在 authentication_policy.properties.in 中，找到 ## GIS/LDAP Authentication 配置条目。
6. 以下是 ##GIS/LDAP Authentication 配置条目，请对 LDAP 参数执行以下更改：

参数	描述	随附值	更改为
#LDAP_SECURITY_TRUSTSTORE	到本地信任库的路径。信任库中必须存储了需要 LDAP 的证书。不能使用来自贸易伙伴的证书。可选项。仅在使用 SSL 时使用此项。	Inactive path	到本地信任库的完整路径。
#LDAP_SECURITY_TRUSTSTORE_PASSWORD	用于访问信任库的密码。可选项。仅在使用 SSL 时使用此项。	changeit	用于访问本地信任库的密码。

参数	描述	随附值	更改为
#LDAP_SECURITY_ KEYSTORE	到本地密钥库的路径。密钥库中必须存储了需要 LDAP 的证书。不能使用来自贸易伙伴的证书。可选项。仅在使用 SSL 时使用此项。	Inactive path	到本地密钥库的完整路径。
#LDAP_SECURITY_ KEYSTORE_ PASSWORD	用于访问密钥库的密码。可选项。仅在使用 SSL 时使用此项。	password	用于访问本地密钥库的密码。
#authentication_ <number>. enabled	启用或禁用 LDAP。 False – 将禁用从该认证主机创建的所有用户（无法登录）。 True – 可以从内部或外部访问每个用户，但不能同时从内部和外部进行访问，因为每个用户标识都是唯一的。如果是进行内部认证，将不检查此值。	False	True
#authentication_<number> .jndi_factory	用于创建 LDAP 服务提供者初始上下文的工厂类的类名。这是 JDK 随附的标准上下文工厂。	com.sun. jndi.ldap. LdapCtx Factory	无更改
#authentication_ <number>.server	用于指定 LDAP 服务器主机名的 URL。	Inactive path	本地 LDAP 主机 URL。
#authentication_ <number>.port	LDAP 服务器的端口号。		
#authentication_ <number>. security_type	供提供者使用的认证方法。系统仅支持简单认证。	simple	无更改
#authentication_ <number>. principle	要认证的主体的身份，系统通过该主体可执行查询。此参数是 LDAP ASN.1 绑定请求中的名称部分。	cn=Manager, dc=amr, dc=stercomm, dc=com	本地命名信息。
#authentication_ <number>. credentials	LDAP 存储库中为 LDAP 主体设置的密码，系统通过该主体可执行查询。	SecretPassword	本地主体配套的本地密码。
#authentication_ <number>. security_protocol	用于指定供提供者使用的安全协议的对象。	SSL	无更改。如果选择了不使用 SSL，那么此参数不可视。

参数	描述	随附值	更改为
#authentication_ <number>. password_attribute	包含用户密码的 LDAP 属性的名称。 仅在将 #LDAP_ AUTHENTICATE_ WITH_USER_BIND 设置为 false 时才使用此参数。	userPassword	包含密码的本地属性。
#authentication_ <number>. search_root	用于指定用户查询所基于的根目录的对象。	dc=amr, dc=stercomm, dc=com	本地搜索路径。
#authentication_ <number>.search_filter	用于指定要在搜索中使用的模板的对象。<userid> 值在请求时将动态替换为请求认证的用户的用户标识。	(uid=<userid>)	Windows Active Directory 服务器可能会使用如下条目： (sAMAccount Name=<userid>)
#authentication_ <number>. with_user_bind	指定是否根据成功绑定来认证用户。 False – 系统从 LDAP 服务器抽取用户密码的值，并将其与提供的用户凭证进行比较。 True – 系统使用用户的专有名称和提供的凭证绑定到 LDAP 服务器。成功绑定意味着认证成功。	false	如果要通过用户绑定进行认证，那么将其更改为 true。

7. 保存 authentication_policy.properties.in 文件。
8. 输入 */install_dir*/install/bin/setupfiles.sh (UNIX) 或 *install_dir*\install\bin\setupfiles.cmd (Windows) 以将 LDAP 条目从 authentication_policy.properties.in 文件更新到 authentication_policy.properties 文件。
9. 启动 Sterling B2B Integrator。

   这样会应用对 authentication_policy.properties 文件的更改，并且您现在可以开始使用 LDAP 服务器来认证用户。

   启动后，系统将通过 authentication_policy.properties 文件来识别 LDAP 服务器。外部用户登录时，系统将对其进行认证。

验证 LDAP 配置

要验证是否在 Sterling B2B Integrator 中正确配置了 LDAP，请复审"用户认证"下的 Authentication.log 文件以确保系统接受了 LDAP 配置。

关于此任务

如果连接到 LDAP 目录时发生问题或 LDAP 认证失败，请检查 Authentication.log 文件中的 DEBUG 日志语句以对问题进行故障诊断。Authentication.log 文件记录了所有成功和不成功的登录尝试。

对 LDAP 密码加密

通过在 customer_overrides.property 文件中对 LDAP 相关密码进行加密，可以在属性文件中将这些密码隐藏。

关于此任务

以下参数/属性可用于在 customer_overrides.properties 文件中对 LDAP 密码加密：

参数/属性	描述
authentication_policy.authentication_1.credentials	此参数或属性管理访问 LDAP 实例所必需的主体密码。应对该项给予保护，因为不应以纯文本形式暴露用于管理安全性和访问的密码。
authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD	此参数或属性管理用于保护 LDAP 连接的信任库密码（JKS 格式）。必须提供此 JKS 的口令，以便能够访问信任库，因为信任库是加密文件。
authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD	此参数或属性管理在使用基于客户机的 SSL 认证来保护与给定 LDAP 实例的连接时使用的密码。

要加密 LDAP 密码：

过程

1. 浏览至 bin 目录。
2. 使用 encrypt_string.[sh/cmd] 来确定要加密的属性/参数的实际值。
3. 更新 customer_overrides.properties 文件中的参数/属性以使其具有以下条目。使用 bin/encrypt_string.sh（或 .cmd）将所有 <ENCVAL> 替换为针对该属性注释掉的非加密字符串的加密值。例如：

```
authentication_policy.LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/../
woodstock2/com/sterlingcommerce/woodstock/security/units/cacerts
# non-encrypted
#authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# encrypted
authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=<ENCVAL>
authentication_policy.LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/../woodstock2/
com/sterlingcommerce/woodstock/security/units/keystore
# non-encrypted
#authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=password
# encrypted
authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=<ENCVAL>
authentication_policy.authentication_2.display_name=LDAP Server agrona 2
authentication_policy.authentication_2.enabled=true
authentication_policy.authentication_2.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
authentication_policy.authentication_2.server=agrona.sci.local
authentication_policy.authentication_2.port=18100
authentication_policy.authentication_2.security_type=simple
authentication_policy.authentication_2.principle=cn=Manager,dc=amr,dc=stercomm,dc=com
# non-encrypted
#authentication_policy.authentication_2.credentials=Sterling
```

```
# encrypted
authentication_policy.authentication_2.credentials=<ENCVAL>
authentication_policy.authentication_2.security_protocol=ssl
authentication_policy.authentication_2.password_attribute=userPassword
authentication_policy.authentication_2.search_root=dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_2.search_filter=(uid=<userid>)
authentication_policy.authentication_2.with_user_bind=false
authentication_policy.authentication_2.className=com.sterlingcommerce.woodstock.security
.LDAPAuthentication
```

用户新闻

用户新闻

用户新闻功能使您能够向"管理员控制台"主页发布消息。用户新闻可通知用户有关重要事件和任务的更改情况，或就重要事件和任务提醒用户。

可针对以下人员发布消息：

- 所有用户
- 特定用户
- 多个用户

新闻项将根据生效日期和截止日期显示。您还可以将消息设置为：

消息类型	符号	描述
注意		提供一般优先级或低优先级的声明信息。
警报		提供高优先级的声明信息。

您必须具备"帐户"的写许可权才可创建用户新闻消息。删除旧消息可降低存储需求和检索特定消息所需的工作量。

用户新闻任务包括：

- 针对特定用户创建用户新闻消息
- 针对所有用户创建用户新闻消息
- 搜索用户新闻消息
- 编辑用户新闻消息
- 删除用户新闻消息

针对所有用户创建用户新闻消息

您可以通过**管理**菜单为所有用户创建用户新闻消息。

关于此任务

在开始之前，您需要了解以下信息：

字段	描述
类型	要创建的消息的类型。有效值包括"通知"和"警报"。
主题	要创建的消息的主题。

字段	描述
消息	要创建的消息的正文。

过程

1. 在**管理菜单**中，选择**帐户** > **用户新闻**。
2. 单击**新建消息**旁边的**执行！**。
3. 输入**类型**。
4. 输入**主题**。
5. 输入**消息**。
6. 单击**下一步**。
7. 选择**所有用户**并单击**下一步**。
8. 输入消息的**生效日期** (yyyy-mm-dd)。
9. 输入消息的**截止日期** (yyyy-mm-dd)。
10. 单击**下一步**。
11. 复审新闻消息设置。
12. 单击**完成**。

针对特定用户创建用户新闻消息

您可以通过**管理**菜单为特定用户创建用户新闻消息。

关于此任务

在开始之前，您需要了解以下信息：

字段	描述
类型	要创建的消息的类型。有效值包括"通知"和"警报"。
主题	要创建的消息的主题。
消息	要创建的消息的正文。

过程

1. 在**管理菜单**中，选择**帐户** > **用户新闻**。
2. 单击**新建消息**旁边的**执行！**。
3. 输入**类型**。
4. 输入**主题**。
5. 输入**消息**。
6. 单击**下一步**。
7. 选择**所选用户**。
8. 选择希望接收此消息的每个用户的名称。
9. 单击**下一步**。
10. 输入消息的**生效日期** (yyyy-mm-dd)。
11. 输入消息的**截止日期** (yyyy-mm-dd)。
12. 单击**下一步**。

13. 复审新闻消息设置。
14. 单击**完成**。

搜索用户新闻消息

您可以通过**管理**菜单搜索用户新闻消息。

关于此任务

要搜索用户新闻消息：

过程

1. 在**管理菜单**中，选择**帐户** > **用户新闻**。
2. 使用以下某个"搜索选项"：

用户新闻搜索选项	Action
按用户标识	从列表中选择"全部"或特定用户。
按主题	输入部分消息文本。
按生效日期范围	输入日期范围 (mm/dd/yyyy)。

3. 单击**执行！** "用户新闻"页面将列出与您的搜索标准相匹配的所有消息。

编辑用户新闻消息

您可以通过**管理**菜单编辑用户新闻消息。

关于此任务

要编辑用户新闻消息：

过程

1. 在**管理菜单**中，选择**帐户** > **用户新闻**。
2. 搜索要编辑的用户新闻消息。
3. 针对要编辑的用户新闻消息，单击"编辑"。
4. 如有需要，更新消息类型、主题或消息。
5. 单击**下一步**。
6. 如有需要，更新将接收此消息的用户，并单击**下一步**。
7. 如有需要，更新消息的**生效日期** (yyyy-mm-dd)。
8. 如有需要，更新消息的**截止日期** (yyyy-mm-dd)。
9. 单击**下一步**。
10. 复审新闻消息设置。
11. 单击**完成**。

删除用户新闻消息

您可以通过**管理**菜单删除用户新闻消息。

关于此任务

要删除用户新闻消息：

过程

1. 在**管理菜单**中，选择**帐户** > **用户新闻**。
2. 搜索要删除的用户新闻消息。
3. 针对要除去的新闻消息，单击**删除**。
4. 复审新闻消息设置。
5. 单击**删除**。 这样会显示以下消息：

   系统更新已成功完成。

文档加密

文档加密功能概述

文档加密是 Sterling B2B Integrator 随附的功能，可在传统文件和数据库许可权之外配置额外的安全层。如果将 Sterling File Gateway 与 Sterling B2B Integrator 集成，那么将使用相同的文档加密功能在休眠时保护数据。

Sterling File Gateway 是一个用于在使用不同协议、文件命名约定和文件格式的伙伴间安全传输文件的应用程序。

文档加密功能用于在休眠时保护数据免遭盗用。该功能允许您对数据库和/或文件系统中存储的有效内容数据执行加密。该功能还用于防止系统外部人员通过直接访问数据库或文件系统来查看有效内容数据。

文档加密的重要方面：

- 安装时的缺省配置是不加密。如果要对您的文档加密，那么将需要开启该功能。
- 您可以随时开启该功能，但仅对开启加密后收到的文档加密。
- 一旦开启该功能，加密将针对整个系统中的所有有效内容。
- 仅加密文档有效内容数据，**不加密**元数据。
- 使用同一加密密钥进行加密和解密。
- 系统使用预定义的证书 (doccrypto) 来加密文档。您可以创建其他系统证书。如果创建了其他系统证书，那么必须更新 customer_overrides.properties 文件中 CERT_NAME 的值。

虽然启用加密后性能会受到影响，但是每个客户将看到不同的性能影响，具体取决于硬件、所处理文档的数量和大小，以及相对于其他活动，给定服务器执行文档持久保存和检索所耗用的相对处理时间量。

文档加密的加密密钥

将使用同一加密密钥来加密和解密数据库或文件系统文档。数字证书用于生成并加密密钥，系统口令用于加密数字证书。

文档加密对每个文档创建一个密钥，该密钥随文档一起存储为元数据的一部分。数字证书与任何其他系统证书的存储方式一样。

系统使用预定义的证书 (doccrypto) 来生成并加密用于加密文档的密钥。您可以创建其他系统证书。如果创建了其他系统证书，那么必须更新 customer_overrides.properties 文件中 CERT_NAME 的值。

为文档加密分配其他证书

系统使用预定义的证书 (doccrypto) 来加密文档。您可以创建其他系统证书以供加密文档使用（例如，如果之前的证书已过期）。如果创建了其他系统证书，那么必须更新 customer_overrides.properties 文件中 CERT_NAME 的值。

关于此任务

警告：请勿删除或重新命名之前的系统证书。您需要之前的证书用以解密之前用该证书加密的文档。您的新系统证书无法解密这些文档，因为从来没有用该系统证书加密过文档。

在执行本过程之前，您需要：

- 生成新的证书
- 知道证书的名称

要更新 CERT_NAME 的值：

过程

1. 浏览到安装目录。
2. 浏览到属性目录。
3. 打开 customer_overrides.properties 文件。
4. 向文件添加以下行：

   ```
   security.CERT_NAME=name_of_new_system_certificate
   ```
5. 保存并关闭 customer_overrides.properties 文件。
6. 停止并重新启动 Sterling B2B Integrator。

针对文件系统和数据库文档启用文档加密

您可以从属性目录对文件系统和数据库文档进行加密。

关于此任务

要对文件系统和数据库文档加密：

过程

1. 浏览到安装目录。
2. 浏览到属性目录。
3. 打开 customer_overrides.properties 文件。
4. 将以下行添加到该文件中。

   ```
   security.ENC_DECR_DOCS=ENC_ALL
   ```
5. 保存并关闭 customer_overrides.properties 文件。
6. 停止并重新启动 Sterling B2B Integrator。

针对数据库文档启用文档加密

您可以从安装目录对数据库文档加密。

关于此任务

要对数据库文档加密：

过程

1. 浏览到安装目录。
2. 浏览到属性目录。
3. 打开 customer_overrides.properties 文件。
4. 将以下行添加到该文件中。

   ```
   security.ENC_DECR_DOCS=ENC_DB
   ```
5. 保存并关闭 customer_overrides.properties 文件。
6. 停止并重新启动 Sterling B2B Integrator。

针对文件系统文档启用文档加密

您可以从安装目录对文件系统文档加密。

关于此任务

要对文件系统文档加密：

过程

1. 浏览到安装目录。
2. 浏览到属性目录。
3. 打开 customer_overrides.properties 文件。
4. 将以下行添加到该文件中。

   ```
   security.ENC_DECR_DOCS=ENC_FS
   ```
5. 保存并关闭 customer_overrides.properties 文件。
6. 停止并重新启动 Sterling B2B Integrator。

针对文档禁用文档加密

您可以从属性目录禁用文档加密。

关于此任务

安装时的缺省配置是不加密。

要禁用文档加密：

过程

1. 浏览到安装目录。
2. 浏览到属性目录。
3. 打开 customer_overrides.properties 文件。
4. 将 ENC_DECR_DOCS 的值更新为 NONE。 例如：

```
security.ENC_DECR_DOCS=NONE
```

5. 保存并关闭 customer_overrides.properties 文件。
6. 停止并重新启动 Sterling B2B Integrator。

证书

数字证书

使用 IBM Key Management Utility (iKeyman) 可帮助您管理数字证书。

系统使用以下类型的数字证书：

- CA 证书和可信证书 – 系统不具有其专用密钥的数字证书。这些证书以标准 DER 格式进行存储。
- 系统证书 – 其专用密钥保存在系统中的数字证书。这些证书与专用密钥以安全格式存储在一起。

以下是有关如何使用数字证书的一些基本信息：

- 每个交换安全文档的组织都必须具有证书。可使用 iKeyman 生成证书或从外部生成。有关 iKeyman 的信息，请参阅第 58 页的『IBM Key Management Utility (iKeyman)』。
- 与您交换已签名且加密的文档的贸易伙伴的每个贸易概要文件都必须具有证书。
- 一个组织或贸易概要文件一次只能具有一个活动的证书。如果要使用双证书，组织可以具有一对活动的证书：一个用于签名，一个用于加密。
- 组织或贸易概要文件必须具有活动证书才能成功交换已签名且加密的文档。
- 组织或贸易概要文件可以具有多个有效证书。
- 证书可用于签署通过各种传输方法传输的文档。
- 证书的密钥长度不必与贸易伙伴证书的密钥长度相同。
- 在为证书设置有效期之前，建议您阅读并应用 Microsoft PKI Quick Guide 中的最佳实践建议。要了解有关使用证书的最佳实践建议的相关信息，请参阅 http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

受支持的数字证书

Sterling B2B Integrator 支持版本 3 的 X.509 数字证书。数字证书可以是自签名证书或 CA 签名证书。

- 自签名证书是一种使用与证书中的公用密钥相对应的专用密钥签署的数字证书，表明发行者具有与证书中的公用密钥相对应的专用密钥。
- CA 签名证书是一种使用由认证中心保存的密钥签署的数字证书。在发放证书前，CA 通常会评估证书请求者以确定该请求者实际是否为证书中引用的证书持有者。

CA 证书

CA 证书是认证中心 (CA) 发放的数字证书。CA 将验证可信根的可信证书。可信根是在证书中构建信任链的基础。

信任某 CA 根意味着您将信任该 CA 发放的所有证书。如果选择不信任某 CA 根，那么 Sterling B2B Integrator 将不会信任该 CA 发放的任何证书。

CA 证书包含与专用密钥相对应的公用密钥。CA 拥有专用密钥并使用该专用密钥来签署自己发放的证书。要验证可信证书，必须首先检入 CA 证书。

公共 CA 的根证书包含在 Sterling B2B Integrator 随附的 JVM 中的 Java 密钥库 (JKS) 中。与以前必须要在 CA Web 站点搜索并获取证书相比，现在这样可允许用户更轻松地建立一些基于权限的信任关系。

CA 证书与可信证书在产品中分开进行存储。

在用户界面中，您可以检入来自以下任意源的 CA 根证书：

- Sterling B2B Integrator 随附的位于 JKS 密钥库中的公共 CA 根证书。
- 仅能识别证书和可信证书。证书和专用密钥未显示在 UI 中。
- 从贸易伙伴导入的 SSL 证书。
- 从外部获取的其他证书。

根据您站点的安全策略，JKS 密钥库中的 CA 证书还可以通过控制台检入。尽管 CA 证书是公共文档，但对于谁有权添加 CA 证书这一点，您仍必须保持谨慎。某些人可能会恶意添加虚假的 CA 证书从而达到验证虚假的最终用户证书的目的。

CA 证书名称

CA 证书名称并不是证书内容的一部分。它们是使用证书的发行者"相对专有名称"(RDN) 和序列号构建而成。但是，JKS 密钥库中的证书是使用任意字符串命名的。

由于证书名称存储在系统数据库中，并用作引用 GUI 中的证书的别名，因此您可能希望根据您的文件命名约定以使用较短或更有意义的名称来重命名 CA 证书。在检入或编辑证书时可对其进行重命名。

自签名数字证书和 CA 签名数字证书的优势

根据您的需要，自签名证书和 CA 签名数字证书各有利弊。

当您和您的贸易伙伴在决定是要生成自签名证书还是从 CA 购买已签名证书时，请考虑以下内容：

- 您可以使用 Sterling B2B Integrator 轻松创建自签名证书。但是，这些自签名证书未经可信的第三方验证。
- 使用 CA 证书的主要优势在于证书持有者的身份是经过可信的第三方验证的。劣势包括导致额外的成本和管理工作。如果决定使用第三方证书，请从 CA 获取。
- CA 提供了发布和获取证书相关信息（包括有关已撤销证书的信息）的集中信息来源。

缺省情况下，系统会信任所有 CA 证书和应用程序生成的自签名证书。然而，您可以指定应信任特定 CA 发放的所有还是部分证书。您还可以明确指明不信任某个贸易伙伴的自签名证书。

证书截止日期

如果适配器和 servlet 用于入站通信，那么必须监控系统证书的截止日期以确保证书有效。在证书到期前，必须将其替换为有效证书。

系统证书参数定义

如果适配器和 servlet 用于入站通信，那么必须监控系统证书的截止日期以确保证书有效。在证书到期前，必须将其替换为有效证书。

参数	描述
alias	HSM 中存储的密钥名称。仅使用包含字符 a-z、A-Z、0-9 或连字符 (-) 且其总长度不超过系统 GUID 长度的别名名称。
certname	要分配给数据库中的系统证书的名称。
Certtype	要导入的证书类型。支持四种类型的证书文件：pkcs12、pkcs8、pem 和 keystore。Sterling B2B Integrator 仅支持使用 DES 或 3DES 加密的 pem 密钥。 使用 keystore 可列出或导入密钥库。
file	要导入的文件的名称。
keypass	Eracom 设备上的插槽的 PIN。
keystoretype	要导入的密钥库类型。有效值为 CRYPTOKI。
keystoreprovider	提供者类型。Eracom 是唯一受 HSM 支持的提供者类型。 有效值为： • ERACOM • ERACOM.n（如果要将证书导入到第一个位置以外的插槽）
password	证书文件的存储口令。
pkcs12file	要导入的 PKCS12 文件的名称。
pkcs12storepass	用于生成 PKCS12 文件的存储口令。
pkcs12keypass	PKCS12 文件的有效口令。
storepass	密钥库所在的 Eracom 设备上的插槽的 PIN。
systempass	系统口令。

IBM Key Management Utility (iKeyman)

IBM Key Management Utility (iKeyman) 是可生成密钥、证书请求和自签名证书的 IBM SDK 的一个组件。

您可以使用 iKeyman 创建证书以保护通信，对数据进行加密和解密。在使用 SSL 的安全传输中，证书提供增强级别的安全性。

在 Sterling B2B Integrator 中，您可以使用 iKeyman 创建：

- 证书签署请求 (CSR) – 要通过电子邮件发送到认证中心以请求 X.509 证书的文件。
- 密钥证书 – ASCII 编码的证书和 ASCII 编码的 PKCS12 加密专用密钥的组合。如果利用标准格式（缺省值）以使用某些密码来生成密钥证书，那么在将输出证书导入 Sterling B2B Integrator 中时会发生错误。 PKCS12 是密钥证书的推荐格式。

有关配置和使用 iKeyman 的更多信息，请参阅针对 IBM SDK, Java Technology Edition 7.0.0 的 iKeyman 概述

证书任务

创建自签名证书

您可以通过**管理**菜单创建自签名证书。

关于此任务

要创建自签名证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 单击**创建自签名证书**旁边的**执行！**。
3. 输入自签名证书的**名称**。
4. 输入源**组织**的名称。
5. 选择自签名证书的**国家或地区**或者源。
6. 输入组织中负责证书的人员的联系**电子邮件**地址，然后单击**下一步**。
7. 输入证书的**序列号**。 序列号是要分配给自签名证书的编号。
8. 输入自签名证书有效的天数（**持续时间**）。

   注：在 V5.2.6.2 或更高版本中，最迟到期日期为 *2080* 年 *1* 月 *1* 日。如果输入的任何持续时间将导致到期日期超出 2080 年 1 月 1 日，那么到期日期缺省为 *2080* 年 *1* 月 *1* 日。在较早发行版中，没有上限。
9. 在"主题备用名称"字段中输入要与证书关联的网络接口的 **IP 地址**。
10. 在"主题备用名称"字段中输入要与证书关联的网络接口的 **DNS 名称**。
11. 选择**密钥长度**。选择以下某个密钥长度：
    - 512
    - 1024
    - 2048

    注：密钥长度 1024 可提供安全性、互操作性和效率之间的良好平衡。密钥长度 2048 是最安全的，但也是最慢的，并且可能对某些应用无效。

    注：如果选择密钥长度 512，还必须使用 JDK 7 SR5。JDK 7 SR7 FP1 不支持低于 1024 的密钥长度。
12. 选择**签名算法**。
13. 选择**使用时进行验证**选项。验证选项包括：
    - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
    - 认证链 – 为没有自签名的证书构造信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
14. 通过选中相应复选框以设置**证书签名位**。

15. 单击**下一步**。
16. 复审自签名证书的相关信息。
17. 单击**完成**。

自动从贸易伙伴获取可信证书

"证书捕获实用程序"将自动执行从贸易伙伴获取 SSL 证书的过程。这种获取证书信息的方法允许伙伴轻松连接和保存证书。

关于此任务

如有需要，可在将证书作为 CA 或可信证书检入系统之前执行频带外安全检查。

开始之前：

- 验证您伙伴的主机系统是否启用 SSL。
- 获取贸易伙伴服务器的主机和端口信息。
- 如果将使用 FTPS 方式，那么请确定是显式方式还是隐式方式。
- 配置缺省 SSLCertGrabberAdapter 服务实例以使用相应的外围服务器和（仅限 HTTPS）代理服务器。请参阅适配器文档以了解详细信息。

要自动从贸易伙伴获取 SSL 证书：

过程

1. 在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 证书捕获实用程序**。
2. 在**捕获伙伴证书**旁边，单击**执行！**
3. 选择服务器的连接类型，然后单击**下一步**。
   - FTPS
   - HTTPS
4. 输入**主机名**或 **IP 地址**。
5. 输入**端口**号。
6. 选择 FTPS 连接方式（如果使用的是 HTTPS，请跳过此步骤）：
   - 显式 - 建立 FTP 连接后进行 SSL 协商。缺省值。
   - 隐式 - 建立 FTP 连接前进行 SSL 协商。
7. 单击**下一步**。 系统尝试连接并检索证书。
8. 捕获完成后，复审摘要信息并确定要保存哪些证书。
9. 为每个证书选择编码方法，然后单击**保存**。编码格式有：
   - BASE64 - 在标准 DER 证书上使用 BASE64 编码。缺省值。
   - DER - 大多数应用程序都接受的数字证书标准格式。
10. 单击**保存**并浏览到要保存文件的位置。
11. 接受缺省文件名，或者根据您的文件命名约定进行编辑，然后单击**保存**。
12. 保存后，可以将证书检入到系统中。如果决定将证书检入系统：
    a. 验证每个证书是否有效且可信。
    b. 将证书作为 CA 或可信证书检入系统，具体取决于功能。对于基于认证中心的信任，您可能需要检入证书链，不包括最终用户证书。对于直接信任，检入最终用户证书。

配置证书摘要上的状态信息

缺省情况下，如果选择了以超链接形式显示的证书名称，那么将在摘要弹出窗口底部提供证书状态信息。您可以包含或排除状态信息。由于状态信息是实时编译的，您可能不希望将其包含在内。

关于此任务

VerificationOnPopupInfo 属性控制是否在证书摘要中显示状态信息。该属性位于 ui.properties 文件中。VerificationOnPopupInfo 属性的值包括：

- true - 包含验证信息（缺省值）
- false - 不编译验证信息或不在弹出窗口中显示验证信息
- （任何其他值）- 包含验证信息

要防止编译和显示状态信息：

过程

1. 打开 ui.properties 文件。
2. 将 VerificationOnPopupInfo 的值更新为 false。例如：

   ```
   VerificationOnPopupInfo=false
   ```

3. 保存并关闭该文件。
4. 重新启动 Sterling B2B Integrator。

配置拇指纹显示

除了预先计算的 SHA1 Hash 外，还可以在证书显示、确认和摘要屏幕中包含额外的证书拇指纹。可在生成显示时根据需要执行 Hash 计算。

关于此任务

附加拇指纹显示在 GUI 屏幕上，但不影响消息处理或系统通信。

要配置系统以计算和显示附加证书拇指纹：

过程

1. 在 ui.properties 文件中，修改以下行：

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   要显示多个附加 Hash，请使用逗号分隔这些值。例如：

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

参数	描述
hash_algorithm	要应用到证书拇指纹的 Hash 算法的名称。有效值为： • SHA-256 • SHA-384 • SHA-512

2. 保存并关闭 ui.properties 文件。
3. 重新启动 Sterling B2B Integrator。

搜索 CA 证书

您可以通过**管理**菜单搜索 CA 证书。

关于此任务

要搜索 CA 证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > CA**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 请完成以下操作之一，然后单击**执行!**
   - 在"搜索"下的**按证书名称**字段中，输入要搜索的 CA 证书的部分名称或完整名称。"CA 数字证书"页面将列出与您的搜索标准相匹配的所有 CA 证书。
   - 在"列出"下的**按字母顺序排列**字段中，选择**全部**或要搜索的 CA 证书名称的开头字母。选择"全部"将列出所有 CA 证书。"CA 数字证书"页面将列出与您的搜索标准相匹配的所有 CA 证书。

查看 CA 证书摘要信息

显示证书列表时，可以单击证书名称以查看与该证书有关的摘要信息。您可以配置系统名称、拇指指纹和状态。

关于此任务

系统中可配置以下字段。

证书摘要字段	描述
系统名称	"证书名称"是数据库标签。用于在 GUI 中指代该证书并将该名称存储在自己的数据库中。 JKS 密钥库证书的缺省名称是任意字符串。其他证书名称是利用发行者的相对专有名称 (RDN) 和证书序列号构建的。 检入或编辑证书时可以将证书名称更改为较短或更具识别性的名称。
拇指指纹	缺省情况下包含 SHA1 Hash 的信息。要为其他 Hash 配置拇指指纹信息的计算和显示，请编辑 ui.properties 文件。
状态	当前状态的实时检查，表明证书日期是否有效以及证书是否经过验证。要配置显示时是否计算该信息，请编辑 ui.properties 文件。

尽管该信息适用于 CA 证书的摘要信息，但对于其他类型的证书，相似字段仍会出现在摘要和确认屏幕上。

从用户界面检入 CA 证书

您可以从**管理**菜单下的用户界面来检入 CA 证书。

关于此任务

根据您站点的安全策略，JKS 密钥库中的 CA 证书还可以通过控制台检入。

在开始之前，请将从外部获取的所有 CA 证书保存到一个本地文件中。

要检入 CA 证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > CA**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 单击**检入新证书**旁边的**执行！**。
3. 选择导入证书的方法：

导入方法	后续步骤
从 JVM 导入 – 从 JKS 密钥库导入	1. 单击"从 **JVM 导入**"。 2. 接受密码字段中显示的缺省密码，然后单击**下一步**。 缺省密钥库密码由 Sun Microsystems 提供。如果密码字段为空，系统仍使用缺省密码。
从文件导入 – 导入保存为本地驱动器上的文件的证书	1. 单击"从**文件导入**"。 2. 输入文件名，或者单击**浏览**以选择 CA 证书文件。单击"下一步"。 您可以忽略密码字段中显示的密码。无需清除该条目。

   这样会列出包含识别信息摘要的可用证书。缺省情况下，会选中所有证书。
4. 单击每个条目左侧的复选框以选中或取消选中要导入的证书。
5. 对于每个选定的证书，接受建议的证书名称或根据您的文件命名约定编辑该名称。
6. 选择**使用时进行验证**选项并单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 尝试为没有自签名的证书构造直达根的信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
7. 如果收到表明证书与数据库中已存在的某个证书重复的消息，请输入 Y 或 N 以指示是否要导入重复证书。

   该检查仅针对单一证书执行。在从文件检入一个或多个证书时将不执行该检查。

   证书通过 SHA1 Hash 来标识，以用于确定重复项。数据库中可以存在证书的多个副本，因为每个副本将填充到不同的行中，并具有不同的对象标识。将不会覆盖现有证书。
8. 复审 CA 证书信息。

9. 单击**完成**。

从控制台检入 CA 证书

在将任何 CA 证书保存到本地文件之后，您可以在控制台从安装目录检入 CA 证书。

关于此任务

公共 CA 证书包含在 JKS 密钥库中，该密钥库属于 Sterling B2B Integrator 随附的 JVM。JKS 密钥库位于 /install_dir/jdk/jre/lib/security/cacerts 中。您也可以从外部获取证书。

要将证书导入 Sterling B2B Integrator 可信存储库，请修改 /install_dir/install/bin/ImportCACerts.sh (UNIX) 或 \install_dir\install\bin\ImportCACerts.cmd (Windows) 中的命令。

在开始之前，请将从外部获取的所有 CA 证书保存到一个本地文件中。

要在控制台检入 CA 证书：

过程

1. 浏览到安装目录。
2. 浏览至 bin 目录。
3. 输入以下命令：

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   将列出文件中的所有证书（一次列出一个），但存在以下例外情况：
   - 不处理或不列出包含对称密钥或专用密钥的条目。
   - 仅处理和列出 DER 格式文件中的第一个证书。
4. 根据提示，对要导入的任意证书输入 Y（不区分大小写）。
5. 对于每个接受的证书，接受建议的证书名称或根据您的文件命名约定编辑该名称。
6. 如果证书标签与数据库中已存在的标签重复，请输入 `Y` 或 `N`（不区分大小写）以指示是否要更改标签。 尽管证书通常不是由标签来标识，且数据库允许标签重复，但某些服务是根据标签来查找证书。避免重复标签以避免发生意外行为的可能性。
7. 如果证书与数据库中已经存在的证书重复（由证书的 SHA1 Hash 指示），请指定 Y 或 N 以指示是否要导入重复证书。

   证书通过 SHA1 Hash 来标识，以用于确定重复项。数据库中可以存在证书的多个副本，因为每个副本将填充到不同的行中，并具有不同的对象标识。将不会覆盖现有证书。

编辑 CA 证书

您可以通过**管理**菜单编辑 CA 证书。

关于此任务

要编辑 CA 证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > CA**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 使用"搜索"或"列出"查找要编辑的 CA 证书，然后单击**执行！**。
3. 单击要编辑的 **CA 证书**旁边的**编辑**。
4. 输入证书名称。
5. 选择**使用时进行验证**选项并单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 为没有自签名的证书构造信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
6. 复审 CA 证书信息。
7. 单击**完成**。

删除 CA 证书

您可以通过**管理**菜单删除 CA 证书。

关于此任务

要删除 CA 证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > CA**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 单击**按字母顺序排列**旁边的**执行！**。
3. 单击要删除的 CA 证书旁边的**删除**。

搜索系统证书

您可以通过**管理**菜单搜索系统证书。

关于此任务

要搜索系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 在系统证书中，请完成以下操作之一，然后单击**执行！**

- 在"搜索"下的**按证书名称**字段中，输入要搜索的系统证书的部分名称或完整名称。"系统证书"页面将列出包含您输入的完整或部分名称的所有系统证书。
- 在**列出**下的**按字母顺序排列**字段中，选择**全部**或要搜索的 CA 证书名称的开头字母。选择"全部"将列出所有系统证书。"系统证书"页面将列出与您的搜索标准相匹配的所有系统证书。

编辑系统证书

您可以通过**管理**菜单编辑系统证书。

关于此任务

要编辑系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 使用"搜索"或"列出"查找要编辑的**系统证书**，然后单击**执行！**。
3. 单击要编辑的系统证书旁边的**编辑**。
4. 输入**证书名称**。
5. 选择**使用时进行验证**选项并单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 为没有自签名的证书构造信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
6. 复审系统证书信息。
7. 单击**完成**。

确定 Sterling B2B Integrator 中的系统证书

您可以通过**管理**菜单确定系统证书。

关于此任务

要确定系统证书：

过程

1. 在**管理菜单**中，选择**部署 > 服务 > 配置**。
2. 在"列表"部分中，从**按服务类型**列表中选择适用的服务或适配器类型，然后单击**执行！**
3. 在配置列表中，选择配置。
4. 单击**服务名称**以查看配置信息。
5. 复审证书摘要信息。

检查系统证书的截止日期

如果适配器和 servlet 用于入站通信，那么必须监控系统证书的截止日期以确保证书有效。

关于此任务

要检查系统证书的截止日期：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 要查看所有系统证书，请从按字母顺序排列的下拉列表中选择**全部**并单击**执行！**。
3. 选择要查看的系统证书名称。 这样会显示"证书摘要"。
4. 在"证书摘要"的**描述**部分中，请复审**生效日期**字段中提供的信息。
5. 如果日期有效且证书已经过验证，请复审**状态**部分中提供的信息。

在 Sterling B2B Integrator 中导出系统证书

此导出命令仅适用于 Sterling B2B Integrator 系统证书。不能使用此命令在 HSM 上导出系统证书。

关于此任务

要导出系统证书，请输入带有适当参数的以下命令：

```
./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass
```

参数	描述
keyname	要导出的系统密钥的密钥名称。
pkcs12filename	包含导出信息的文件的名称。
pkcs12storepass	用于保护存储的存储密码。
pkcs12keypass	用于保护密钥的密钥密码。

删除 Sterling B2B Integrator 中的系统证书

在删除系统证书前，可以将系统证书副本导出到本地磁盘。OpsDrv、OpsKey 和 UIKeys 是不能删除的系统证书。

关于此任务

要删除系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。

2. 单击**按字母顺序排列**旁边的**执行！**。
3. 单击要删除的系统证书旁边的**删除**。
4. 在"确认"页面上，单击**删除**。

检出系统证书

要导出系统证书，必须检出该证书。此过程仅导出公用证书（而非专用密钥），并为您提供要发送给贸易伙伴的公用证书。

关于此任务

要检出系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 使用"搜索"或"列出"查找要检出的系统证书。
3. 单击要检出的系统证书旁边的**检出**。
4. 在**检出系统证书**对话框中，选择证书格式，然后单击**执行！**：
   - PKCS12 – 此选项会将数字证书格式化为 PKCS12 文件。您还可以选择输入专用密钥密码和密钥库密码。
   - BASE64 – 此选项对标准 DER 证书使用 BASE64 编码。
   - DER – 大多数应用程序都可以接受数字证书的这种标准格式。
5. 在**文件下载**对话框中，单击**保存**。
6. 在**另存为**对话框中，选择要用于保存证书的位置，然后单击**保存**。 不支持证书打开选项。必须在操作系统中打开证书。如果收到错误消息"这是无效的安全证书文件"，请在文本编辑器中打开该文件并删除 -----BEGIN CERTIFICATE----- 之前的所有空白行。保存已编辑的文件，然后尝试打开该文件。
7. 在"检出系统证书"对话框中，单击**关闭**。 这样会显示"系统证书"页面。

搜索可信证书

您可以通过**管理**菜单搜索可信证书。

关于此任务

要搜索可信证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 可信**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 在"可信数字证书"页面上，请完成以下操作之一，然后单击**执行！**
   - 在"搜索"下的**按证书名称**字段中，输入要搜索的可信证书的部分名称或完整名称。"可信数字证书"页面将列出与您的搜索标准相匹配的所有可信证书。

- 在"列出"下的**按字母顺序排列**字段中，选择**全部**或要搜索的可信证书名称的开头字母。"可信数字证书"页面将列出与您的搜索标准相匹配的所有可信证书。

检入可信系统证书

您可以检入可信证书，如从贸易伙伴导入的 SSL 证书或其他外部证书。

关于此任务

可信证书可能来自以下源：

- 从贸易伙伴导入的 SSL 证书
- 从外部获取的其他证书

在开始之前，将可信系统证书保存到本地计算机上的一个文件中。

要检入可信系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 可信**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 单击**检入新证书**旁边的**执行！**。
3. 输入**文件名**或单击**浏览**以选择可信证书的文件名，然后单击**下一步**。
4. 输入**证书名称**。
5. 验证要检入的可信证书的名称。 对于每个选定的证书，"证书名称"字段都显示建议名称，后跟证书中识别信息的摘要。您可以根据您的文件命名约定更改该名称。
6. 如果所选文件中包含多个可信证书，那么选中每个证书左侧的复选框以检入所有证书。
7. 选择**使用时进行验证**选项并单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 尝试为没有自签名的证书构造直达根的信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
   - CRL 高速缓存 – 控制每次使用系统证书时是否参考 CRL 高速缓存。
8. 复审可信证书信息。
9. 单击**完成**。

编辑可信证书

您可以通过**管理**菜单编辑可信证书。

关于此任务

要编辑可信证书：

过程

1. 请选择一项：

- 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 可信**。
- 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。

2. 使用"搜索"或"列出"查找要编辑的可信证书，然后单击**执行！**。
3. 单击要编辑的可信证书旁边的**编辑**。
4. 输入**证书名称**。
5. 选择**使用时进行验证**选项并单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 尝试为没有自签名的证书构造直达根的信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
   - CRL 高速缓存 – 控制每次使用系统证书时是否参考 CRL 高速缓存。
6. 复审证书信息。
7. 单击**完成**。

删除可信系统证书

您可以通过**管理**菜单删除可信系统证书。

关于此任务

要删除可信系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 可信**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 单击**按字母顺序排列**旁边的**执行！**。
3. 单击要删除的可信证书旁边的**删除**。

导入 PKCS12 系统证书

您可以导入 PKCS12 系统证书。

关于此任务

要导入 PKCS12 系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入：

```
./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file
pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass
keypass
```

检入 PKCS12 系统证书

将 PKCS12 系统证书保存到本地计算机上的文件之后，可以通过**管理**菜单检入 PKCS12 系统证书。

关于此任务

在开始之前，您需要将 PKCS12 系统证书保存到本地计算机上的一个文件中。

要检入 PKCS12 系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 在"系统证书"页面的"检入"下，单击 **PKCS12 证书**旁边的**执行！**。
3. 输入 PKCS12 **证书名称**。
4. 输入**专用密钥密码**。 这是用于加密 PKCS12 证书的密码。
5. 输入**密钥库密码**。 这是 PKCS12 对象的密码。可能与专用密钥密码相同。
6. 输入**文件名**或单击**浏览**以选择 PKCS12 证书的文件名，然后单击**下一步**。
7. 选择**使用时进行验证**选项，然后单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 为没有自签名的证书构造信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
8. 复审 PKCS12 系统证书信息。
9. 单击**完成**。

导入 Pem 系统证书

您可以导入使用 DES 或 3DES 加密的 pem 系统证书。

关于此任务

仅支持使用 DES 或 3DES 加密的 pem 密钥。

要导入 pem 系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入：

```
./ImportSystemCert.sh -pem systempass certname file password
keystoretype keystoreprovider storepass keypass
```

导入键控系统证书

您可以导入键控系统证书。

关于此任务

要导入键控系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入：

```
./ImportSystemCert.sh -keycert systempass certname file
password keystoretype keystoreprovider storepass keypass
```

导入密钥库系统证书

您可以在 HSM 上生成密钥库系统证书。

关于此任务

要在 HSM 上生成密钥库系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入：

```
./ImportSystemCert.sh -keystore systempass certname
alias keystoretype keystoreprovider storepass keypass
```

检入密钥系统证书

将密钥系统证书保存到本地计算机上的文件之后，可以通过**管理**菜单检入密钥系统证书。

关于此任务

在开始之前，将密钥系统证书保存到本地计算机上的一个文件中。

要检入密钥系统证书：

过程

1. 请选择一项：
   - 如果使用 Sterling B2B Integrator，请在**管理菜单**中，选择**贸易伙伴 > 数字证书 > 系统**。
   - 如果使用 AS2 Edition，请在 **AS2 管理**菜单中，选择**证书**。
2. 单击**密钥证书**旁边的**执行！**。
3. 输入**证书名称**。
4. 输入**专用密钥密码**。 这是用于加密专用密钥的密码。
5. 输入**文件名**或单击**浏览**以选择密钥证书的文件名，然后单击**下一步**。
6. 选择**使用时进行验证**选项并单击**下一步**。验证选项包括：
   - 有效性 – 验证证书有效期限内的日期是否仍然有效。如果日期无效，将不使用证书。
   - 认证链 – 为没有自签名的证书构造信任链。如果无法使用有效证书构造信任链，那么将不使用证书。如果证书是自签名证书，那么此选项将仅验证证书签名。
7. 复审密钥证书信息。

8. 单击**完成**。

联机证书状态协议 (OCSP)

Sterling B2B Integrator 中的联机证书状态协议 (OCSP) 支持

联机证书状态协议 (OCSP) 是一组 ASN.1 定义的数据结构，用于请求和接收与证书撤销状态有关的信息。原则上，这些数据结构可以通过许多传输协议发送和接收。而实际上使用 HTTP。

OCSP 客户机发送问题并处理响应。OCSP 响应程序回答问题并生成响应。

OCSP 客户机功能

OCSP 客户机实施包括用于管理 OCSP 响应程序相关信息的数据结构、用于生成 OCSP 请求的功能、用于处理 OCSP 响应的功能以及用于传输 OCSP 请求和接收 OCSP 响应的功能。

OCSP 客户机实施包括：

- 数据结构，用于管理与 OCSP 响应程序有关的信息
- 用于生成 OCSP 请求的功能
- 用于处理 OCSP 响应的功能
- 用于传输 OCSP 请求和接收 OCSP 响应的功能

Sterling B2B Integrator 如何执行 OCSP 检查

当 Sterling B2B Integrator 中的 OCSP 检查作为内部系统 API 的一部分实施，供服务用于从数据库获取证书和密钥时，将确定对 Sterling B2B Integrator 中的证书执行 OCSP 检查。

关于此任务

当调用方法以从对象（将证书和密钥封装到数据库的对象）获取证书和密钥时，Sterling B2B Integrator 将执行 OCSP 检查。

以下步骤描述如何在 Sterling B2B Integrator中实施 OCSP 检查：

过程

1. 系统检查封装证书的对象以确定是否启用 OCSP 检查。这允许系统决定在没有额外数据库调用的情况下，是否尝试 OCSP 检查。
2. 如果启用 OCSP 检查，系统将从证书获取已编码的发行者名称。
3. 系统使用 SHA1 对已编码的发行者名称执行 Hash。
4. 系统尝试查找系统中配置的权限，该权限的 Hash 名称与证书的 Hash 名称相匹配。
5. 如果没有找到权限，那么将不执行检查。
6. 如果找到权限，那么系统将检查权限的 OCSP 策略。如果策略许可或要求 OCSP 检查，那么请参阅 CERT_AUTHORITY 表以了解更多信息。系统尝试查找针对权限的 OCSP 响应程序。
7. 如果没有找到权限的 OCSP 响应程序，那么将发生以下某种情况：
   - 如果权限策略设置为始终检查，那么将抛出异常且检查失败。

- 如果权限策略设置为仅在配置了响应程序时执行检查，那么将不执行检查。
- 如果找到了权限的 OCSP 响应程序，那么将尝试执行 OCSP 检查。

数据库表

已添加 CERT_AUTHORITY 和 OCSP_RESPONDER 来管理与 OCSP 相关的信息。

已添加以下两个新的数据库表来管理与 OCSP 相关的信息：

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

CERT_AUTHORITY 表保存有关认证中心的信息。

列	类型	描述
OBJECT_ID	VARCHAR (255)	这是构成记录唯一标识的 GUID。这是主键。不能为 null。
NAME	VARCHAR (255)	记录的名称。允许为 Null。
CREATE_DATE	DATETIME	记录的创建日期。
MODIFIED_DATE	DATETIME	上次修改记录的日期。
MODIFIED_BY	VARCHAR(255)	有关记录修改者的信息。
ISSUER_NAME	BLOB	从其证书获取的中心的 RDN。
HASH_ALG	VARCHAR(128)	用于计算名称和密钥散列的散列算法。仅支持 SHA1。
RDN_HASH	VARCHAR(255)	从中心证书获取的 DER 编码发行者 RDN 的 BASE64 编码 SHA1 Hash。此列已建立索引。
KEY_HASH	VARCHAR(255)	发行者证书中已编码公用密钥的 BASE64 编码 SHA1 Hash。
CERT_OID	VARCHAR(255)	CA_CERT_INFO 表内中心证书的 OBJECT_ID。每个中心在数据库中必须有一个 CA 证书。不允许为 Null。

列	类型	描述
OCSP_POLICY	VARCHAR(128)	中心的 OCSP 策略。这包含两个值，它们之间用逗号分隔。这两个值描述何时使用 OCSP 以及要检查的内容。 可能的值包括： **OCSP_When** • never - 从不使用 OCSP • resp – 仅在发出请求的过程中配置响应程序时使用 OCSP • always - 始终在发出请求时使用 OCSP。这要求配置响应程序；如果没有配置响应程序，那么会导致证书检查失败。 **OCSP_What** • none - 从不检查任何证书 • end-user - 仅检查最终用户证书 • both - 检查最终用户证书以及中间证书。当前不受支持 • 此列中不允许为 Null
CRL_POLICY	VARCHAR(128)	当前未使用。

OCSP_RESPONDER

OCSP_RESPONDER 表保存有关 OCSP 响应程序的信息。

列	类型	描述
OBJECT_ID	VARCHAR (255)	这是构成记录唯一标识的 GUID。这是主键。不能为 null。
NAME	VARCHAR (255)	记录的名称。允许为 Null。
CREATE_DATE	DATETIME	记录的创建日期。
MODIFIED_DATE	DATETIME	上次修改记录的日期。
MODIFIED_BY	VARCHAR(255)	有关记录修改者的信息。
ISSUER_NAME	BLOB	从其证书获取的中心的 RDN。
HASH_ALG	VARCHAR(128)	用于计算名称和密钥散列的散列算法。仅支持 SHA1。
RDN_HASH	VARCHAR(255)	从中心证书获取的 DER 编码发行者 RDN 的 BASE64 编码 SHA1 Hash。此列已建立索引。
KEY_HASH	VARCHAR(255)	发行者证书中已编码公用密钥的 BASE64 编码 SHA1 Hash。
CERT_OID	VARCHAR(255)	CA_CERT_INFO 表内中心证书的 OBJECT_ID。每个中心在数据库中必须有一个 CA 证书。不允许为 Null。

列	类型	描述
CACHE_TTL	VARCHAR(64)	允许 OCSP 响应在内部响应高速缓存中生存的时间（以秒计）。 如果该列为 NULL，OCSP 响应将仅高速缓存 1 秒，而这实际上意味着根本不进行高速缓存。
TRANS_PROF_OID	VARCHAR(255)	GIS 数据库中的概要文件的 OBJECT_ID。您必须创建 OCSP 响应程序的概要文件，其中包含响应程序的正确 URL。
COMM_BP	VARCHAR(255)	用于与 OCSP 响应程序通信的业务流程的名称。这必须是执行 HTTP 通信的业务流程。必须将业务流程中的服务配置为分别在发送和接收时不需要或不显示 HTTP 头。可以使用并建议使用系统随附的流程 HTTPClientSend。
COMM_WAIT	VARCHAR(24)	在推断出发生错误之前，等待与 OCSP 响应程序通信的秒数。

OCSP 配置

在配置系统以使用 OCSP 时，您可以创建无限数量的认证中心和响应程序。

关于此任务

在配置系统时，您可以创建所需数量的认证中心和响应程序。

要配置系统以使用 OCSP：

过程

1. 检查认证中心（发放要使用 OCSP 检入到 Sterling B2B Integrator 的证书）的证书以验证其是否为 CA 证书。
2. 列出系统中的 CA 证书并获取刚刚安装的证书的对象标识。
3. 如果中心的 OCSP 响应签署证书不同于中心的证书发放证书，请将中心的 OCSP 响应签署证书作为可信证书检入到 Sterling B2B Integrator。

   注：利用 5.2.4.2 和更高版本，您可以检入将响应程序证书作为 CA 而非作为可信证书进行发布的根证书。由于根据 CA 频繁更改响应程序证书，可能会导致 OCSP 失败，直至该证书替换为有效证书。最好的办法是从即时起一直检入根证书，因为根证书很少更改。但是，将继续支持这两种类型。
4. 如果检入了其他 OCSP 签署证书，那么列出系统中的 CA 证书并获取刚刚安装的证书的对象标识。
5. 转至 Sterling B2B Integrator 安装的 bin 目录。
6. 如有必要，请启动数据库。
7. 启动 bash 或 sh shell。
8. 找到文件 tmp.sh
9. 使用类 com.sterlingcommerce.security.ocsp.SCICertAuthority 中的实用程序创建中心。

10. 使用类 com.sterlingcommerce.security.ocsp.SCIOCSPResponder 中的实用程序创建 OCSP 响应程序
11. 更新中心的证书或个别证书以启用 OCSP。实用程序 com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo 将为中心配置所有可信证书和系统证书。实用程序 com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo 将配置 1 个系统证书。实用程序 com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo 将配置 1 个可信证书。

OCSP 配置脚本

以下脚本已包含在 OCSP 最新修订程序中，用于运行 OCSP 配置实用程序。每个脚本都有 UNIX/Linux 和 Windows 版本。脚本与其调用的实用程序采用相同的命令行自变量。脚本位于产品安装的 bin 目录。实际上，有关命令行自变量的信息刚刚在描述脚本的该部分中重复说明。

ManageCertAuthority.sh and ManageCertAuthority.cmd

自变量	描述
-a、-r 和 -d	要执行的操作： -a 添加 -l 列出 -d 删除 –l 选项不使用任何额外自变量。 –d 选项使用一个自变量：要删除的记录的对象标识
Name	权限的名称。对 -a 为必需。
Modified_by	修改或创建身份的用户。对–a 为必需。
Hash_alg	权限的 Hash 算法。仅支持值"SHA1"。对–a 为必需。
Certificate_id	与权限关联的 CA 证书的对象标识。对–a 为必需。

OCSP_policy	权限的 OCSP 策略字符串。这是以逗号分隔的字符串，如 CERT_AUTHORITY 表中的部分所描述。对–a 为必需。 对于字符串的第一个元素，许可以下各项： • never - 从不使用 OCSP • resp - 仅在配置响应程序的情况下发出请求时使用 OCSP • always - 始终在发出请求时使用 OCSP。这要求配置响应程序，如果没有配置响应程序，将导致证书检查失败。 对于字符串的第二个元素，许可以下各项： **OCSP 内容** • none - 从不检查任何证书 • end-user - 仅检查最终用户证书 • both - 检查最终用户证书以及中间证书。目前不受支持。 示例： • never,none • always,end-user
Crl_policy	权限的 CRL 策略字符串。对–a 为必需。此自变量需要值，但当前未使用。可以接受 "None"。
Object_ID	创建此记录时要使用的对象标识。对 -a 为可选。

ManageOCSPResponder.sh 和 ManageOCSPResponder.cmd

自变量	描述
-l	获取当前配置的 OCSP 响应程序的列表。 此选项不使用任何额外自变量。
-d	删除已配置的 OCSP 响应程序以及为响应程序配置数据提供的对象标识。 此选项将 object_id 作为额外自变量。
-u2	使用权限证书公用密钥以及权限证书的主题 DN 的正确信息更新数据库中的现有记录。 需要对认证中心和 OCSP 响应程序的所有现有记录运行此自变量，或者需要删除并重新创建记录以将正确信息存入数据库。 此选项将 object_id 作为额外自变量。

-a	添加新 OCSP 响应程序的配置数据，以用于检查提供权限发出的证书的状态。 附加自变量有 name、modified_by、hash_alg、authority_cert_oid、response_signing_cert_oid、resp_signing_cert _in_ca_store、cache_ttl、trans_prof_oid、 comm_bp、comm_wait、send_nonce、require_nonce 和 object_id。
name	（对 -a 为必需）权限的名称。
modified_by	（对 -a 为必需）修改或创建身份的用户。
hash_alg	（对 -a 为必需）权限的 Hash 算法。仅支持值"SHA1"。
authority_cert_oid	（对 -a 为必需）与权限关联的 CA 证书的对象标识。
response_signing_cert_oid	（对 -a 为必需）OCSP 服务提供者用来签署响应（提供证书状态）的证书的对象标识。此证书必须添加到 CA 数字证书库或可信数字证书库。这是证书出现在库中时的系统证书标识。
resp_signing_cert_in_ca_store	（对 -a 为必需）用于指示是否在 Sterling B2B Integrator 的 CA 数字证书库中找到了 response_signing_cert_oid 自变量的先前值的标志。
cache_ttl	（对 -a 为必需）OCSP 响应在内部高速缓存中的生存时间，以秒计。
trans_prof_oid	（对 -a 为必需）为与 OCSP 响应程序通信而配置的传输的对象标识。
comm_bp	（对 -a 为必需）用于与 OCSP 响应程序进行通信的业务流程的名称。这必须是执行 HTTP 通信的业务流程。必须配置业务流程中的服务，以在发送和接收时分别不需要或不显示 HTTP 头。可以使用并建议使用系统随附的流程 HTTPClientSend。
comm_wait	（对 -a 为必需）在表明发生错误之前，等待与响应程序通信的秒数。
send_nonce	（对 -a 为必需）指示是否将 NONCE 值发送到 OCSP 服务。NONCE 值用于阻止某些 OCSP 提供者发起重放攻击。
require_nonce	（对 -a 为必需）指示服务器是否应要求 OCSP 服务在响应中提供 NONCE 值。
object_id	（对 -a 为可选）创建此记录时要使用的对象标识。

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

此实用程序将在数据库中为单一系统证书设置 OCSP 信息

自变量	描述
-o 和 -n	如何解释第二个变量： -o object_ID -n name
Object_ID/Name	通过自变量 1 确定的权限的对象标识和名称。

SetSystemCertOCSPInfo.sh 和 SetTrustedCertOCSPInfo.cmd

此实用程序将在数据库中为单一系统证书设置 OCSP 信息

自变量	描述
-o 和 -n	如何解释第二个变量： -o object_ID -n name
Object_ID/Name	通过自变量 1 确定的权限的对象标识和名称。

运行 OCSP 脚本

以下示例显示了如何运行 OCSP 配置脚本。这些脚本假定您已经检入了中心的 CA 证书，启动了数据库，位于 Sterling B2B Integrator 安装的 bin 目录，并且在 bin 目录中找到了 tmp.sh 文件。

关于此任务

从中心获取 CA 证书的对象标识后，在 Sterling B2B Integrator 的**管理菜单**中，选择**贸易伙伴 > 数字证书 CA**。选择证书。显示包含证书信息的"证书摘要"对话框，包括对象标识。

完成以下步骤以运行 OCSP 脚本。要获取 OCSP 脚本命令的完整列表，请参阅第 77 页的『OCSP 配置脚本』。

过程

1. 运行类似以下命令以在系统中创建中心：

   ```
   ./ManageCertAuthority.sh -a VPCA admin SHA1 "sedna:a1807c:11dc6d53ba4:-7b4b"
    "always,end-user" "none"
   ```

2. 创建中心和创建用于与 OCSP 响应程序通信的概要文件后，运行类似以下命令以在系统中创建 OCSP 响应程序：

   ```
   ./ManageOCSPResponder.sh -a CertAuth_TestOCSP admin SHA1
   "kenny:node1:13727b3f8e4:29762" "kenny:node1:13727275fd9:40698" false (use
   true if the checked in signing certificate
   is the same from the responding certificate, that is, checked in to the
   certificate authority in step 3) "2400" "14ffd4a0:1371823040d:-77c8"
   HTTPClientSend 3600 false false
   ```

3. 运行类似以下命令以列出系统中的所有中心：

```
./ManageCertAuthority.sh -l
```

每个中心的返回输出显示：

```
CERT_AUTHORITY:
OBJECT_ID: sedna:1ded0fd:11dc9d22929:-7fbd
NAME: VPCA
CREATE_DATE: 2008-11-23
MODIFIED_DATE: 2008-11-23
MODIFIED_BY: null
ISSUER_NAME: Country=US, StateOrProvince=Dublin, OrganizationUnit=GIS
 Development, Organization=Sterling,
CommonName=Test CA
HASH_ALG: SHA1
RDN_HASH: 24E63F8AE9F51497529EA0CC34467A4680737A9F
ENCODED_RDN_HASH: JOY/iun1FJdSnqDMNEZ6RoBzep8=
KEY_HASH: C96F2FF442EBFA07672DCEC49B729D4D24898313
ENCODED_KEY_HASH: yW8v9ELr+gdnLc7Em3KdTSSJgxM=
CERT_OID: sedna:a1807c:11dc6d53ba4:-7b4b
OCSP_WHEN_POLICY: always
OCSP_WHAT_POLICY: end-user
CRL_POLICY: null
```

4. 使用类似以下命令以针对中心发出的所有可信和系统证书启用 OCSP：

```
./SetAuthorityCertsOCSPInfo.sh -o sedna:1ded0fd:11dc9d22929:-7fbd yes
```

OCSP 检查逻辑

以下步骤描述了 OCSP 检入 Sterling B2B Integrator 的逻辑。如果证书状态为正常，那么表明 OCSP 检查成功。否则失败。

过程

1. 如果发现了其生存时间尚未到期的现有响应，那么该响应将用作 OCSP 响应。
2. 如果高速缓存中没有找到现有响应，或者高速缓存中响应的生存时间已到期，那么将创建 OCSP 请求。
3. 如果系统创建 OCSP 请求，那么将启动为 OCSP 响应程序配置的业务流程以发送请求和获取响应。如果响应程序配置为发送现时标志值，那么请求将包含现时标志值。
4. 如果业务流程成功完成，那么系统会尝试将其主文档解析为 OCSP 响应。用于发送 OCSP 请求和接收 OCSP 响应的业务流程从响应中取出 HTTP 头。
5. 如果可以将主文档解析为 OCSP 响应，那么系统将检查响应的状态。
6. 如果响应状态指示请求生成了有效响应，那么系统将尝试使用为 OCSP 响应程序配置的证书来验证 OCSP 响应上的签名。
7. 如果签名通过验证并且已将响应程序配置为需要现时标志，那么系统将尝试获取并检查响应的现时标志。
8. 如果所有其他验证均已通过，那么系统将查找为其构建和发送请求的证书的证书状态信息。
9. 如果找到状态信息，那么系统将针对证书的现有 OCSP 响应更新内部高速缓存。

联邦信息处理标准 (FIPS)

联邦信息处理标准 (FIPS) 140-2

要符合 FIPS 200 的安全需求，应用程序必须使用经"密码模块验证程序"认证且符合 FIPS 140-1 或 140-2 的密码模块。

使用应用程序验证的密码术应满足以下最低需求：

- 必须由经验证的密码模块执行所有密码操作，包括密钥生成。
- 仅许可经核准的安全功能。
- 仅许可经核准的密钥确定方法。

针对 Sterling B2B Integrator 的 FIPS 140-2

Certicom Government Service Edition (GSE) 是随 Sterling B2B Integrator 一起分发的经 FIPS 140-2 级别 1 认证的密码模块。GSE 是使用 Java 编写的低级密码工具箱，用于实施各种安全功能，包括未经核准的安全功能。

当处于 FIPS 方式时，执行以下任务：

- 启用 GSE FIPS 状态机并调用开机自检。
- 将核心系统的密码函数调用集中到 GSE。

安装期间启用 FIPS

在完成新的安装期间，如果询问是否要以 FIPS 方式运行，请选择 TRUE。

手动启用 FIPS 方式

在安装 Sterling B2B Integrator 后，可以手动启用 FIPS 方式。在开始之前，验证您是否具有在 FIPS 方式下运行的许可证，然后再启用 FIPS 方式。将在启动时检查您的许可证，如果 FIPS 方式已启用但未经许可，那么该产品将不启动。

关于此任务

要手动启用 FIPS 方式：

过程

1. 浏览到 /*install_dir*/properties/。
2. 找到 security.properties 文件。
3. 在文本编辑器中打开 security.properties 文件。 如果更改 security.properties 文件，请确保对 security.properties.in 文件执行相同的更改。这样将防止您的定制设置遭到覆盖。应使用安全性属性文件来定制 FIPS，而不是直接编辑属性文件。
4. 指定以下配置：FIPSMode=true
5. 保存并关闭 security.properties 文件。
6. 重新启动 Sterling B2B Integrator。为使系统能够识别更改，此步骤是必需的。

禁用 FIPS 方式

您可以手动禁用 FIPS 方式。

关于此任务

要手动禁用 FIPS 方式：

过程

1. 浏览到 */install_dir*/properties/。
2. 找到 security.properties 文件。
3. 在文本编辑器中打开 security.properties 文件。
4. 指定以下配置：FIPSMode=false
5. 保存并关闭 security.properties 文件。
6. 重新启动 Sterling B2B Integrator。 为使系统能够识别更改，此步骤是必需的。

代理服务器

代理服务器

代理服务器可提高系统的安全性。

配置 HTTP 代理服务器

您可以通过**管理**菜单配置 HTTP 代理服务器。

关于此任务

要配置 HTTP 代理服务器：

过程

1. 在**管理菜单**中，选择**操作** > **代理服务器**。
2. 单击**添加**。
3. 输入代理服务器的**名称**。
4. 选择 **HTTP** 作为**类型**。
5. 输入**主机名**。 IPV6 地址应使用方括号括起。
6. 输入**端口**号。
7. 输入**重试计数**。
8. 单击**下一步**。
9. 如果想要对用户进行基本认证：
   - 选择**是**并单击**下一步**。
   - 如果选择"否"（缺省值），请单击**下一步**并跳至步骤 13。
10. 输入**认证用户标识**。
11. 输入**认证密码**。
12. 单击**下一步**。
13. 复审代理服务器设置。
14. 单击**完成**。

配置 SSP 代理服务器

您可以通过**管理**菜单配置 SSP 代理服务器。

关于此任务

要配置 SSP 代理服务器：

过程

1. 在**管理菜单**中，选择**操作** > **代理服务器**。
2. 单击**添加**。
3. 输入代理服务器的**名称**。
4. 选择 **SSP** 作为**类型**。
5. 输入**主机名**。 IPV6 地址应使用方括号括起。
6. 输入**端口**号。
7. 输入**重试计数**。
8. 单击**下一步**。
9. 对于"用户需要基本认证"，请选择"是"或"否"。
10. 对于"需要 SSL"，请选择"是"或"否"。
11. 单击**下一步**。
12. 如果为此用户选择了基本授权，那么必须输入**认证用户标识**和**认证密码**并单击**下一步**。 如果不需要此授权，那么将不显示此页面。
13. 如果对"需要 SSL"选择"是"，那么必须选择**密码强度**、**CA 证书**以及**密钥证书**并单击**下一步**。 如果不需要 SSL，那么将不显示此页面。
14. 单击**下一步**。
15. 复审代理服务器设置。
16. 单击**完成**。

针对 SSL 配置代理服务器

您可以通过创建或导入 SSL 证书并在相应的适配器配置中将**使用 SSL** 字段设置为**必须**，来将 SSL 用于 SSP 代理服务器配置。

关于此任务

如果决定要将 SSL 用于 SSP 代理服务器配置，那么必须：

过程

1. 在 Sterling B2B Integrator 中创建 SSL 证书或者从认证中心导入证书。
2. 在相应的适配器配置中，将**使用 SSL** 字段设置为**必须**。

编辑代理服务器

您可以通过**管理**菜单编辑代理服务器配置。

关于此任务

要编辑代理服务器配置：

过程

1. 在**管理菜单**中，选择**操作** > **代理服务器**。
2. 针对要编辑的代理服务器，单击**编辑**。
3. 根据需要更新字段。
4. 单击**下一步**。
5. 复审代理服务器设置。
6. 单击**完成**。

删除代理服务器

关于此任务

删除代理服务器配置可能会导致 Sterling B2B Integrator 的某些功能出错。您可能需要重新配置特定适配器和服务，以使其在无特定代理服务器配置的情况下正常工作。

要编辑代理服务器配置：

过程

1. 在**管理菜单**中，选择**操作** > **代理服务器**。
2. 针对要编辑的代理服务器，单击**删除**。
3. 复审代理服务器设置。
4. 单击**删除**。

SSL

关于在 Sterling B2B Integrator 中实施 SSL

安全套接字层 (SSL) 在因特网上提供安全通信。同时使用对称和非对称密码术。

SSL 安全协议在 Sterling B2B Integrator 中提供服务器认证和客户机认证：

- 客户机连接到服务器时执行服务器认证。初始握手后，服务器将其数字证书发送到客户机。客户机验证服务器证书或证书链。
- 服务器在握手期间向客户机发送证书请求时执行客户机认证。如果客户机证书或链经过验证，并且证书验证消息已经过验证，那么握手将继续进行。
- 对照从逆向域名服务器 (DNS) 查找获取的服务器标准域名，检查证书中的公共名称，执行可选的额外认证。

信任类型

Sterling B2B Integrator 中支持针对 SSL 证书的两种类型的信任：

- CA 信任 - 层次结构信任，基于用来发出其他证书的根证书。这是标准的 SSL 证书信任模型。
- 直接信任 - 自签名证书的直接信任，假定通过安全频带外机制分发。直接信任和自签名证书不属于 SSL 标准，但经常在某些贸易社区中使用。

SSL 证书

要使用 SSL 进行通信，请配置涉及到的系统以支持服务器认证或客户机/服务器认证。要对服务器执行认证，您需要链中的根认证中心 (CA) 证书和中间证书集，或自签名证书副本（如果服务器使用的是自签名证书）。

为支持客户机/服务器认证，您需要 CA 证书或自签名证书以及系统证书。

您可以通过向可信 CA 提供证书签名请求 (CSR) 来从该 CA 获取 SSL 证书。该 SSL 证书将公用密钥与 SSL 服务器或客户机绑定在一起。

如果打算使用客户机/服务器认证，请配置系统证书。您可以通过以下方法创建系统证书：

- 检入现有的密钥证书文件或 PKCS12 文件
- 生成自签名系统证书
- 使用 Key Management Utility (iKeyman) 生成 CSR 并从 CA 获取证书。有关 iKeyman 的信息，请参阅第 58 页的『IBM Key Management Utility (iKeyman)』。

密码套件

在使用 Sterling B2B Integrator 之前，您应查看可用的预定义密码列表，并根据公司的安全要求进行定制。

可以在以下位置找到 IBM SDK Java Technology Edition V7 密码套件：http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html。对于 Sterling B2B Integrator 中其他支持的 JDK，请参阅 JDK 供应商文档，以获取受支持的密码套件列表。

在 `security.properties` 或 `customer_overrides.properties` 中配置密码强度。可用密码套件的级别包括：

- AllCipherSuite（UI 选项是**全部**）- 包含"弱"和"强"中列出的所有项。
- WeakCipherSuite（UI 选项是**弱**）- 添加要用于 Sterling B2B Integrator 的受支持的弱密码套件。
- StrongCipherSuite（UI 选项是**强**）- 添加要用于 Sterling B2B Integrator 的受支持的强密码套件。
- CipherSuiteDefault（在 V5.2.6 和更高版本中可用）- 缺省情况下，包含针对 IBM JDK7 的受支持密码的子集。如果 WeakCipherSuite 和 StrongCipherSuite 为空，将使用此项。

SSL 客户机适配器

FTP 客户机适配器、HTTP 客户机适配器和 Sterling Connect:Direct® FTP+ 请求者适配器（包含 Secure+ 选项）支持 SSL。

以下客户机适配器支持 SSL：

- FTP 客户机适配器
- HTTP 客户机适配器

- Sterling Connect:Direct FTP+ 请求者适配器（包含 Secure+ 选项）

可在贸易伙伴概要文件中或针对适配器设置 SSL 的参数。对于 FTP 客户机适配器，在 FTP 客户机开始会话服务中设置这些参数。对于 HTTP 客户机适配器，在 HTTP 客户机开始会话服务中设置这些参数。在开始会话服务中设置的参数将覆盖贸易伙伴概要文件中的设置。

下表中的参数通过客户机透视图来控制 SSL。请参阅正在配置的特定适配器或服务的文档。

参数	描述
SSL	确定 SSL 套接字协商。
CACertificateId (trusted_root)	可信 CA 公用证书的列表。在流程数据中，此参数显示为对象标识。
CipherStrength	要应用于通过套接字连接流动的数据的加密级别。
SystemCertificateId	从可用系统证书列表中选择。此证书向服务器确认客户机的身份。

SSL 服务器适配器

FTP Server 适配器、HTTP Server 适配器、Sterling Connect:Direct Server 适配器（包含 Secure+ 选项）和 SMTP 发送适配器支持 SSL。

以下服务器适配器支持 SSL：

- FTP Server 适配器
- HTTP Server 适配器
- Sterling Connect:Direct Server 适配器（包含 Secure+ 选项）
- SMTP 发送适配器

下表中的参数通过服务器透视图来控制 SSL。请参阅正在配置的特定适配器或服务的文档。

参数	描述
SSL	SSL 是否活动。
Key Certificate Passphrase	保护服务器密钥证书的密码。此口令供系统内部使用，用于初始化 SSL 库。
CipherStrength	用于加密数据的算法强度。
Key Certificate（系统存储）	服务器认证的专用密钥和证书。
CA 证书	用于验证客户机证书的证书（如果有）。

检入证书

为支持客户机/服务器认证，您需要 CA 证书或自签名证书以及系统证书。

关于此任务

您可以将 CA 证书或自签名证书检入到 CA 证书库中，方法是从**管理菜单**中依次选择**贸易伙伴** > **数字证书** > **CA** > **检入新证书**。

创建自签名证书以进行测试

为进行测试，您可以使用自签名证书。自签名证书可在 Sterling B2B Integrator 中生成并进行管理。

关于此任务

要创建自签名证书：

过程

1. 选择**贸易伙伴** > **数字证书** > **系统证书** > **创建自签名证书**。
2. 创建后，查找该证书并将其检出到文件。
3. 通过选择**贸易伙伴** > **数字证书** > **CA** > **检入新证书**可将该证书作为 CA 证书检入回 Sterling B2B Integrator。

SSL/TLS 重新协商（V5.2.6 或更高版本）

Sterling B2B Integrator 使用 IBM JSSE 参数控制对 SSL/TLS重新协商的限制程度。可在 `security.properties` 文件中更新以下参数。

参数名称	定义	有效值
com.ibm.jsse2.extended.renegotiation.indicator	使用该属性强制所有协商（而不仅是重新协商）要求 RFC 5746。只有在所有必需的通信伙伴都已实施 RFC 5746 之后，该协商实用。缺省设置为 OPTIONAL。	有效值为： • BOTH - 仅当同伴表示支持 RFC 5746 重新协商时，才会让 IBM JSSE2 服务器或 IBM JSSE2 客户机进行连接。注：将该属性设置为 BOTH 将导致尚未更新为支持 RFC 5746 的客户机或服务器出现互操作性问题。 • CLIENT - 仅当服务器表示支持 RFC 5746 重新协商时，才会让 IBM JSSE2 客户机进行连接。注：将该属性设置为 CLIENT 将导致尚未更新为支持 RFC 5746 的服务器出现互操作性问题。 • OPTIONAL - 该设置是缺省设置。使用该选项表示，在初始握手期间 IBM JSSE2 服务器或 IBM JSSE2 客户机不需要重新协商指示符。 • SERVER - 仅当客户机表示支持 RFC 5746 重新协商时，才会让 IBM JSSE2 服务器进行连接。注：将该属性设置为 SERVER 将导致尚未更新为支持 RFC 5746 的客户机出现互操作性问题。

参数名称	定义	有效值
com.ibm.jsse2.renegotiate	使用该属性更改 IBM JSSE2 的重新协商能力。缺省值为 NONE。	有效值为： • ABBREVIATED - 该设置将替代设置，并且在重新协商期间会话连续性获得以证明时允许不安全的简短握手。允许 RFC 5746 重新协商。 • ALL - 该设置将替代设置，并且在重新协商期间允许不完全的握手和不安全的简短握手。允许 RFC 5746 重新协商。 • DISABLED - 该设置将取代设置， 并且禁用所有不安全的重新协商和 RFC 5746 重新协商。 • NONE - 该设置是缺省设置。不允许不安全的握手重新协商。只允许 RFC 5746 重新协商。
com.ibm.jsse2. renegotiation .peer.cert.check	使用该属性更改 IBM JSSE2 的重新协商能力，以要求 RFC 5746 中指定的对等支持。只有在所有必需的通信伙伴都已实施 RFC 5746 之后，该要求才实用。缺省值为 OFF。	有效值为： • OFF - 该设置是缺省设置。将阻止 IBM JSSE2 客户机或 IBM JSSE2 服务器比对同级对象中的证书执行身份检查。结果是在重新协商期间允许更改同级对象证书。 • ON - 该设置将使 IBM JSSE2 客户机或 IBM JSSE2 服务器比对同级对象中的证书执行比较。原因是确保证书在重新协商期间不会更改。该比较适用于安全重新协商和非安全重新协商。

对 SSL 进行故障诊断

如果您收到错误消息，可以对 SSL 进行故障诊断。

损坏或无用证书错误消息

如果收到以下错误消息：

```
FATAL Alert:BAD_CERTIFICATE - A corrupt or unusable certificate was received.
```

Perimeter 日志的信息如下：

```
ERROR <HTTPClientAdapter_HTTPClientAdapter_node1-Thread-19>
HTTPClientAdapter_HTTPClientAdapter_node1-Thread-172105824724com.
sterlingcommerce.perimeter.api.conduit.SSLByteDataConduit@4c2b95c6:
Doing reset3 c
```

```
om.certicom.net.ssl.SSLKeyException: FATAL Alert:BAD_CERTIFICATE -
A corrupt or unusable certificate was received.
 at com.certicom.tls.d.b.a(Unknown Source)
 at com.certicom.tls.d.b.do(Unknown Source)
```

在检入证书时，Sterling B2B Integrator 将在命名屏幕上显示状态值"无效签名"。如果使用 SSL 执行出站 HTTP POST 的业务流程在 HTTP 方法服务上失败并出现错误，那么将显示以下消息：

```
HTTP Status Code: -1
HTTP Reason Phrase: Internal Error: Connection was closed from the
perimeter side with error: CloseCode.CONNECTION_RESET
```

获取贸易伙伴的相应 CA 证书。如果贸易伙伴使用的是自签名证书，那么该证书本身可用作 CA 证书。

CA 和直接信任

当 Sterling B2B Integrator 是客户机时，如果服务器具有 CA 发出的证书，且该证书具有主题相对专有名称 (RDN) 中的服务器的 DNS 名称，那么您可以将根 CA 证书放在 CA 库中并信任该证书。如果 SSL 仍不工作，请尝试直接信任。将服务器证书放在 CA 库中并信任该证书。

如果服务器上用的是自签名证书，请将该证书放在 CA 库中并信任该证书。在此情况下同样是执行直接信任。

不通过证书使用 SSL

如果没有所需的证书或系统证书，那么不能使用启用 SSL 的适配器。

使用基于 CBC 的密码套件时，SSL 不工作

如果选择了 CBC 方式密码套件，并且 SSL 不工作，那么您必须关闭 CBC 保护。

对于 V5.2.5 和更低版本，请执行以下步骤：

1. 打开 tmp.sh 文件进行编辑。
2. 查找正在配置的操作系统的服务器标志并添加以下值：

   ```
   -DDisableSSLEmptyRecords=true
   ```
3. 保存并关闭该文件。

对于 V5.2.6 和更高版本，请执行以下步骤：

1. 在 *<B2Bi Install>*/bin 目录中，查找 InstallNoappsWindowsService.cmd.in 和 InstallContainerWindowsService.cmd.in（针对 Windows）；查找 tmp.sh_platform_ifcresources_ext.in（针对所有其他操作系统）。
2. 编辑文件以将下列属性的所有实例更改为 false：

   ```
   jsse.enableCBCProtection=true
   ```
3. 运行 setupfiles 脚本。

针对 GPM 的 HTTPS 配置

对于 Sterling B2B Integrator 中的大部分 Web 应用程序，已经支持在基本 HTTP 端口 + 1 上通过 SSL 执行安全 HTTP 访问。

此 SSL 增强功能：

- 针对图形化流程建模器 (GPM) 启用 HTTPS（HTTP w/ SSL 加密）
- 支持禁用基本 HTTP 端口上的 Web 应用程序并将其重定向到另一端口（使用 HTTPS）
- 通过在安全 HTTP Server 适配器实例上部署 Web 应用程序实现对 Web 应用程序的安全访问支持
- 降低安全风险

如果使用此功能，您将需要配置图形化流程建模器 (GPM) 以使用 HTTPS（而非 HTTP）与仪表板 Web 应用程序进行通信。与在基本端口上进行访问相比，访问通过安全 HTTP Server 适配器部署的 Web 应用程序可能较慢。

注：在 V5.2.6 和更高版本中，缺省安全协议为 TLS 1.2（针对基本 HTTP 端口 + 1）。如果需要，可以通过更新 properties_platform_ifcresources_ext 中的 **jsseProtocol** 参数来将此更改为 TLS 1.1 或 TLS 1.0。有效值包括以下参数：

- **TLS1-TLS1.1** - 针对 TLS1.0 和 TLS1.1
- **TLS1.1-TLS1.2** - 针对 TLS1.1 和 TLS1.2
- **TLS1** - 仅针对 TLS1.0
- **TLS1.1** - 仅针对 TLS1.1
- **TLS1.2** - 仅针对 TLS1.2

新的 SSL 参数

已添加了若干新参数以实现增强的 SSL 功能。您需要配置这些参数来促进图形化流程建模器 (GPM) 和服务器间的 SSL 通信。必须在其各自属性文件中定义这些新参数。

针对您环境的所有定制属性应在 customer_overrides.properties 文件中设置，这样便不会在升级或补丁安装期间被覆盖。sandbox.cfg 文件中定义的属性不得在 customer_overrides.properties 中进行定义，因为 customer_overrides.properties 中将忽略这些属性。这些属性是唯一没有在 customer_overrides.properties 中定义的属性。

下表描述了新的 SSL 参数，并提供了可在其中找到这些参数的属性文件的名称。

参数名称	定义	属性文件
WEBAPP_LIST_PORT	确定 GPM 客户机与服务器进行通信应使用的端口。缺省值为安装期间的基本端口。 如果仪表板和 GPM Web 应用程序已部署到安全 HTTP Server 适配器实例，那么应修改此参数以与该安全 HTTP Server 适配器实例的端口相匹配。 如果是将基本 SSL 端口（基本 HTTP 端口 +1）用于 GPM 和仪表板的安全部署，那么应修改此参数以与基本 SSL 端口（sandbox.cfg 中的 SSL_PORT）相匹配。	sandbox.cfg 文件

参数名称	定义	属性文件
WEBAPP_PROTOCOL	确定与仪表板 Web 应用程序进行通信所使用的协议 (http/https)。	sandbox.cfg 文件
SKIP_BASEPORT_ DEPLOYMENT_WARS	指示在基本端口上部署 war 期间应跳过的 Web 应用程序。war 列表以逗号分隔，区分大小写，且不包含 .war 后缀。 缺省值是不跳过任何 war。在安全 HTTP Server 适配器上成功部署仪表板和 GPM Web 应用程序后，此参数可以设置为 =admin,dashboard,gbm，以除去在基本端口上访问这些 Web 应用程序。Web 应用程序的完整列表包括： • myaft • portlets 值 ALL 可用作通配符，用于指示应跳过基本 HTTP 端口上部署的所有 war。如果已针对外部访问阻塞基本端口，那么这可能是不必要的。值 ALL 不得与其他任何值一起使用。	customer_overrides.properties
HTTPS_REDIRECT_WARS	指示将从基本 HTTP 端口自动重定向到安全 HTTP Server 适配器或基本 SSL 端口的 war。 值 ALL 可以用于将基本 HTTP 端口上跳过的所有 war 重定向到 HTTPS_LIST_PORT（安全 HTTP Server 适配器或基本 SSL 端口）。 值 ALL 不得与其他任何值一起使用。	customer_overrides.properties
HTTPS_LIST_PORT	指示针对基本 HTTP 端口所发出请求的重定向目标端口。应设置为安全 HTTP Server 适配器或基本 SSL 端口的值。	customer_overrides.properties
HTTPS_CLIENT_CERTS	其公用密钥需要添加到缺省信任库的系统证书的列表（以逗号分隔）。当从独立于应用程序服务器 (ASI) 的服务器发出 HTTPS 调用并返回到服务器本身时，SSL 握手期间将使用这些证书进行客户机端验证。 此参数需要具有 **SubjectAltName** 的服务器证书密钥。如果使用现有密钥而不包含此参数，那么此功能将失败并带有非常模糊的消息。 **注：**针对 baseport+1 (sslCert) 上的 HTTPS 配置的证书自动添加到信任库，并无需添加到此列表。	customer_overrides.properties

在配置此功能时，如果仅定义 SKIP_BASEPORT_DEPLOYMENT_WARS，而不定义 HTTPS_REDIRECT_WARS 和 HTTPS_LIST_PORT，那么不能在基本端口上访问 Web 应用程序，并且不会将用户自动重定向到 HTTPS 端口。如果用户出于安全原因而希望不自动重定向，那么这是有效的方案。在安全 HTTP Server 适配器或基本 SSL 端口上访问 Web 应用程序时，这些 Web 应用程序将仍可用。

启用自动重定向到 HTTPS

您可以启用自动重定向到 HTTPS。

关于此任务

已添加了允许自动重定向到 HTTPS 的支持，该 HTTPS 是针对部署在安全端口 (Http Server 适配器或基本 SSL 端口）上并跳过基本端口的 Web 应用程序配置的。这是可选配置，但强烈建议配置。

注：针对您环境的所有定制属性应在 customer_overrides.properties 文件中设置，这样便不会在升级或补丁安装期间被覆盖。

要启用自动重定向到 HTTPS：

过程

1. 浏览至 /<install_dir>/install/properties。
2. 打开 customer_overrides.properties 文件并设置以下参数值，如下所示：

   ```
   HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
   HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_port>
   ```

   配置这些参数可自动将用户重定向到 Web 应用程序的 HTTPS 实例。

   注：customer_overrides.properties 文件不属于缺省系统代码。必须在初始系统安装后创建该文件，然后填充该文件以与环境匹配。
3. 保存并关闭该文件。

示例实施

customer_overrides.properties 文件中的示例实施：

```
 ## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_port>
```

注：如果使用安全 HTTP Server 适配器实例，那么配置将要求所有指定为 HTTPS_REDIRECT_WARS 的 war 都必须部署在同一 HTTP Server 适配器实例上。

HTTPS_CLIENT_CERTS

如果使用了安全 HTTP Server 适配器实例，那么用于配置安全 HTTP Server 适配器实例的 SSL 证书必须添加到可信证书列表。

这是必需的，因为某些仪表板屏幕使 https 调用返回到 ASI 服务器。为使这些调用成功完成 SSL 握手，必须在 ASI 服务器上的信任库中配置证书。可通过在 HTTPS_CLIENT_CERTS 列表中指定证书名称来执行此操作。

这些系统证书必须具有在创建系统证书时指定为备用名称的 DNS 名称和 IP 地址。JDK 提供的缺省 SSL 主机名验证要求 SSL 服务器提供的证书名称与 http url 中使用的主机名相匹配，或者与证书中"SubjectAltName"属性中的某个字符串相匹配。仪表板上的某些屏幕在缺少"SubjectAltName"配置时无法工作。

备用名称是通过"系统证书"创建向导（**贸易伙伴** > **数字证书** > **系统**）的"以逗号分隔的 IP 地址列表"字段和"以逗号分隔的 DNS 名称列表"字段配置的。

针对 GPM 的 HTTPS 支持

Java Web Start (JavaWS) 用于通过 HTTP 启动图形化流程建模器 (GPM)。与浏览器类似，它支持 HTTPS 以及证书动态导入。

在 SSL 握手期间，服务器提供证书，JavaWS 处理信任验证。如果 JavaWS 无法验证证书，将提示用户接受或拒绝证书。SSL 证书无法由 JavaWS 自动验证，必须由用户进行验证。

为 Java Web Start 导入证书

如果要避免在 Java Web Start (JavaWS) 操作期间提示不可信证书，可以在启动图形化流程建模器 (GPM) 之前将证书导入本地机器存储。

关于此任务

这样可以在用户本地机器不信任与安全 HTTP Server 适配器或基本 SSL 端口关联的 SSL 证书时减少用户混乱。

要将可信根证书导入 JavaWS：

过程

1. 将可信根证书保存到本地计算机上的文件。
2. 打开本地计算机上的 **Java 控制面板**（javaws.exe，位于 `jre\bin` 下）。
3. 打开**安全性**选项卡并单击**证书**。
4. 单击**导入**以浏览到可信根证书并将其选中。
5. 单击**打开**以导入新的可信根证书。 检入可信根证书后，JavaWS 将使用该证书在 SSL 握手期间执行信任验证。

使用基本 SSL 端口从 HTTP 切换到 HTTPS

您可以使用基本 SSL 端口从 HTTP 切换到 HTTPS。

关于此任务

要使用基本 SSL 端口从 HTTP 切换到 HTTPS：

过程

1. 浏览到 `/install_dir/install/properties`。
2. 打开 sandbox.cfg 文件。
3. 修改以下参数：

```
WEBAPP_PROTOCOL=https
WEBAPP_LIST_PORT=<base_port + 1>
```

这些参数供图形化流程建模器 (GPM) 用于与服务器通信。

4. （可选，建议）如果要关闭在基本端口上访问仪表板和 GPM Web 应用程序，并配置自动重定向到 HTTPS 端口，请在 customer_overrides.properties 文件中指定以下参数：

```
SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<base_port + 1>
```

例如：

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<base_port + 1>
```

5. 保存并关闭该文件。
6. 浏览到 /install_dir/install/bin。
7. 停止 Sterling B2B Integrator。
8. 应用配置更改。输入 ./setupfiles.sh。
9. 部署新配置。输入 ./deployer.sh。
10. 启动 Sterling B2B Integrator。
11. （可选）如果关闭了在基本端口上访问仪表板和 GPM Web 应用程序（步骤 4），请验证所作更改。例如，可以验证：
    - 不能在 http://host:baseport/dashboard 上访问仪表板 Web 应用程序或自动重定向到 https://host:<base_port + 1>/dashboard。
    - 不能在 http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp 上访问 GPM Web 应用程序或自动重定向到 https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp。

使用安全 HTTP Server 适配器从 HTTP 切换到 HTTPS 方式

您可以使用安全 HTTP Server 适配器从 HTTP 切换到 HTTPS 方式。

关于此任务

要从 HTTP 切换到 HTTPS 方式：

过程

1. 在启用 SSL 的情况下创建新的 HTTP Server 适配器实例。必须按照指定配置以下参数：
   - **需要用户认证**设置为**否**
   - **使用 SSL** 设置为**必须**
2. 在启用 SSL 的情况下将必需的 WAR 文件部署到 HTTP Server 适配器实例。

注：在配置 HTTP Server 适配器实例时，所有 WAR 文件都必须从 /install_dir/install/noapp/deploy 目录中提取。此外，管理员 Web 应用程序的上下文名称必须与 /install_dir/install/properties/sandbox.cfg 文件中的 ADMIN_CONTEXT_PATH 参数相匹配。对于所有其他 Web 应用程序，该上下文名称应为不带".war"扩展名的 war 文件的名称。

这是必要的，因为这样可以在 HTTP Server 适配器部署中自动反映通过补丁或最新修订程序执行的任何更改。

必需的 WAR 文件包括：

- admin.war
- dashboard.war
- gbm.war
- myaft.war
- portlets.war

可能需要附加 WAR 文件以支持您添加到仪表板的新功能。

3. 打开 sandbox.cfg 文件并修改以下参数：

```
WEBAPP_PROTOCOL=https
WEBAPP_LIST_PORT=<secure_http_server_adapter_port>
```

这些参数供 GPM 用于与服务器通信。

4. （可选，建议）如果要关闭在基本端口上部署仪表板和 GPM Web 应用程序，请在 customer_overrides.properties 文件中指定以下参数：

```
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

例如：

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port.
## Use comma-separated list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars.
## If specified, this should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

5. 如果想要为该功能使用其他证书，请修改 /install_dir/install/properties/customer_overrides.properties 以添加以下行：*noapp.sslCert={mention_name_of_your_own_cert}*。如果未指定其他证书，该功能将使用 ASISslCert。
6. （可选）如果要从使用安全协议（如 HTTPS）的浏览器发送 cookie，请导航至 /install_dir/install/properties，并在 customer_overrides.properties 文件中指定以下参数：

```
## sending cookies as secure over https
http.useSecureCookie=true
```

7. 浏览到 /install_dir/install/bin。

8. 停止 Sterling B2B Integrator。
9. 应用配置更改。输入 `./setupfiles.sh`。
10. 部署新配置。输入 `./deployer.sh`。
11. 启动 Sterling B2B Integrator。
12. 11. 通过访问 https://host:<*secure_http_server_adapter_port*>/dashboard 来验证仪表板 Web 应用程序是否可通过 HTTP Server 适配器进行访问。
13. 通过访问 https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp 来验证 GPM Web 应用程序是否可通过安全 HTTP Server 适配器进行访问。
14. 保存并关闭该文件。
15. 如果已关闭在基本端口上部署仪表板和 GPM Web 应用程序（步骤 4），请验证以下内容：
    - http://host:baseport/dashboard 上的仪表板 Web 应用程序访问是否自动重定向到 https://host:<*secure_http_server_adapter_port*>/dashboard。
    - http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp 上的 GPM Web 应用程序访问是否自动重定向到 https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp。

从 HTTPS 切换到 HTTP 方式

您可以从 HTTPS 切换到 HTTP 方式。

关于此任务

要从 HTTPS 切换到 HTTP 方式：

过程

1. 浏览到 `/install_dir/install/properties`。
2. 打开 **sandbox.cfg** 文件。
3. 修改以下参数：

```
WEBAPP_PROTOCOL=http
WEBAPP_LIST_PORT=<base_port>
```

4. 保存并关闭该文件。
5. （可选）如果在切换到 HTPPS 方式时关闭了在基本端口上部署仪表板和 GPM Web 应用程序，那么必须打开 customer_overrides.properties 文件并注释掉以下参数，这样便不会应用这些参数：

```
## SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## HTTPS_LIST_PORT=<http_server_adapter_port>
```

6. （可选）保存并关闭文件。
7. 浏览到 `/install_dir/install/bin`。
8. 停止 Sterling B2B Integrator。
9. 应用配置更改。输入 `./setupfiles.sh`。
10. 部署新配置。输入 `./deployer.sh`。
11. 启动 Sterling B2B Integrator。

12. 验证以下项：
    - 可在 http://host:baseport/dashboard 上访问仪表板 Web 应用程序
    - 可在 http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp 上访问 GPM Web 应用程序
13. （可选）从支持 SSL 的 HTTP Server 适配器实例取消 Web 应用程序部署。

硬件安全模块 (HSM) V5.2.3 - 5.2.5

硬件安全模块 (HSM)

HSM 是基于硬件的安全设备，用于生成、存储和保护密钥。您可以通过使用 Sterling B2B Integrator 将系统证书存储在数据库中或 HSM 上。

Sterling B2B Integrator 支持以下 HSM 设备：

- SafeNet Eracom ProtectServer Orange External
- ProtectServer Gold PCI 设备

您可以使用 HSM 执行以下操作：

- 在 HSM 上创建系统证书
- 从 Sterling B2B Integrator 导入系统证书
- 从 Sterling B2B Integrator 导出系统证书
- 从 HSM 除去系统证书
- 在 HSM 上查看证书的系统证书详细信息。

针对 HSM 支持的 Sterling B2B Integrator 功能

对于每个密钥对和证书，Sterling B2B Integrator 都在 CERTS_AND_PRI_KEY 表中存储了一个条目。

该条目包含有关以下项的信息：

- 密钥和证书，包括有效期、序列号、使用限制、发行者以及在用户无需实际访问密钥或证书的情况下，UI 用于向该用户显示的主题。
- 在搜索中对系统使用的专有名称执行的规范化。
- 对记录执行的修改。
- 证书撤销状态信息。
- 密钥库类型。
- 对 DATA_TABLE 中存储的二进制密钥库对象的引用。当使用软件密钥库时，引用对象可能包含密钥信息。如果是 HSM，那么其包含引用信息 (nCipher) 或占位符 (Eracom)。

HSM 系统证书参数

下表提供了 CreateSystemCert、ImportSystemCert 和 ExportSystemCert 命令的参数。

参数	描述
autogen	是否使用系统生成的信息来控制对密钥和密钥库的访问。对于 HSM 上的密钥，必须设置为 false。

参数	描述
alias	HSM 中存储的密钥名称。仅包含字符 a-z、A-Z、0-9 或连字符 (-) 且其总长度不超过系统 GUID 长度的别名名称。
Certtype	要导入的证书类型。支持四种类型的证书文件：pkcs12、pkcs8、pem 和 keystore。Sterling B2B Integrator 仅支持使用 DES 或 3DES 加密的 pem 密钥。使用 keystore 列出或导入密钥库。
certname	要分配给 Sterling B2B Integrator 数据库中的证书的名称。
file	要导入的密钥证书或 PEM 文件。
keyname	要创建的 Sterling B2B Integrator 系统密钥的名称。
keypass	用于保护密钥库所在的 SafeNet Eracom HSM 的令牌的 PIN。
key passphrase	专用密钥的口令。在命令行上，此值可选。如果您未提供此值，将提示您输入。密钥库所在的 SafeNet Eracom HSM 上令牌的 PIN。
keysize	RSA 模数的长度，以位计。有效值有 768、1024、2048、3072 或 4096
keystoretype	要导入的密钥库类型。有效值为 CRYPTOKI。
keystoreprovider	提供者类型。SafeNet Eracom 是唯一受 HSM 支持的类型。ERACOM 或 ERACOM.n，前提是将证书导入到缺省槽 0 以外的槽。
keytype	公用密钥算法。RSA 是唯一受支持的算法。
ObjectID	系统证书的标识。
pkcs12file	要导入的 pkcs12 文件。
password	密钥证书或 PEM 文件的存储口令。
pkcs12storepass	PKCS12 文件的存储口令。
pkcs12keypass	用于加密 PKCS12 文件中专用密钥的密钥口令。
提供者	密钥库类型的提供者。ERACOM 或 ERACOM.n，前提是将证书导入到缺省槽 0 以外的槽。
rfc1779rdnsequence	专有名称字符串字段包含"有效值"列中标识的所有字段。仅需要 CN 字段。使用逗号分隔每个字段。有效信息： • CN = 公共名称 • O = 组织 • OU = 组织单元 • L = 所在地 • ST = 省/自治区/直辖市 • C = 国家或地区（提供双字母 ISO3166-1 alpha-2 代码）
storetype	密钥库类型。CRYPTOKI 是唯一支持的密钥库类型。
signingbit	为自签名证书设置签名密钥使用位。值有 true 或 false。
serial	证书序列号。
system passphrase	Sterling B2B Integrator 系统口令。在命令行上，此值可选。
store passphrase	访问密钥库的口令。密钥库所在的 SafeNet Eracom HSM 上令牌的 PIN。在命令行上，此值可选。
systempass	Sterling B2B Integrator 系统口令。
storepass	用于保护密钥库所在的 SafeNet Eracom HSM 的令牌的 PIN。

参数	描述
totrusttable	确定证书是否添加到可信证书表格。值有 true 或 false。
validityindays	证书有效的时间长度，以天计。

SafeNet Eracom HSM

在能够将 HSM 与 Sterling B2B Integrator 一起使用，您必须配置 Sterling B2B Integrator 以使用和识别 SafeNet Eracom HSM。

要安装和设置 SafeNet Eracom HSM，请遵循供应商提供的指示信息；确保您安装了 Java 运行时。将提供者用于设置和使用实用程序时将存储 Sterling B2B Integrator 密钥的槽。为 SafeNet Eracom 槽创建 PIN 后，请勿更改 PIN。如果更改了 PIN，Sterling B2B Integrator 将无法访问 HSM 上的密钥。

SafeNet Eracom 体系结构将 HSM 分成多个槽。根据供应商指示信息安装和配置卡或 HSM。每个槽都具有一个关联的安全提供者，并可以通过单独的个人识别号码 (PIN) 进行保护。您可以在 HSM 上为 Sterling B2B Integrator 创建单独的槽并使用唯一 PIN 保护该槽。缺省槽 0 的提供者是 ERACOM。其他槽的提供者命名为 ERACOM.*n*，其中 *n* 是槽编号。确保 java 运行时组件可用于与设备交互。

配置 Sterling B2B Integrator 以使用 SafeNet Eracom HSM

您可以配置 Sterling B2B Integrator 以使用 SafeNet Eracom HSM。

过程

1. 浏览至 */install_dir*/install/bin。
2. 将以下行添加到 tmp.sh 和 tmp.sh.in 文件：

   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib

   export LD_LIBRARY_PATH
   ```

3. 如果要配置基于网络的服务器，请将以下行添加到 tmp.sh 和 tmp.sh.in 文件，其中 *network_device_IP_OR_hostname* 是 SafeNet Eracom 基于网络的服务器的 IP 地址或标准域名：

   ```
   ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname

   export ET_HSM_NETCLIENT_SERVERLIST
   ```

4. 将 jprov.jar 从 /opt/Eracom/lib 目录复制到 */install_dir*/install/jdk/jre/lib/ext 目录。
5. 向 */install_dir*/install/bin/jdk/jre/lib/security/java.security 文件添加各个安全提供者的定义。要添加定义，请确定分配给 Certicom 提供者的编号，并将 n+1 分配给 SafeNet Eracom 提供者。对于在 SafeNet Eracom 提供者后确定的所有其他提供者，将 security.provider 编号加 1。

   ```
   security.provider.n=com.certicom.ecc.jcae.Certicom

   security.provider.n+1=au.com.eracom.crypto.provider.ERACOMProvider
   ```

如果要使用 SafeNet Eracom HSM 上插槽 0 以外的插槽，请按如下所示指定插槽，其中 *x* 是插槽编号：

```
security.provider.n+1=au.com.eracom.crypto.provider.slotx.ERACOMProvider
```

6. 在 */install_dir*/install/properties/security.properties 文件中定义 TLSProviderPolicy。
   - 如果在插槽 0 中定义提供者，请确保以下是 TLSProviderPolicy 参数唯一未注释的行：

```
TLSProviderPolicy= TLS:*:ECMQV:P:.CT;TLS:SIG:MD2withRSA:P:ERACOM;TLS:Cipher:RawRSA:P:ERACOM;TLS:*
:RSA:P:ERACOM;TLS:*:*:P:Certicom
```

   - 如果在插槽 0 以外的插槽中定义提供者，请按如下所示修改 TLSProviderPolicy 参数，其中 *x* 是要配置的插槽：

```
TLSProviderPolicy=TLS:*:ECMQV:P:.CT;TLS:SIG:MD2withRSA:P:ERACOM.x;TLS:Cipher:RawRSA:P:ERACOM.
x;TLS:*:RSA:P:ERACOM.x;TLS:*:*:P:Certicom
```

7. 在 */install_dir*/install/properties/security.properties 文件中定义 KeyStoreProviderKey 命令：
   - 如果在插槽 0 中定义提供者，请确保 KeyStoreProviderMap 定义如下：

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;
nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM, true,ERACOM,ERACOM,true
```

   - 如果在插槽 0 以外的任何插槽中定义提供者，请按如下所示修改 KeyStoreProviderMap 参数，其中 *x* 是插槽编号：

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;
nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true; CRYPTOKI,ERACOM.x,true,ERACOM.x,ERACOM.x,true
```

受支持的 nCipher 和 SafeNet/Eracom 网络及 PCI 设备

除了支持 nCipher，Sterling B2B Integrator 目前还支持 Safenet/Eracom ProtectServer Orange PCI 卡和 Orange External 网络设备。

支持以下各项：

制造商	受支持的设备类型
nCipher	• nShield 系列的 PCI 卡 • NetHSM 网络设备
Safenet/Eracom	• ProtectServer Gold PCI 卡 • ProtectServer Orange PCI 卡 • ProtectServer Orange External 网络设备

使用硬件安全模块

创建要存储在 HSM 上的系统证书

您可以创建存储在 HSM 上的自签名系统证书。

开始之前

开始之前：

- 停止 Sterling B2B Integrator。
- 确保 Sterling B2B Integrator 数据库正在运行。

关于此任务

要创建将会存储在 HSM 上的自签名系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. 如果未在命令行上提供系统口令、存储口令以及密钥口令，那么将提示您输入这些口令。

列出 HSM 中存储的系统证书

您可以列出与 HSM 中存储的系统证书有关的信息：

关于此任务

要列出与 HSM 中存储的系统证书有关的信息：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

示例

以下是命令输出示例：

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

将 HSM 系统证书导入 Sterling B2B Integrator 数据库

当密钥或证书已存在于 HSM 上且已添加到独立于 Sterling B2B Integrator 的 HSM 时，请使用此过程。您必须将存储在 HSM 上的系统证书的信息导入数据库，该证书才能供 Sterling B2B Integrator 使用。

关于此任务

根据向 HSM 添加专用密钥和证书所采用的方法，列出功能可能会显示一个密钥和证书对的重复条目。

必须获取系统证书别名，然后才能将系统证书的信息导入到数据库。

要导入系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

除去 HSM 中存储的系统证书

您可以从 HSM 中永久删除系统证书。将无法恢复证书包含的专用密钥数据。

关于此任务

要除去 HSM 中存储的系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./RemoveSystemCert.sh -r` *xxxx*

   其中 *xxxx* 是要除去的证书的对象标识。

导出系统证书

您可以从 Sterling B2B Integrator 中导出系统证书以便将其导入 HSM。

关于此任务

HSM 上的系统证书不能使用 ExportSystemCert.sh 进行导出。

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. 输入您的口令。

示例：HSM 系统证书

您可以采用密钥证书、pkcs12 或 pem 格式将系统证书导入 HSM。导入系统证书将向 HSM 添加密钥和证书，并在 Sterling B2B Integrator 数据库中创建对应条目。

如果导入 pem 类型的证书和密钥，请确保以 DES 或三重 DES 加密格式创建专用密钥。

以下是以三重 DES 格式创建的样本 pem 专用密钥：

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
```

```
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

管理系统证书实用程序

HSM 密钥对和证书签名请求

GenCSR 实用程序在 HSM 上生成密钥对，并使用该密钥对的公用密钥创建 PKCS10 证书签名请求 (CSR)。然后，您可以将 CSR 提交到认证中心 (CA)。

收到 CA 发出的证书后，请使用 GenCSR 更新证书。在使用 CA 发出的证书更新系统证书之前，Sterling B2B Integrator 中将不会提供该系统证书。

您还可以使用该实用程序来查看 CSR 列表，将 CSR 信息写入文件，删除 CSR 或将与 HSM 上存储的 CA 发出的证书有关的信息写入文件。与 CSR 有关的信息保存在 Sterling B2B Integrator 数据库中，而实际的密钥存储在 HSM 上。

要使用该实用程序，请首先确定要执行的操作。然后，在命令行中使用 GenCSR 实用程序并确定操作。对于每个操作，请在属性文件中提供操作所需的自变量。*/install_dir*/install/properties 目录中提供了名为 csr.properties.sample 的样本属性文件。

GenCSR 实用程序位于 */install_dir*/install/bin 目录中。

命令语法为：`GenCSR.sh -a ACTION -p PROPERTIES`

GenCSR 参数

下表提供了运行 GenCSR 脚本时所使用的参数。

参数	描述	有效值
-a ACTION	要执行的操作。	有效操作包括： • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	包含操作所需的附加参数的属性文件。您需要包含属性文件的路径。	属性文件的名称。 例如：`csr_create.properties`

使用 CA 发出的证书更新 HSM 密钥库

将 GenCSR 实用程序和 update 自变量一起使用以向 HSM 密钥库添加 CA 发出的证书信息。

过程

1. 确保正确配置了 csr_update.properties 文件。

   下表描述了 csr_update.properties 文件中 update 自变量所需的参数。

参数	描述	有效值
提供者	密钥库提供者的名称。	ERACOM 或 ERACOM.n
keystoretype	所使用的密钥库的名称。	CRYPTOKI
certificate.request.Name	要更新的 CSR 的名称。	分配给 CSR 的名称
add.trusted	确定证书信息是否添加到可信证书表。	True | false
ca.cert.file	要将 CA 发出的证书的相关信息写入到的文件的路径和文件名。	CA 发出的证书文件的有效路径和文件名

2. 更新 HSM 密钥库。

   命令语法为：`./GenCSR.sh -a update -p ../properties/csr_update.properties`

列出证书签名请求

将 GenCSR 实用程序与 list 自变量一起使用以显示 HSM 数据库中的 CSR。list 自变量不需要属性文件配置。

关于此任务

命令语法为：`./GenCSR.sh -a list`

删除证书签署请求

将 GenCSR 实用程序与 delete 自变量一起使用以删除 CSR。该实用程序仅删除 CSR。并不会删除与 CA 发放的证书一起更新的系统证书。

过程

1. 确保正确配置了 cacert.properties 文件。 在使用 delete 自变量前，必须配置该属性文件。下表描述了 cacert.properties 文件中用于 delete 自变量的必需参数。

参数	描述	有效值
certificate.request.Name	要删除的 CSR 的名称。	CSR 的名称
keystoretype	所使用的密钥库的名称。	CRYPTOKI
提供者	密钥库提供者的名称。	ERACOM[.N]

2. 删除 CSR。 该命令语法为 `./GenCSR.sh -a delete -p ../properties/cacert.properties`

将 CSR 信息写成 pkcs10 格式

将 GenCSR 实用程序与 getpkcs10 自变量一起使用以将 CSR 以 pkcs10 格式写入指定文件。

过程

1. 确保正确配置了 csr_getpkcs10.properties 文件。

   下表描述了 csr_getpkcs10.properties 文件中 getpkcs10 自变量所需的参数。在使用 getpkcs10 自变量之前，必须配置该属性文件。

参数	描述	有效值
certificate.request.Name	CSR 的名称。	分配给 CSR 的名称
keystoretype	所使用的密钥库的名称。	CRYPTOKI
csr.file	要将 CSR 信息写入到的文件的标准路径。	要写入 CSR 信息的文件的路径和文件名

2. 将 CSR 写入文件。

   命令语法为 `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

将系统证书移到 HSM

您可以将自签名证书或 CA 发行的证书从数据库移动到 HSM。

关于此任务

使用 CreateSystemCert.sh 或 GenCSR.sh 来重新生成密钥和证书更为安全。

要将自签名证书或 CA 发出的证书从数据库移动到 HSM：

过程

1. 浏览至 */install_dir*/install/bin。
2. 停止 Sterling B2B Integrator。
3. 启动数据库。
4. 将系统证书导出到 PKCS12 文件：

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass
   ```

5. 查找要除去的系统证书的对象标识。输入：

   ```
   ./RemoveSystemCert.sh -l.
   ```

6. 从数据库除去系统证书。输入：

   `RemoveSystemCert.sh -r xxxx`，其中 *xxxx* 是要除去的证书的对象标识。

7. 要将导出的系统证书导入到 HSM 并创建对应的数据库条目：

   ```
   ./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file pkcs12storepass
   pkcs12keypass keystoretype keystoreprovider storepass keypass
   ```

注：如果将 OpsDrv、OpsKey 和 UIKey 移动到 HSM，请使用准确名称。否则，Sterling B2B Integrator 将不能正常运行。对于所有其他系统证书，名称并不重要。在移动除 OpsDrv、OpsKey 和 UIKey 以外的其他系统证书时，服务和适配器所使用的对象标识将发生更改。重新配置使用已移动的系统证书的所有服务。

将 CA 发出的证书写入文件

将 GenCSR 实用程序与 getcacert 自变量一起使用以将 CA 发出的证书写入文件。

过程

1. 确保正确配置了 getcacert.properties 文件。

   下表描述了 getcacert.properties 文件中 getcacert 操作所需的参数。在使用 getcacert 自变量之前，必须配置 getcacert.properties 文件。

参数	描述	有效值
certificate.request.Name	CSR 的名称。	证书名称
keystoretype	所使用的密钥库的名称。	CRYPTOKI
ca.cert.file	要将 CA 证书信息写入到的文件的标准路径。	CA 证书文件的名称和路径

2. 将证书写入文件。

   命令语法为 `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

在 HSM 上生成内部系统证书（OpsDrv、OpsKey、UIKey）

有三个系统证书随 Sterling B2B Integrator 一起安装，以保护内部操作。将它们移到 HSM 上对安全性的益处并不大。安全策略可能需要包含 HSM 上存储的专用密钥的所有证书。

关于此任务

在 HSM 上生成名为 OpsDrv、OpsKey 和 UIKey 的 Sterling B2B Integrator 内部系统证书时，请使用确切的名称。否则，Sterling B2B Integrator 将不能正常运行。

要生成内部系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入 `./RemoveSystemCert.sh -l` 以查看数据库中的证书。请记录每个系统证书的对象标识。
3. 要通过针对每个证书运行以下命令从数据库中删除系统证书：`./RemoveSystemCert.sh -r xxxx`，其中 *xxxx* 是要除去的证书的对象标识。
4. 在 HSM 上针对每个证书生成系统证书，请输入：

   ```
   ./CreateSystemCert.sh storetype provider autogen totrusttable signingbit
   keytype keysize keyname rfc1779rdnsequence serial validityindays [system
   passphrase] [store passphrase] [key passphrase]
   ```

使用 nCipher 和 SafeNetEracom

密钥库提供者映射

由于 Sterling B2B Integrator 具有在密码服务提供者中唯一的密钥库类型，因此它能够定义密钥库类型与提供者之间的映射，这是实施密钥库对象本身、签名算法及密钥传输算法所必需的。

密钥和密钥信息抽象对象包含此信息，以及对 com.sterlingcommerce.security.PrivateKeyInfo 的引用。

这使 Sterling B2B Integrator 能够同时使用 HSM 上密钥以及数据库的软件存储中密钥的组合，而无需除将密钥或密钥信息初始装入数据库之外的其他配置。对于 Sterling B2B Integrator，无论密钥存储在什么位置，看起来都相同。

在 security.properties 中，映射作为 KeyStoreProviderMap 属性实施。它由以分号 (;) 分隔的一组条目构成。每个条目包含由逗号分隔的六个元素，格式如下：

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

下表中描述了这些元素：

元素	描述	附加信息
KeyStoreType	密钥库的字符串类型	
KeyStoreProvider	实施密钥库的密码服务提供者的名称	
DoesAliasMatter	密钥别名对此密钥库类型是否必须唯一	该元素可为 true 或 false。如果每个设备只有一个密钥库，那么密钥必须具有唯一别名。
SignatureProvider	要用于通过密钥库的密钥来创建签名的密码服务提供者的名称	
EncryptionProvider	使用密钥库中的密钥解密信息时要使用的密码服务提供者的名称	这主要针对 RSA 密钥传输操作
KeyOnHSM	密钥库是否位于 HSM 上	

字符串 null 是可接受的值，将按照未指定提供者那样进行处理。一个条目必须至少包含两个值。如果条目包含的值少于六个，那么会从左到右将这些值分配给密钥库提供者，无论存储密钥、签名提供者、加密提供者时别名是否重要，以及无论 HSM 上是否存在密钥库类型的密钥都将如此。其他将视为 null，将不会针对具有此类型密钥的操作请求特定提供者。

缺省 KeyStoreProviderMap 当前是：

```
KeyStoreProviderMap=SCIKS,SCIKS,false,Certicom,Certicom,false;nCipher.sworld,
nCipherKM,false,nCipherKM,nCipherKM,true;CRYPTOKI,ERACOM,true,ERACOM,ERACOM,true
```

管理 HSM 密钥和密钥信息

Sterling B2B Integrator 具有若干用于在 HSM 上管理密钥的 java 脚本。

java 程序列示如下。

程序	目的
com.sterlingcommerce.db.RemoveSystemCert	列出和删除 Sterling B2B Integrator 系统证书。在删除期间，程序尽量清除密钥库中的密钥，并覆盖数据库中的密钥库对象。
com.sterlingcommerce.db.CreateCertEx	在 HSM 上生成密钥对，并生成包含密钥对的公用密钥的自签名证书。
com.sterlingcommerce.security.util. CertificateSigningRequest	在 HSM 上生成密钥对，并创建和管理关联的 PKCS10 证书签名请求。可向认证中心提供 PKCS10 以获取认证中心签署的证书。然后，此程序可用于将该证书装入密钥库并使之与正确的密钥对关联。
com.sterlingcommerce.db.ImportSystemCert	将专用密钥和受支持格式（PKCS12 或 PEM）的证书导入 HSM 上的密钥库。将与 HSM 上的专用密钥和证书有关的信息导入 Sterling B2B Integrator 数据库。

针对 nCipher HSM 支持的 JDK 更改

要使 Sterling B2B Integrator 可以使用 nCipher HSM，您必须安装 nCipher java 密码服务提供者。要进行安装，请将以下 jar 文件复制到 JDK 的 jre/lib/ext 子目录。修改 java.security 以装入 nCipher 提供者。

以下文件由 nCipher 安装程序放置在 /opt/nfast/java/classes 中：

- rsaprivenc.jar
- nfjava.jar
- kmjava.jar
- jutils.jar
- kmcsp.jar

应在 IBM JCE 提供者之后，Certicom 提供者之前添加 nCipher 提供者。例如：

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
```

在具有 SUN JDK 的 Solaris 系统上，应将 nCipher 提供者放在 Sun JCA 和 JCE 提供者之后，Certicom 提供者之前。例如：

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.4=com.ncipher.provider.km.nCipherKM
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=com.sun.net.ssl.internal.ssl.Provider
security.provider.7=com.sun.rsajca.Provider
security.provider.8=sun.security.jgss.SunProvider
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
```

使用 security.properties 中的样本设置 TLSProvider 策略。例如：

```
TLSProviderPolicy=TLS:MD:MD5:P:Certicom;TLS:MD:SHA1:P:Certicom;TLS:MAC:HmacMD5:P:Certicom;
TLS:MAC:HmacSHA1:P:Certicom;TLS:SIG:MD2withRSA:P:Certicom;TLS:Cipher:RawRSA:P:Certicom;
TLS:*:ECDH:P:Certicom;TLS:*:ECDSA:P:Certicom;TLS:*:*:P:nCipherKM
```

针对 Eracom HSM 支持的 JDK 更改

为使 Sterling B2B Integrator 能够使用 Eracom HSM，必须安装 Eracom java 密码服务提供者。要进行安装，请将 appropriate.jar 文件放置在 JDK 的 jre/lib/ext 子目录，然后修改 java.security 以装入 nCipher 提供者。

以下文件由 nCipher 安装程序放置在 /opt/nfast/java/classes 中：

- jcprov.jar
- jprov.jar

应在 Certicom 提供者后添加 Eracom 提供者。例如：

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=au.com.eracom.crypto.provider.ERACOMProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.8=com.sterlingcommerce.security.provider.SCI
```

注：Eracom 包含可为卡上的每个槽进行指定的提供者。对于槽 8 的提供者，请使用：

```
security.provider.3=au.com.eracom.crypto.provider.slot8.ERACOMProvider
```

针对 nCipher HSM 支持的 Linux 环境更改

nCipher 建议您创建特殊用户帐户以运行 nCipher 硬服务器。

用于运行 Sterling B2B Integrator 的帐户需要具有等效许可权，或者需要利用 nCipher 特殊帐户或以 root 用户身份运行 Sterling B2B Integrator。如果采用上述任一方法而使用 MySQL，那么必须更改 MySQL 的许可权，或者从普通帐户启动 MySQL，然后再调用 run.sh。

针对 Eracom HSM 支持的 Linux 环境更改

要使用 Eracom 设备，您必须在环境变量中对访问该设备的会话提供额外信息。

建议对 PATH、LD_LIBRARY_PATH 和 MANPATH 执行如下更改：

```
PATH=$PATH:/opt/Eracom/bin LD_LIBRARY_PATH=$LD_LIBRARY_PATH
:/opt/Eracom/lib MANPATH=$MANPATH:/opt/Eracom/man
```

此外，如果使用的是网络设备而非本地 PCI 卡，那么还必须提供 ET_HSM_NETCLIENT_SERVERLIST，如下所示：

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

应将这些变量导出到 tmp.sh 中。

硬件安全模块 (HSM) V5.2.6 或更高版本

硬件安全模块 (HSM)

HSM 是基于硬件的安全设备，用于生成、存储和保护密钥。您可以通过使用 Sterling B2B Integrator 将系统证书存储在数据库中或 HSM 上。

Sterling B2B Integrator 支持以下 HSM 设备：

- SafeNet Luna SA
- nCipher nShield Connect

您可以使用 HSM 执行以下操作：

- 在 HSM 上创建系统证书
- 从 Sterling B2B Integrator 导入系统证书
- 从 Sterling B2B Integrator 导出系统证书
- 从 HSM 除去系统证书
- 在 HSM 上查看证书的系统证书详细信息。

针对 HSM 支持的 Sterling B2B Integrator 功能

对于每个密钥对和证书，Sterling B2B Integrator 都在 CERTS_AND_PRI_KEY 表中存储了一个条目。

该条目包含有关以下项的信息：

- 密钥和证书，包括有效期、序列号、使用限制、发行者以及在用户无需实际访问密钥或证书的情况下，UI 用于向该用户显示的主题。
- 在搜索中对系统使用的专有名称执行的规范化。
- 对记录执行的修改。
- 证书撤销状态信息。
- 密钥库类型。
- 对 DATA_TABLE 中存储的二进制密钥库对象的引用。当使用软件密钥库时，引用对象可能包含密钥信息。如果是 HSM，那么它包含引用信息 (nCipher) 或占位符 (Luna)。

HSM 系统证书参数

下表提供了 CreateSystemCert、ImportSystemCert 和 ExportSystemCert 命令的参数。

参数	描述
autogen	是否使用系统生成的信息来控制对密钥和密钥库的访问。对于 HSM 上的密钥，必须设置为 false。

参数	描述
alias	HSM 中存储的密钥名称。仅包含字符 a-z、A-Z、0-9 或连字符 (-) 且其总长度不超过系统 GUID 长度的别名名称。
Certtype	要导入的证书类型。支持四种类型的证书文件：pkcs12、pkcs8、pem 和 keystore。Sterling B2B Integrator 仅支持使用 DES 或 3DES 加密的 pem 密钥。使用 keystore 列出或导入密钥库。
certname	要分配给 Sterling B2B Integrator 数据库中的证书的名称。
file	要导入的密钥证书或 PEM 文件。
keyname	要创建的 Sterling B2B Integrator 系统密钥的名称。
keypass	用于保护密钥库所在位置的 SafeNet 或 nCipher HSM 的令牌的 PIN。
key passphrase	专用密钥的口令。在命令行上，此值可选。如果您未提供此值，将提示输入此值。
keysize	RSA 模数的长度，以位计。有效值是 1024、2048、3072 或 4096
keystoretype	要导入的密钥库类型。有效值是 nCipher.sworld、Luna 或 PKCS11IMPLKS（自 V5.2.6.2 起）。
keystoreprovider	提供者类型。有效值是 nCipherKM、LunaProvider 或 IBMPKCS11Impl（自 V5.2.6.2 起）。
keytype	公用密钥算法。RSA 是唯一受支持的算法。
ObjectID	系统证书的标识。
pkcs12file	要导入的 pkcs12 文件。
password	密钥证书或 PEM 文件的存储口令。
pkcs12storepass	PKCS12 文件的存储口令。
pkcs12keypass	用于加密 PKCS12 文件中专用密钥的密钥口令。
提供者	密钥库类型的提供者。有效值是 nCipherKM、LunaProvider 或 IBMPKCS11Impl（自 V5.2.6.2 起）。
rfc1779rdnsequence	专有名称字符串字段包含"有效值"列中标识的所有字段。仅需要 CN 字段。使用逗号分隔每个字段。有效信息： • CN = 公共名称 • O = 组织 • OU = 组织单元 • L = 所在地 • ST = 省/自治区/直辖市 • C = 国家或地区（提供双字母 ISO3166-1 alpha-2 代码）
storetype	密钥库类型。有效值是 nCipher.sworld、Luna 或 PKCS11IMPLKS（自 V5.2.6.2 起）。
signingbit	为自签名证书设置签名密钥使用位。值有 true 或 false。
serial	证书序列号。
system passphrase	Sterling B2B Integrator 系统口令。在命令行上，此值可选。
store passphrase	访问密钥库的口令。在命令行上，此值可选。如果您未提供此值，将提示输入此值。
systempass	Sterling B2B Integrator 系统口令。

参数	描述
storepass	用于保护密钥库所在位置的 SafeNet 或 nCipher HSM 的令牌的 PIN。
totrusttable	确定证书是否添加到可信证书表格。值有 true 或 false。
validityindays	证书有效的时间长度，以天计。

使用硬件安全模块

创建要存储在 HSM 上的系统证书

您可以创建存储在 HSM 上的自签名系统证书。

开始之前

开始之前：

- 停止 Sterling B2B Integrator。
- 确保 Sterling B2B Integrator 数据库正在运行。

关于此任务

要创建将会存储在 HSM 上的自签名系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. 如果未在命令行上提供系统口令、存储口令以及密钥口令，那么将提示您输入这些口令。

列出 HSM 中存储的系统证书

您可以列出与 HSM 中存储的系统证书有关的信息：

关于此任务

要列出与 HSM 中存储的系统证书有关的信息：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

示例

以下是命令输出示例：

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

注：自 V5.2.6.2 起，Keystoretype 的有效值是 PKCS11IMPLKS。

将 HSM 系统证书导入 Sterling B2B Integrator 数据库

当密钥或证书已存在于 HSM 上且已添加到独立于 Sterling B2B Integrator 的 HSM 时，请使用此过程。您必须将存储在 HSM 上的系统证书的信息导入数据库，该证书才能供 Sterling B2B Integrator 使用。

关于此任务

根据向 HSM 添加专用密钥和证书所采用的方法，列出功能可能会显示一个密钥和证书对的重复条目。

必须获取系统证书别名，然后才能将系统证书的信息导入到数据库。

要导入系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

除去 HSM 中存储的系统证书

关于此任务

本过程将从 HSM 永久删除系统证书。将无法恢复证书包含的专用密钥数据。

要除去 HSM 中存储的系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./RemoveSystemCert.sh -r` *xxxx*

   其中 *xxxx* 是要除去的证书的对象标识。

导出系统证书

您可以从 Sterling B2B Integrator 中导出系统证书以便将其导入 HSM。

关于此任务

HSM 上的系统证书不能使用 ExportSystemCert.sh 进行导出。

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入： `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. 输入您的口令。

示例：HSM 系统证书

您可以采用密钥证书、pkcs12 或 pem 格式将系统证书导入 HSM。导入系统证书将向 HSM 添加密钥和证书，并在 Sterling B2B Integrator 数据库中创建对应条目。

如果导入 pem 类型的证书和密钥，请确保以 DES 或三重 DES 加密格式创建专用密钥。

以下是以三重 DES 格式创建的样本 pem 专用密钥：

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

管理系统证书实用程序

HSM 密钥对和证书签名请求

GenCSR 实用程序在 HSM 上生成密钥对，并使用该密钥对的公用密钥创建 PKCS10 证书签名请求 (CSR)。然后，您可以将 CSR 提交到认证中心 (CA)。

收到 CA 发出的证书后，请使用 GenCSR 更新证书。在使用 CA 发出的证书更新系统证书之前，Sterling B2B Integrator 中将不会提供该系统证书。

您还可以使用该实用程序来查看 CSR 列表，将 CSR 信息写入文件，删除 CSR 或将与 HSM 上存储的 CA 发出的证书有关的信息写入文件。与 CSR 有关的信息保存在 Sterling B2B Integrator 数据库中，而实际的密钥存储在 HSM 上。

要使用该实用程序，请首先确定要执行的操作。然后，在命令行中使用 GenCSR 实用程序并确定操作。对于每个操作，请在属性文件中提供操作所需的自变量。*/install_dir*/install/properties 目录中提供了名为 csr.properties.sample 的样本属性文件。

GenCSR 实用程序位于 */install_dir*/install/bin 目录中。

命令语法为：`GenCSR.sh -a ACTION -p PROPERTIES`

GenCSR 参数

下表提供了运行 GenCSR 脚本时所使用的参数。

参数	描述	有效值
-a ACTION	要执行的操作。	有效操作包括： • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	包含操作所需的附加参数的属性文件。您需要包含属性文件的路径。	属性文件的名称。 例如：`csr_create.properties`

使用 CA 发出的证书更新 HSM 密钥库

关于此任务

将 GenCSR 实用程序和 update 自变量一起使用以向 HSM 密钥库添加 CA 发出的证书信息。

过程

1. 确保正确配置了 csr_update.properties 文件。

   下表描述了 csr_update.properties 文件中 update 自变量所需的参数。

参数	描述	有效值
提供者	密钥库提供者的名称。	IBMPKCS11IMPL（自 V5.2.6.2 起）、nCipherKM 或 LunaProvider
keystoretype	所使用的密钥库的名称。	PKCS11IMPLKS（自 V5.2.6.2 起）、nCipher.sworld 或 Luna **注：**"keystoretype"值应与"provider"值同步。
certificate.request.Name	要更新的 CSR 的名称。	分配给 CSR 的名称
add.trusted	确定证书信息是否添加到可信证书表。	True | false
ca.cert.file	要将 CA 发出的证书的相关信息写入到的文件的路径和文件名。	CA 发出的证书文件的有效路径和文件名

2. 更新 HSM 密钥库。

   命令语法为：`./GenCSR.sh -a update -p ../properties/csr_update.properties`

列出证书签名请求

将 GenCSR 实用程序与 list 自变量一起使用以显示 HSM 数据库中的 CSR。list 自变量不需要属性文件配置。

关于此任务

命令语法为：`./GenCSR.sh -a list`

删除证书签署请求

将 GenCSR 实用程序与 delete 自变量一起使用以删除 CSR。该实用程序仅删除 CSR。并不会删除与 CA 发放的证书一起更新的系统证书。

过程

1. 确保正确配置了 cacert.properties 文件。 在使用 delete 自变量前，必须配置该属性文件。下表描述了 cacert.properties 文件中用于 delete 自变量的必需参数。

参数	描述	有效值
certificate.request.Name	要删除的 CSR 的名称。	CSR 的名称
keystoretype	所使用的密钥库的名称。	PKCS11IMPLKS（自 V5.2.6.2 起）、nCipher.sworld 或 Luna
提供者	密钥库提供者的名称。	IBMPKCS11IMPL（在 V5.2.6.2 之前）、nCipherKM 或 LunaProvider **注：** "keystoretype"值应与"provider"值同步。

2. 删除 CSR。 该命令语法为 `./GenCSR.sh -a delete -p ../properties/cacert.properties`

将 CSR 信息写成 pkcs10 格式

关于此任务

将 GenCSR 实用程序与 getpkcs10 自变量一起使用以将 CSR 以 pkcs10 格式写入指定文件。

过程

1. 确保正确配置了 csr_getpkcs10.properties 文件。

   下表描述了 csr_getpkcs10.properties 文件中 getpkcs10 自变量所需的参数。在使用 getpkcs10 自变量之前，必须配置该属性文件。

参数	描述	有效值
certificate.request.Name	CSR 的名称。	分配给 CSR 的名称
keystoretype	所使用的密钥库的名称。	PKCS11IMPLKS（自 V5.2.6.2 起）、nCipher.sworld 或 Luna
csr.file	要将 CSR 信息写入到的文件的标准路径。	要写入 CSR 信息的文件的路径和文件名

2. 将 CSR 写入文件。

   命令语法为 `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

将系统证书移到 HSM

您可以将自签名证书或 CA 发行的证书从数据库移动到 HSM。

关于此任务

使用 CreateSystemCert.sh 或 GenCSR.sh 来重新生成密钥和证书更为安全。

要将自签名证书或 CA 发出的证书从数据库移动到 HSM：

过程

1. 浏览至 */install_dir*/install/bin。
2. 停止 Sterling B2B Integrator。
3. 启动数据库。
4. 将系统证书导出到 PKCS12 文件：

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass
   ```

5. 查找要除去的系统证书的对象标识。输入：

   ```
   ./RemoveSystemCert.sh -l.
   ```

6. 从数据库除去系统证书。输入：

   `RemoveSystemCert.sh -r` *xxxx*，其中 *xxxx* 是要除去的证书的对象标识。

7. 要将导出的系统证书导入到 HSM 并创建对应的数据库条目：

   ```
   ./ImportSystemCert.sh -pkcs12 systempass certname pkcs12file pkcs12storepass pkcs12keypass keystoretype keystoreprovider storepass keypass
   ```

   注：如果将 OpsDrv、OpsKey 和 UIKey 移动到 HSM，请使用准确名称。否则，Sterling B2B Integrator 将不能正常运行。对于所有其他系统证书，名称并不重要。在移动除 OpsDrv、OpsKey 和 UIKey 以外的其他系统证书时，服务和适配器所使用的对象标识将发生更改。重新配置使用已移动的系统证书的所有服务。

将 CA 发出的证书写入文件

关于此任务

将 GenCSR 实用程序与 getcacert 自变量一起使用以将 CA 发出的证书写入文件。

过程

1. 确保正确配置了 getcacert.properties 文件。

   下表描述了 getcacert.properties 文件中 getcacert 操作所需的参数。在使用 getcacert 自变量之前，必须配置 getcacert.properties 文件。

参数	描述	有效值
certificate.request.Name	CSR 的名称。	证书名称

参数	描述	有效值
keystoretype	所使用的密钥库的名称。	PKCS11IMPLKS（自 V5.2.6.2 起）、nCipher.sworld 或 Luna
ca.cert.file	要将 CA 证书信息写入到的文件的标准路径。	CA 证书文件的名称和路径

2. 将证书写入文件。

   命令语法为 `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

在 HSM 上生成内部系统证书（OpsDrv、OpsKey、UIKey）

有三个系统证书随 Sterling B2B Integrator 一起安装，以保护内部操作。将它们移到 HSM 上对安全性的益处并不大。安全策略可能需要包含 HSM 上存储的专用密钥的所有证书。

关于此任务

在 HSM 上生成名为 OpsDrv、OpsKey 和 UIKey 的 Sterling B2B Integrator 内部系统证书时，请使用确切的名称。否则，Sterling B2B Integrator 将不能正常运行。

要生成内部系统证书：

过程

1. 浏览至 */install_dir*/install/bin。
2. 输入 `./RemoveSystemCert.sh -l` 以查看数据库中的证书。请记录每个系统证书的对象标识。
3. 要通过针对每个证书运行以下命令从数据库中删除系统证书：`./RemoveSystemCert.sh -r xxxx`，其中 *xxxx* 是要除去的证书的对象标识。
4. 在 HSM 上针对每个证书生成系统证书，请输入：

   ```
   ./CreateSystemCert.sh storetype provider autogen totrusttable signingbit
   keytype keysize keyname rfc1779rdnsequence serial validityindays [system
   passphrase] [store passphrase] [key passphrase]
   ```

配置 nCipher 和 SafeNet Luna 设备

密钥库提供者映射

由于 Sterling B2B Integrator 具有在密码服务提供者中唯一的密钥库类型，因此它能够定义密钥库类型与提供者之间的映射，这是实施密钥库对象本身、签名算法及密钥传输算法所必需的。

密钥和密钥信息抽象对象包含此信息，以及对 com.sterlingcommerce.security.PrivateKeyInfo 的引用。

这使 Sterling B2B Integrator 能够同时使用 HSM 上密钥以及数据库的软件存储中密钥的组合，而无需除将密钥或密钥信息初始装入数据库之外的其他配置。对于 Sterling B2B Integrator，无论密钥存储在什么位置，看起来都相同。

在 security.properties 中，映射作为 KeyStoreProviderMap 属性实施。它由以分号 (;) 分隔的一组条目构成。每个条目包含由逗号分隔的六个元素，格式如下：

```
KeyStoreType, KeyStoreProvider, DoesAliasMatter, SignatureProvider,
EncryptionProvider, KeyOnHSM
```

下表中描述了这些元素：

元素	描述	附加信息
KeyStoreType	密钥库的字符串类型	
KeyStoreProvider	实施密钥库的密码服务提供者的名称	
DoesAliasMatter	密钥别名对此密钥库类型是否必须唯一	该元素可为 true 或 false。如果每个设备只有一个密钥库，那么密钥必须具有唯一别名。
SignatureProvider	要用于通过密钥库的密钥来创建签名的密码服务提供者的名称	
EncryptionProvider	使用密钥库中的密钥解密信息时要使用的密码服务提供者的名称	这主要针对 RSA 密钥传输操作
KeyOnHSM	密钥库是否位于 HSM 上	

字符串 null 是可接受的值，将按照未指定提供者那样进行处理。一个条目必须至少包含两个值。如果条目包含的值少于六个，那么会从左到右将这些值分配给密钥库提供者，无论存储密钥、签名提供者、加密提供者时别名是否重要，以及无论 HSM 上是否存在密钥库类型的密钥都将如此。其他将视为 null，将不会针对具有此类型密钥的操作请求特定提供者。

缺省 KeyStoreProviderMap 当前是：

```
nCipher = nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true
SafeNet Luna = Luna,LunaProvider,true,LunaProvider,LunaProvider,true
对 V5.2.6.2 之后的 nCipher 和 SafeNet Luna 都使用
"PKCS11IMPLKS,IBMPKCS11Impl,true,IBMPKCS11Impl,IBMPKCS11Impl,true"。
```

针对 nCipher HSM 支持的 JDK 更改

要使 Sterling B2B Integrator 可以使用 nCipher HSM，您必须安装 nCipher java 密码服务提供者。要进行安装，请将以下 jar 文件复制到 JDK 的 jre/lib/ext 子目录。修改 java.security 以装入 nCipher 提供者。

注：

1. 如果您在 V5.2.6.2 之后的版本中使用"PKCS11IMPLKS"实施新建密钥或证书，那么将不需要下列设置。
2. 在升级到 V5.2.6.2 后，要继续使用现有密钥或证书，请执行以下步骤。

下列文件由 nCipher 安装程序放置在 /opt/nfast/java/classes 中：

- jcetools.jar
- jutils.jar
- keysafe.jar

- kmjava.jar
- nCipherKM.jar
- nfjava.jar
- rsaprivenc.jar

应在 IBM JCE 提供者之后，Certicom 提供者之前添加 nCipher 提供者。

同时，您必须将 IBMJCEFIPS 从列表中移除。

例如：

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

在 V5.2.6.2 之后的版本中使用下列示例以支持现有密钥或证书。

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.provider.km.nCipherKM
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

SafeNet Luna HSM 支持的 JDK 更改

为使 Sterling B2B Integrator 可以使用 SafeNet Luna HSM，您必须安装 SafeNet Luna java 密码服务提供者。要进行安装，请将 appropriate.jar 文件放置在 JDK 的 jre/lib/ext 子目录并修改 java.security 以装入 Luna 提供者。

注：

1. 如果您在 V5.2.6.2 之后的版本中使用"PKCS11IMPLKS"实施新建密钥或证书，那么将不需要下列设置。
2. 在升级到 V5.2.6.2 后，要继续使用现有密钥或证书，请执行以下步骤。

以下文件由 nCipher 安装程序放置在 /opt/nfast/java/classes 中：

- libLunaAPI.so
- LunaProvider.jar

您应该在 IBM JCE 提供者之后和 Certicom 提供者之前添加 LunaProvider。

同时，您必须将 IBMJCEFIPS 从列表中移除。

例如：

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.safenetinc.luna.provider.LunaProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

在 V5.2.6.2 之后的版本中使用下列示例以支持现有密钥或证书。

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.safenetinc.luna.provider.LunaProvider
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

使用 IBM PKCS11IMPLKS（V5.2.6.2 或更高版本）配置 HSM

使用 IBM PKCS11IMPLKS 实施（V5.2.6.2 或较新版本）配置 HSM

关于此任务

在 V5.2.6.2 之后的版本中，对于 HSM 设备，系统支持 IBM PKCS11 实施。HSM 实施 Java JCE API。此接口访问该设备中的密钥。

过程

1. 添加用于支持 PKCS11IMPLKS/IBMPKCS11Impl 的新属性文件 **hsm.properties.in**。

   下表列出了专门用于配置 HSM 的属性。

属性	描述
HSM_KEYSTORE_TYPE	如果 HSM_ENABLED 设置为 *true*，那么属性值必须是 *IBMPKCS11IMPLKS*。
HSM_KEYSTORE_PROVIDER	如果 HSM_ENABLED 设置为 *true*，那么属性值必须是 *IBMPKCS11Impl*。
HSM_KEYSTORE_FILE	<应保留空白>

属性	描述
HSM_ADAPTER_TYPE	ncipher 或 safeNetFor ncipher，在创建、更新密钥或证书时，会运行下列命令 - 对于 UNIX：export CKNFAST_OVERRIDE_SECURITY_ASSURANCES= "longterm;tokenkeys" 对于 Windows：set CKNFAST_OVERRIDE_SECURITY_ASSURANCES ="longterm;tokenkeys"
HSM_ENABLED	此属性必须设置为 *true* 以支持 HSM。
HSM_PRNG_ALGORITHM	如果 HSM_ENABLED 设置为 *true*，那么属性值必须是 *PKCS11DeviceRNG*。
HSM_CONFIG_FILE_LOCATION	如果 HSM_ENABLED 设置为 *true*，那么属性值必须设置为 IBMPKCS11 配置文件的位置

2. 根据 HSM 类型更新或创建 HSM 设置所需的配置文件。

   关于 HSM 类型，可按下面所示方法找到配置文件，或联系 IBM 支持人员获取配置文件。如果有需要，您可以更新任何缺省设置。如果您的位置与缺省位置不同，那么必须编辑 *library* 值。

```
For SafeNet Luna Device:

lunasa_5_0_jsse.cfgname = B2Bi
library=/usr/safenet/lunaclient/lib/libCryptoki2_64.so
description=Luna SA 5.0 IBM SSP config - JSSE

publickeyimportonly=false
slotListIndex = 0
disabledMechanisms = {
   CKM_MD5
   CKM_SHA_1
   CKM_MD5_HMAC
   CKM_SHA_1_HMAC
   CKM_DES_CBC
   CKM_DES_CBC_PAD
   CKM_DES_ECB
   CKM_DES3_CBC
   CKM_DES3_ECB
   CKM_DES3_CBC_PAD
   CKM_AES_CBC
   CKM_AES_ECB
   CKM_AES_CBC_PAD
   CKM_RC4
   CKM_SSL3_MASTER_KEY_DERIVE
   CKM_SSL3_KEY_AND_MAC_DERIVE
   CKM_SSL3_PRE_MASTER_KEY_GEN
   CKM_TLS_PRE_MASTER_KEY_GEN
   CKM_TLS_MASTER_KEY_DERIVE
   CKM_TLS_KEY_AND_MAC_DERIVE
   CKM_TLS_MASTER_KEY_DERIVE_DH
   CKM_TLS_PRF
   CKM_SHA256_HMAC
   CKM_SHA384_HMAC
   CKM_SHA512_HMAC
   CKM_EC_KEY_PAIR_GEN
```

```
   CKM_ECDSA_KEY_PAIR_GEN
   CKM_ECDH1_DERIVE
   CKM_ECDH1_COFACTOR_DERIVE
   CKM_ECMQV_DERIVE
   CKM_DH_PKCS_KEY_PAIR_GEN
   CKM_DH_PKCS_PARAMETER_GEN
   CKM_DH_PKCS_DERIVE
}
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN = true
CKA_DECRYPT = true
CKA_DERIVE=true}
attributes (*, CKO_PUBLIC_KEY, *) = {
CKA_VERIFY = true
CKA_ENCRYPT = true
CKA_DERIVE = true}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT = true
CKA_DECRYPT = true
CKA_SIGN = true
CKA_VERIFY = true}
```

For nCipher Device:

```
======= ncipher_gen2.cfg.jsse
#nCipher nShield, nForce - Generation 2 cards
name =B2Bi
library=/opt/nfast/toolkits/pkcs11/libcknfast.so
description= IBM SSP NCIPHER HSM ADAPTER config for JSSE

slotListIndex =  1
disabledMechanisms = {
   CKM_MD5
   CKM_SHA_1
   CKM_MD5_HMAC
   CKM_SHA_1_HMAC
   CKM_SHA256_HMAC
   CKM_SHA384_HMAC
   CKM_SHA512_HMAC
   CKM_EC_KEY_PAIR_GEN
   CKM_ECDSA_KEY_PAIR_GEN
   CKM_ECDSA
   CKM_ECDSA_SHA1
   CKM_ECDH1_DERIVE
   CKM_ECDH1_COFACTOR_DERIVE
   CKM_ECMQV_DERIVE
}
attributes(*, CKO_SECRET_KEY, *) = {
   CKA_ENCRYPT=true
   CKA_DECRYPT=true}
attributes (*, CKO_PRIVATE_KEY, *) = {
   CKA_TOKEN=false
   CKA_SIGN=true
   CKA_SENSITIVE=false}
attributes(GENERATE, CKO_PRIVATE_KEY, CKK_RSA) = {
   CKA_DECRYPT=true
   CKA_UNWRAP=true
   CKA_EXTRACTABLE=true}
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
   CKA_TOKEN=false
   CKA_VERIFY=true}
attributes(*, CKO_PUBLIC_KEY, CKK_RSA) = {
   CKA_ENCRYPT=true
   CKA_WRAP=true
   CKA_VERIFY=true}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
```

```
CKA_EXTRACTABLE=true
CKA_DECRYPT=true
CKA_UNWRAP=true
CKA_DERIVE=true}
```

注：SafeNet Luna 不允许导入任何外部创建的专用密钥。必须在 HSM 设备上创建并存储。

声明

本信息是为在美国国内供应的产品和服务而编写的。本资料的其他语言版本可以从 IBM 获取。然而，您可能需要拥有产品或产品版本的该语言副本才能进行访问。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户任何使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

有关双字节字符集（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION"按现状"提供本出版物，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关非侵权、适销和适用于某特定用途的保证。某些管辖区域在某些事务中不允许免除明示或默示的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而不必对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许对已经交换的信息进行相互使用，请与下列地址联系：

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本文档中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

性能数据和客户示例引用仅供说明之用。根据具体配置和操作条件，实际性能结果可能有所不同。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可能会有差异。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

本信息包含在日常业务运营中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若实际人员或商业企业的名称与此雷同，纯属巧合。

版权许可：

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。这些实例程序"按现状"提供，不附有任何种类的保证。对于因使用样本程序所引起的任何损害，IBM 概不负责。

凡这些样本程序的每份拷贝或其他任何部分或任何演绎作品，都必须包括下一列显示的版权声明。

© 2015.
此部分代码是根据 IBM Corp. 公司的样本程序衍生出来的。
© Copyright IBM Corp. 2015.

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上"版权和商标信息"部分获得。

Adobe、Adobe 徽标、PostScript 和 PostScript 徽标是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

IT Infrastructure Library 是英国中央计算机与电信局（现在隶属于英国政府商务部）的注册商标。

Intel、Intel 徽标、Intel Inside、Intel Inside 徽标、Intel Centrino、Intel Centrino 徽标、Celeron、Intel Xeon、Intel SpeedStep、Itanium 和 Pentium 是 Intel Corporation 或其附属公司在美国和其他国家或地区的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

ITIL 是一个注册商标，是英国政府商务部注册的共同体商标，并且已在美国专利与商标局进行注册。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java™ 和所有基于 Java 的商标和徽标是 Oracle 和/或其附属公司的商标或注册商标。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美国和/或其他国家或地区的商标，并且根据许可使用。

Linear Tape-Open、LTO、LTO 徽标、Ultrium 和 Ultrium 徽标是 HP、IBM Corp. 和 Quantum 在美国和其他国家或地区的商标。

Connect Control Center®、Connect:Direct®、Connect:Enterprise®、Gentran®、Gentran®:Basic®、Gentran:Control®、Gentran:Director®、Gentran:Plus®、Gentran:Realtime®、Gentran:Server®、Gentran:Viewpoint®、Sterling Commerce™、Sterling Information Broker® 和 Sterling Integrator® 是 Sterling Commerce®, Inc.（一家 IBM 子公司）的商标或注册商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

产品文档相关条款和条件

此类出版物使用许可的授予受以下条件和条款的约束。

适用范围

这些条款和条件是对 IBM Web 站点上一切使用条款的补充。

个人用途：

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 明确许可，不能分发或展示这些出版物或其中任何部分，也不能制作其衍生产品。

商业用途

您仅可在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 明确许可，您不得在企业范围以外制作这些出版物的衍生产品，或者复制、分发或显示这些出版物或其中任何部分。

权限

除非此许可权中另有明确授权，否则不会将任何其他许可权、许可证或权利授予（无论是明示的还是默示的）这些出版物或其中包含的任何信息、数据、软件或其他知识产权。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，IBM 将有权撤销本文授予的许可权。

除非完全遵守所有适用的法律法规（其中包括美国的所有出口法律法规），否则不得下载、出口或者再出口本资料。

IBM 对这些出版物的内容不作任何保证。本出版物以"按现状"的基础提供，不附有任何形式的（无论是明示的，还是默示的）保证，包括但不限于默示的有关适销性、非侵权以及适用于某特定用途的保证。

程序号：

Printed in China