Sterling B2B Integrator

安全（5.2.3 版或更新版本）

版本 *5.2.3*

Sterling B2B Integrator

安全（5.2.3 版或更新版本）

版本 *5.2.3*

附註

在使用本資訊及其支援的產品之前，請先閱讀第 125 頁的『注意事項』中的資訊。

目錄

安全（5.2.3 版或更新版本）

Sterling B2B Integrator 使用各種安全機制，包括用於管理功能的系統密碼、以公司的安全原則為基礎的密碼原則，以及角色型安全，以便對組織內的不同使用者提供不同層次的存取權。

下列安全特性隨 Sterling B2B Integrator 提供：

- 角色型安全可根據與使用者帳戶相關聯的許可權，將檔案、商業程序、Web 範本、服務及產品特性的存取權，提供給使用者。
- 密碼原則是安全決策集，讓您可以根據公司的安全原則，製作與套用不同的使用者帳戶。這些選擇包括下列項目：密碼的有效天數、密碼的上限長度與下限長度。
- 可使用 LDAP 鑑別將外部使用者帳戶的鑑別委派給 LDAP 目錄，並使用公司內用於其他應用程式的相同安全資訊提供鑑別。如果公司已採用 LDAP，您可以使用現有 LDAP 目錄搭配應用程式。
- 系統安裝通行詞組 - 安裝期間，您為您的 Sterling B2B Integrator 安裝建立系統通行詞組。通行詞組是長度超過 16 個字元的高度複雜字串。啟動系統及存取受保護的系統資訊時，需要系統通行詞組。
- 支援 x.509 憑證加密、簽章和傳輸層安全。
- 美國聯邦資訊處理標準 (FIPS) 140-2 認證軟體模組，支援 nCipher 和 Safenet 的 FIPS 140-2 認證硬體。
- 啟用 Secure Socket Layer (SSL) 和傳輸層安全 (TLS)。

還可以設定下列安全特性：

- 安全逾時特性提供您設定使用者階段作業逾時的能力。
- 「自訂密碼原則」特性容許您新增其他密碼原則規則。這些附加的密碼規則可協助您避免使用強度弱且容易被駭的密碼，同時拒絕不符合規定的密碼。
- 單一登入 (SSO) 特性是一種鑑別處理程序，可讓使用者只需輸入一個使用者名稱和密碼，即可存取數個應用程式。
- 「文件加密」特性容許其他層的安全配置超越傳統檔案和資料庫權限。

角色型安全

角色型安全概觀

角色型安全可根據與使用者帳戶相關聯的許可權，將特定檔案、商業程序、Web 範本、服務及產品特性的存取權，提供給使用者。

您必須瞭解群組、許可權和使用者帳戶如何協同作業，方能瞭解如何管理角色型安全。

- 許可權提供使用者介面頁面和頁面所提供的功能之存取。
- 群組是許可權的集合。
- 會將使用者帳戶指派給許可權和密碼原則。

管理角色型安全包括下列作業：

- 建立許可權
- 建立群組
- 建立密碼原則
- 建立使用者帳戶

群組

群組是許可權的集合。群組可以從單一位置維護數個使用者的存取權。群組有助於將維護帳戶所涉及的工作量降到最低，尤其是在數個使用者執行相同工作功能時更是如此。

您可以針對每一個工作功能而非每一個使用者來建立群組，以將許多許可權關聯於不同的使用者。您也可以將某個群組指派為另一個群組的子群組。

例如，採購部門有五個全都執行相同工作的採購專員。您可以建立採購群組並且維護該群組中所有採購專員的存取權，而不需要將許可權套用到每個個別採購專員的使用者帳戶。在採購群組內，您可以指派子群組，根據專員處理的採購類型來進一步修正存取權。您可以將名為辦公用品、機器、一般設備或車輛的子群組指派給採購群組，以修正存取權。

如果要在套用升級或修補程式時避免改寫，請勿修改系統預先配置的群組。

群組作業包括：

- 建立群組
- 搜尋群組
- 編輯群組
- 刪除群組

預先配置群組

如果要指派許可權給使用者，您可以指派預先配置群組。使用者會繼承與群組相關聯的所有許可權。針對使用者帳戶定義「協助工具」和「佈景主題」時，可將預先定義群組指派給使用者。

您必須具有「帳戶」模組的許可權，才可建立群組。

群組命名慣例

群組命名有一系列的慣例。

使用下列群組命名慣例：

- 群組 ID 必須不同。
- 名稱要區分大小寫。
- 大小寫不同的兩個群組名稱視為不同的名稱。
- 如果群組名稱已使用，則無法作為新群組的名稱。畫面會顯示一則錯誤訊息。

搜尋群組

您可以從**管理**功能表搜尋群組。

關於這項作業

如果要搜尋群組：

程序

1. 從**管理功能表**中，選取**帳戶** > **群組**。
2. 完成下列其中一項動作：
   - 在「搜尋」之下，輸入要搜尋的部分**群組名稱**或完整**群組名稱**，然後按一下**執行！**「群組」頁面會列出符合搜尋準則的所有群組。
   - 在**依英文字母順序**欄位的「列出」之下，選取「全部」或要搜尋的群組的名稱的第一個字母，然後按一下**執行！**「群組」頁面會列出符合搜尋準則的所有群組。

建立群組

您可以從**管理**功能表建立群組。

關於這項作業

在您開始之前，您必須知道：

- 建立中群組的「群組 ID」。
- 建立中群組的群組名稱。
- 群組的擁有者名稱。
- 與群組相關聯的交易夥伴身分。一個交易夥伴僅能與一個群組相關聯，但一個使用者帳戶可以與許多群組相關聯。這樣可讓使用者帳戶與一個以上的交易夥伴相關聯。「身分」欄位用於遞送「信箱」中的訊息。

如果要建立群組，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **群組**。
2. 按一下**建立新群組**旁的**執行！**
3. 在「新群組」頁面中，輸入**群組 ID**。
4. 輸入**群組名稱**。
5. 輸入**擁有者**。
6. 選取**身分**。
7. 按**下一步**。
8. 在「指派子群組」頁面中，如果您想要依名稱過濾群組，請在**依名稱**欄位中的「過濾資料」下，就您想要過濾的群組輸入其部分或完整名稱，然後按一下過濾按鈕。
9. 選取您想要指派給此群組的群組。將群組從「可用」窗格移至「已指派」窗格。
10. 按**下一步**。
11. 您要在「指派權限」頁面中過濾許可權嗎？
    - 如果您想要依名稱過濾，請在**依名稱**欄位中的「過濾資料」下，就您想要過濾的許可權輸入其部分或完整名稱，然後按一下**依類型**欄位右側的過濾按鈕。

- 如果要依類型過濾，請在「過濾資料」下，從「依類型」清單選取您要過濾的許可權類型，然後按一下**依類型**欄位右側的過濾按鈕。

12. 選取您要指派給此群組的許可權。將許可權從「可用」窗格移至「已指派」窗格。 依預設，與指派給此群組之子群組相關聯的許可權已選取。在可用的直欄中不會顯示相關聯的許可權；不過它們會顯示在確認頁面中。
13. 按**下一步**。
14. 檢閱群組資訊。
15. 按一下**完成**。

編輯群組

您可以編輯群組來更新設定、子群組及許可權。

關於這項作業

在編輯群組時，您可以更新下列項目：

- 設定
- 子群組
- 許可權

您無法變更「群組 ID」。如果需要變更「群組 ID」，您必須建立新群組。

如果要編輯群組，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **群組**。
2. 使用「群組名稱搜尋」或「按字母順序排列的清單」來搜尋您要編輯的群組，然後按一下**執行！**
3. 針對您要更新的群組，選取**編輯**。
4. 更新任何群組設定，然後按**下一步**。
5. 更新任何已指派的子群組，然後按**下一步**。
6. 更新任何已指派的許可權，然後按**下一步**。
7. 按**下一步**。
8. 檢閱群組資訊。
9. 按一下**完成**。

刪除群組

您可以從**管理**功能表刪除群組。

關於這項作業

您無法移除 Sterling B2B Integrator 管理群組或管理者使用者的「UI 帳戶」許可權。這些可讓系統管理者進行系統管理。

如果要刪除群組，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **群組**。
2. 在「群組」頁面中，使用「搜尋」或「列出」選項，尋找您要刪除的群組。
3. 在「群組」頁面中，按一下所要刪除群組旁的**刪除**。

系統隨即刪除群組並顯示訊息：
已順利完成系統更新。

檢閱群組名稱和 ID

您可以從**管理**功能表檢閱群組名稱和 ID。

關於這項作業

如果要檢閱群組名稱和 ID：

程序

1. 從**管理功能表**中，選取**帳戶** > **群組**。
2. 在「群組」頁面中，使用「搜尋」或「列出」選項尋找您要檢閱的群組。
3. 選取群組。 隨即顯示群組名稱和 ID。

許可權

許可權可供存取 Sterling B2B Integrator 內不同的模組，且它們是角色型安全的基礎。使用者的許可權包含群組許可權以及個別指派的任何許可權。

請利用許可權來執行下列動作：

- 從單一位置管理數個使用者的存取權。
- 以最小的工作量管理使用者帳戶，尤其是針對執行相同工作功能的多個使用者。

許可權作業包括：

- 建立許可權
- 搜尋許可權
- 編輯許可權名稱
- 刪除許可權

在建立、編輯或刪除許可權之前，請決定該群組中使用者需要或不需要存取的模組，以執行其指派的功能。您必須獲指派「帳戶」模組的許可權，才能建立許可權。

如果要在套用升級或修補程式時避免改寫，請勿修改系統預先配置的許可權。當需要自訂許可權分組時，請建立新群組。

許可權命名慣例

許可權名稱區分大小寫，而且不能重複。

許可權命名慣例包括：

- 名稱區分大小寫，且大小寫不同的兩個名稱分別視為唯一的名稱。例如，"Any document" 和 "Any Document" 是兩個不同的許可權名稱。

- 如果某個名稱已用於現有許可權，則該名稱無法作為新許可權的名稱。畫面會顯示一則錯誤訊息。

雖然可以用相同的名稱但不同大小寫來表示兩個許可權，但不建議這麼做。

繼承自群組的許可權

這些是預先安裝的群組，而當許可權群組指派給使用者帳戶時，就會繼承許可權。當群組指派為子群組時，會繼承相同的許可權。

每一個群組都包含功能表項目的許可權，以及用來授與頁面存取權的對應使用者介面 (UI) 許可權。例如，EBXML 包含 UI EBXML。

群組名稱	群組 ID	繼承自群組的許可權
ACCOUNTS	ACCOUNTS	PasswordPolicy、Permissions、UI Accounts、UserNews
ADAPTER_UTILITIES	ADAPTER_UTILITIES	BEATuxedo、CDNetmaps、CDNetmapXref、CDNodes、SAPRoutes、SAPRouteXREF、SAPSuiteBuilder、UI Adapter Utilities
ADVANCED_SETUP	ADVANCED_SETUP	DeliveryChannels、DocumentExchange、Identities、Packaging、Profiles、Transports、UI Advanced Trading Profile Setup
AS2 Edition	as2admin	來自 BPMONITOR 子群組的所有許可權，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、UI trading Parners
異常事件通知	eventAbnormal	無
帳戶	acctadmin	來自 ACCOUNTS 子群組的所有許可權，以及 UI Groups、UI User Accounts。
警示通知	notifications	無
BPMONITOR	BPMONITOR	BPSSCorrelation、BusinessProcesses、CentralSearch、CommunicationSessions、Correlation、CurrentActivities、CurrentDocuments、CurrentProcesses、DataFlows、Documents、EBXMLCorrelation、EDICorrelation、EDIINT、GentranServerforUnix、Message Entry Workstation Home、SWIFTNETCorrelation、UI BP Monitor、RosettaNet
商業程序	bpadmin	來自 BPMONITOR 和 SERVICES 子群組的所有許可權，以及 UI BP Manager、UI Business Process、UI Delete BP。
CD 伺服器 Proxy 管理者	cdsp_admin	來自 ACCOUNTS、BPMONITOR、CD 伺服器 Proxy 使用者、OPERATIONS 和 SERVICES 子群組的所有許可權，以及 UI Groups、UI Licenses、UI Password Policy、UI SQL Tool、UI User Accounts。
CD 伺服器 Proxy 使用者	cdsp_user	依預設，當使用 CDSP Accessibility 建立使用者帳戶時，會指派此群組。 來自 ACCOUNTS、BPMONITOR、OPERATIONS 及 SERVICES 子群組的所有許可權，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、UI Trusted Certs。

群組名稱	群組 ID	繼承自群組的許可權
指令行使用者	commandlineuser	eInvoicing、eInvoicing ALL BUYERS、eInvoicing ALL SUPPLIERS、eInvoicing Archive、eInvoicing Configuration、eInvoicing CREATE/EDIT AGREEMENT、eInvoicing DELETE AGREEMENT、VIEW AGREEMENT
DEPLOYMENT	DEPLOYMENT	UI Deployment、Resource Tags
儀表板使用者	dashboardUsers	依預設，當使用「儀表板使用者介面協助工具」及下列任何儀表板佈景主題建立使用者帳戶時，會指派此群組： • AFT • 預設值 • Community Management Operator、Participant、Participant Sponsor 或 Sponsor 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、Web View Plus Portlet
部署	deploymentadmin	來自 ADAPTER_UTILITIES、DEPLOYMENT、EBXML、MAILBOX、MAPS、SERVICES、WEB_EXTENSIONS 及 WEB_SERVICES 子群組的所有許可權，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、UI XSLT
EBICS 管理者	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、UI EBICS Subscriber Key Validation

群組名稱	群組 ID	繼承自群組的許可權
EBICS 操作員	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、UI EBICS User Profile Configuration
EBXML	EBXML	BPSS、BPSSExtension、CPA、UI EBXML
ENVELOPES	ENVELOPES	ControlNumberHistory、ControlNumbers、EDISequenceCheckQueue、Envelopes、TransactionRegister、UI Envelopes
異常事件通知	eventExceptional	無
MAILBOX	MAILBOX	Configuration、Messages、Routing Rules、UI Mailbox、VirtualRoots
MAPS	MAPS	ExtendedRuleLibraries、Maps、Standards、UI Maps
Mailbox Administrators	mboxadmins	來自 MAILBOX 和「信箱瀏覽器介面使用者」群組的所有許可權，以及 DeadLetter Mailbox、Mailbox Global Delete、Mailbox Global Query、EBICS_DEADLETTER Mailbox
信箱瀏覽器介面使用者	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、MBISearch JSP
OPERATIONS	OPERATIONS	JDBCMonitor、MessageMonitor、Perfdumps、SequenceManager、Statistics、ThreadMonitor、Troubleshooter、Tuning、UI Federated Systems、UI Operations
供應交易夥伴	provisionalpartners	無
SERVICES	SERVICES	Configuration、Installation/Setup、UI Services
SSH	SSH	AuthorizedUserKey、KnownHostKey、RemoteProfiles、UI SSH、UserIdentityKey
階段作業示範 Web 套組買家	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、WebSuite Session Demo Query List Template

群組名稱	群組 ID	繼承自群組的許可權
階段作業示範 Web 套組供應商	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 Session Demo PO Send Business Process、WebSuite Session Demo PO View Template、WebSuite Session Demo Query List Template
Sterling B2B Integrator Admin	super	來自 ACCOUNTS、ADAPTER_UTILITIES、ADVANCED_SETUP、BPMONITOR、DEPLOYMENT、EBXML、ENVELOPES、MAILBOX、MAPS、Mailbox Administrators、OPERATIONS、SERVICES、SSH、WEB_EXTENSIONS 和 WEB_SERVICES 子群組的所有許可權，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 和 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、UI XSLT
系統作業	operator	來自 OPERATIONS 子群組的所有許可權，以及 UI Archive、UI Licenses、UI Lock Manager、UI Logs、UI Notify、UI Perimeter Servers、UI Reports、UI Scheduler、UI SQL Tool、UI Support Case Tool

群組名稱	群組 ID	繼承自群組的許可權
交易設定檔	tpadmin	來自 ADVANCED_SETUP、ENVELOPES 和 SSH 子群組的所有許可權，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、UI Trusted Certs
WEB_EXTENSIONS	WEB_EXTENSIONS	Utilities、WebResources、WebTemplates
WEB_SERVICES	WEB_SERVICES	SchemaMappings、SecurityToken、UI Web Services、WebServicesManager、WSDLCheckin
Web 套組買家	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、WebSuite Self Registration Business Process
Web 套組員工	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、WebSuite TS Send Business Process
Web 套組財務	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、WebSuite Self Registration Business Process

群組名稱	群組 ID	繼承自群組的許可權
Web 套組人力資源	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、WebSuite TimeSheet View Template
Web 套組經理	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、WebSuite TS Send Business Process
Web 套組採購者	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、WebSuite Self Registration Business Process
Web 套組供應商	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、WebSuite Self Registration Business Process

存取使用者介面資源所需的許可權

這是存取功能表項目及其關聯頁面和功能所需的基本許可權集合。指派基本許可權集亦可提供部分附加功能讓使用者使用。如果您沒有功能表項目及其關聯功能的許可權，則不會顯示。

從管理功能表 > 商業程序、使用者介面資源	許可權名稱 / 許可權 ID
商業程序 > 管理程式	使用者介面 BP 管理程式 (BPMANAGE) 加使用者介面商業程序 (BUSINESS_PROCESS)
商業程序 > 監視 > 進階搜尋 > 商業程序	BusinessProcesses (PLTADM2) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > SWIFTNET 相關性	SWIFTNETCorrelation (GISADM9) 加使用者介面 BP 監視 (BPMONITOR) 和使用者介面 SWIFTNet 遞送規則 (SWIFTNET_ROUTING_RULE)
商業程序 > 監視 > 進階搜尋 > 資料流程	DataFlows (GISADM1) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > 文件	文件 (GISADM2) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > 通訊階段作業	通訊階段作業 (GISADM3) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > 相關性	相關性 (GISADM4) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > BPSS 相關性	BPSSCorrelations (GISADM5) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > EBXML 相關性	EBXMLCorrelation (GISADM6) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > EDI 相關性	EDICorrelation (GISADM7) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 進階搜尋 > EDIINT	EDIINT (STDSADM6) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 集中搜尋	CentralSearch (GISADM10) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 現行處理程序	CurrentProcesses (PLTADM3) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 現行文件	CurrentDocuments (GISADM11) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 監視 > 現行活動	CurrentActivities (PLTADM4) 加使用者介面 BP 監視 (BPMONITOR)
商業程序 > 訊息登錄工作站	訊息登錄工作站首頁 (MESSAGE_ENTRY_HOME)

從管理功能表 > 交易夥伴、使用者介面資源	許可權名稱 / 許可權 ID
交易夥伴 > 設定 > 基本	使用者介面基本交易設定檔設定 (BASIC_SETUP)

從管理功能表 > 交易夥伴、使用者介面資源	許可權名稱 / 許可權 ID
交易夥伴 > 設定 > 進階 > 身分	身分 (GISADM12) 加使用者介面進階交易設定檔設定 (ADVANCED_SETUP) 刪除還需要使用者介面刪除交易夥伴許可權 (TP_DELETE)
交易夥伴 > 設定 > 進階 > 傳輸	傳輸 (GISADM13) 加使用者介面進階交易設定檔設定 (ADVANCED_SETUP) 刪除還需要使用者介面刪除交易夥伴許可權 (TP_DELETE)
交易夥伴 > 設定 > 進階 > 文件交換	DocumentExchange (GISADM14) 加使用者介面進階交易設定檔設定 (ADVANCED_SETUP) 刪除還需要使用者介面刪除交易夥伴許可權 (TP_DELETE)
交易夥伴 > 設定 > 進階 > 遞送通道	DeliveryChannels (GISADM15) 加使用者介面進階交易設定檔設定 (ADVANCED_SETUP) 刪除還需要使用者介面刪除交易夥伴許可權 (TP_DELETE)
交易夥伴 > 設定 > 進階 > 包裝	包裝 (GISADM16) 加使用者介面進階交易設定檔設定 (ADVANCED_SETUP) 刪除還需要使用者介面刪除交易夥伴許可權 (TP_DELETE)
交易夥伴 > 設定 > 進階 > 設定檔	設定檔 (GISADM17) 加使用者介面進階交易設定檔設定 (ADVANCED_SETUP) 刪除還需要使用者介面刪除交易夥伴許可權 (TP_DELETE)
交易夥伴 > 數位憑證 > CA	使用者介面 CA 憑證 (CA_CERTS) 加使用者介面系統憑證 (SYSTEM_CERTS) 使用者介面 系統憑證新增「系統」選項。
交易夥伴 > 數位憑證 > 授信	使用者介面授信憑證 (TRUSTED_CERTS)
交易夥伴 > 數位憑證 > 系統	使用者介面系統憑證 (SYSTEM_CERTS)
交易夥伴 > 文件封套 > 封套	封套 (STDSADM1) 加使用者介面封套 (ENVELOPE)
交易夥伴 > 文件封套 > 控制號碼	ControlNumbers (STDSADM2) 加使用者介面封套 (ENVELOPE)
交易夥伴 > 文件封套 > 交易暫存器	TransactionRegister (STDSADM3) 加使用者介面封套 (ENVELOPE)
交易夥伴 > 文件封套 > 控制號碼歷程	ControlNumberHistory (STDSADM4) 加使用者介面封套 (ENVELOPE)
交易夥伴 > 文件封套 > EDI 順序檢查佇列	EDISequenceCheckQueue (STDSADM5) 加使用者介面封套 (ENVELOPE)
交易夥伴 > 合約	使用者介面合約 (CONTRACTS) 加使用者介面進階交易夥伴設定 (ADVANCED_SETUP)

從管理功能表 > 交易夥伴、使用者介面資源	許可權名稱 / 許可權 ID
交易夥伴 > 代碼清單	使用者介面 CodeLists (CODELISTS)
交易夥伴 > AS2	使用者介面 AS2 交易設定檔設定 (AS2_SETUP)
交易夥伴 > SSH > 遠端設定檔	RemoteProfiles (ASSETADM1) 加使用者介面 SSH
交易夥伴 > SSH > 已知的主機金鑰	KnownHostKey (ASSETADM2) 加使用者介面 SSH
交易夥伴 > SSH > 使用者身分金鑰	UserIdentityKey (ASSETADM3) 加使用者介面 SSH
交易夥伴 > SSH > 授權使用者金鑰	AuthorizedUserKey (ASSETADM4) 加使用者介面 SSH
交易夥伴 > AS3	使用者介面 AS3 交易設定檔設定 (AS3_SETUP)
交易夥伴 > Odette FTP 夥伴設定檔 > 實體友機	OftpPhysicalPartner (ASSETOFTP1) 加使用者介面配接器公用程式 (ADAPTER_UTILITIES)
交易夥伴 > Odette FTP 夥伴設定檔 > 實體友機合約	OftpPhysicalPartnerContract (ASSETOFTP3) 加使用者介面配接器公用程式 (ADAPTER_UTILITIES)
交易夥伴 > Odette FTP 夥伴設定檔 > 邏輯友機	OftpLogicalPartner (ASSETOFTP2) 加使用者介面公用程式 (ADAPTER_UTILITIES)
交易夥伴 > Odette FTP 夥伴設定檔 > 邏輯友機合約	OftpLogicalPartnerContract (ASSETOFTP4)
交易夥伴 > PGP > 伺服器管理程式	PGP 伺服器管理程式 (ASSETADM55) 加使用者介面 PGP 設定檔管理程式 (PGP)
交易夥伴 > PGP > 贊助者管理程式	PGP 贊助者管理程式 (ASSETADM56) 加使用者介面 PGP 設定檔管理程式 (PGP)
交易夥伴 > PGP > 友機管理程式	PGP 友機管理程式 (ASSETADM57) 加使用者介面設定檔管理程式 (PGP)

從管理功能表 > 部署、使用者介面資源	許可權名稱 / 許可權 ID
部署 > 服務 > 安裝/設定	安裝/設定 (PLTADM9) 加使用者介面服務 (SERVICES)
部署 > 服務 > 配置	配置 (PLTADM10) 加使用者介面服務 (SERVICES)、使用者介面 BP 管理程式 (BPMANAGE)。從 5.2.4.3 版和更新版本起，亦需要使用者介面配接器 StartStop。
部署 > 排程	使用者介面排程器 (SCHEDULER)
部署 > 對映	對映 (ASSETADM5) 加 UI_Maps
部署 > 標準	標準 (STDSADM7) 加 UI_Maps
部署 > 延伸規則程式庫	ExtendedRuleLibraries (ASSETADM6) 加 UI_Maps

從管理功能表 > 部署、使用者介面資源	許可權名稱 / 許可權 ID
部署 > XSLT	使用者介面 XSLT (XSLT)
部署 > Web 延伸 > Web 資源	WebResources (GISADM19) 加使用者介面 Web 延伸和使用者介面 Web 服務 (WEB_SERVICES) 使用者介面 Web 服務容許使用者移入新的 Web 資源檔案
部署 > Web 延伸 > 公用程式	公用程式 (GISADM20) 加使用者介面 Web 延伸 只有從舊版升級時才會看到。
部署 > 綱目	使用者介面綱目 (SCHEMAS)
部署 > 信箱 > 配置	配置 (MBXADM1) 加使用者介面信箱 (MAILBOX)
部署 > 信箱 > 虛擬根目錄	VirtualRoots (MBXADM2) 加使用者介面信箱 (MAILBOX)
部署 > 信箱 > 遞送規則	RoutingRules (MBXADM3) 加使用者介面信箱 (MAILBOX)
部署 > 信箱 > 訊息	訊息 (MBXADM4) 加使用者介面信箱 (MAILBOX)
部署 > EBXML > BPSS	BPSS (ASSETADM7) 加使用者介面 EBXML (EBXML)
部署 > EBXML > BPSS 延伸	BPSSExtension (ASSETADM8) 加使用者介面 EBXML (EBXML)
部署 > EBXML > CPA	CPA (ASSETADM9) 加使用者介面 EBXM (EBXML)
部署 > 資源管理程式 > 資源標籤	資源標籤 (PLTADM1) 加使用者介面部署 (DEPLOYMENT)
部署 > 資源管理程式 > 匯入/匯出	使用者介面匯入/匯出 (IMPORT_EXPORT)
部署 > 配接器公用程式 > SAP 套組建置器	SAPSuiteBuilder (ASSETADM10) 加使用者介面配接器公用程式
部署 > 配接器公用程式 > Sap 遞送 > Sap 遞送	SAPRoutes (ASSETADM11) 加使用者介面配接器公用程式
部署 > 配接器公用程式 > Sap 遞送 > SapRouteXRef	SAPRouteXREF (ASSETADM12) 加使用者介面配接器公用程式
部署 > 配接器公用程式 > BEATuxedo	BEATuxedo (ASSETADM13) 加使用者介面配接器公用程式 除非已安裝 BEATuxedo jar，否則不顯示功能表項目。
部署 > 配接器公用程式 > SWIFTNET 遞送規則	使用者介面 SWIFTNet 遞送規則 (SWIFTNET_ROUTING_RULE)
部署 > 配接器公用程式 > SWIFTNET 服務設定檔	使用者介面 SWIFTNet 服務設定檔 (SWIFTNET_SVC_PROFILE)
部署 > 配接器公用程式 > SWIFTNET 副本服務設定檔	使用者介面 SWIFTNet 副本服務設定檔 (SWIFTNET_COPY_PROFILE)

從管理功能表 > 部署、使用者介面資源	許可權名稱 / 許可權 ID
部署 > 配接器公用程式 > 鎖定原則管理程式	LockoutPolicyManager (ASSETADM50)
部署 > 配接器公用程式 > C:D Netmaps > C:D 節點	CDNetmaps (ASSETADM51) 加使用者介面配接器公用程式 (ADAPTER_UTILITIES)
部署 > 配接器公用程式 > C:D Netmaps > C:D Netmaps	CDNodes (ASSETADM52) 加使用者介面配接器公用程式 (ADAPTER_UTILITIES)
部署 > 配接器公用程式 > C:D Netmaps > C:D Netmap X-REF	CDNetmapXref (ASSETADM53) 加使用者介面配接器公用程式 (ADAPTER_UTILITIES)
部署 > 配接器公用程式 > 原則配置	配接器設定檔 (ASSETADM54)
部署 > 配接器公用程式 > 檔案系統虛擬根目錄	檔案系統虛擬根目錄 (ASSETADM58)
部署 > SSH 主機身分金鑰	使用者介面 SSH 本端身分金鑰 (SSH_LCL_ID_KEY) 和使用者介面 SSH (SSH)
部署 > Web 服務 > 管理程式	WebServicesManager (ASSETADM16) 和使用者介面 Web 服務 (WEB_SERVICES)
部署 > Web 服務 > 綱目對映	SchemaMappings (ASSETADM17)、使用者介面 Web 服務 (WEB_SERVICES) 和使用者介面 EBXML (EBXML)
部署 > Web 服務 > WSDL 移入	WSDLCheckIn (ASSETADM18) 加使用者介面 Web 服務 (WEB_SERVICES)
部署 > Web 服務 > 安全記號	SecurityToken (ASSETADM18) 加使用者介面 Web 服務 (WEB_SERVICES)

從管理功能表 > e-Invoicing、使用者介面資源	許可權名稱 / 許可權 ID
e-Invoicing > 合約	eInvoicing 檢視合約 (EINV_VIEW_AGREEMENT) 刪除還需要 eInvoicing 刪除合約 (EINV_DELETE_AGREEMENT) 許可權。
e-Invoicing > 整合保存	eInvoicing 保存 (EINVOICING_ARCHIVE) 加 eInvoicing 檢視發票 (EINV_VIEW_INVOICE)
e-Invoicing > 配置	eInvoicing 配置 (EINVOICING_CONFIGURATION)

從管理功能表 > 作業、使用者介面資源	許可權名稱 / 許可權 ID
系統 > 疑難排解專家	疑難排解專家 (PLTADM17) 加使用者介面作業 (OPERATIONS)
系統 > 效能 > 調整	調整 (PLTADM18) 加使用者介面作業 (OPERATIONS)
系統 > 效能 > 統計資料	統計資料 (PLTADM19) 加使用者介面作業 (OPERATIONS)
系統 > 效能 > JVM 監視	Perfdumps (GISADMIN27) 加使用者介面作業 (OPERATIONS)
系統 > 支援工具 > SQL 管理程式	使用者介面 SQL 工具 (SQLMANAGER)
系統 > 支援工具 > 支援案例	使用者介面支援案例工具 (SUPPORT_CASE)

從管理功能表 > 作業、使用者介面資源	許可權名稱 / 許可權 ID
系統 > 日誌	使用者介面日誌 (SYSTEM_LOGS)
系統 > 軟體使用權	使用者介面軟體使用權 (LICENSES)
報告	使用者介面報告 (REPORTS)
執行緒監視器	ThreadMonitor (PLTADM24) 加使用者介面作業 (OPERATIONS)
JDBC 監視器	JDBCMonitor (PLTADM25) 加使用者介面作業 (OPERATIONS) 和使用者介面 SQL 工具 (SQLMANAGER)
保存管理程式	使用者介面保存 (ARCHIVE-UI) 加使用者介面作業 (OPERATIONS)、使用者介面 BP 管理 (BPMANAGE) 和使用者介面商業程序 (BUSINESS_PROCESS)
鎖定管理程式	使用者介面鎖定管理程式 (LOCK_MANAGER)
訊息監視器	MessageMonitor (GISADM24) 加使用者介面作業 (OPERATIONS)
周邊服務	使用者介面周邊服務 (PSERVERS)
Proxy 伺服器	使用者介面 Proxy 伺服器 (PROXYSERVERS) 加 Sterling B2B Integrator 管理群組

從管理功能表 > 帳戶、使用者介面資源	許可權名稱 / 許可權 ID
群組	使用者介面群組 (GROUPS) 加使用者介面帳戶 (ACCOUNTS)
許可權	許可權 (PLTADM27) 加使用者介面帳戶 (ACCOUNTS)
使用者帳戶	使用者介面使用者帳戶 (USER_ACCOUNTS) 加使用者介面帳戶 (ACCOUNTS)
密碼原則	PasswordPolicy (PLTADM29) 加使用者介面帳戶 (ACCOUNTS)
使用者新聞	UserNews (GISADM25) 加使用者介面帳戶 (ACCOUNTS)
我的帳戶	MyAccount (PLTADM30)

預先配置許可權

預先配置許可權隨系統提供。就像自訂許可權一般，會提供系統內不同模組的存取。

搜尋許可權名稱

您可以從**管理**功能表搜尋許可權。

關於這項作業

如果要搜尋許可權：

程序

1. 從**管理功能表**中，選取**帳戶 > 許可權**。
2. 在「許可權」頁面中，完成下列其中一項動作：

- 在**許可權名稱**欄位的「搜尋」之下，輸入要搜尋的部分許可權名稱或完整許可權名稱，然後按一下**執行！**「許可權」頁面會列出符合搜尋準則的所有許可權。
- 在**依英文字母順序**欄位的「列出」之下，選取**全部**或要搜尋的許可權的名稱的第一個字母，然後按一下**執行！**「許可權」頁面會列出符合搜尋準則的所有許可權。

建立權限

如果您的系統已從舊版升級，現有權限依預設會設定為「其他」。您可能必須編輯每一個權限，以套用新的權限類型。

關於這項作業

在您開始之前，您必須知道下列資訊：

欄位	說明
許可權 ID	正要建立的許可權其「許可權 ID」。「許可權 ID」是您為其設定許可權之商業程序、XSLT 文件、Web 範本或資源的名稱。在 ID 之後併入資源的延伸。必要。 許可權 ID： • 它們必須是唯一的。 • 它們有區分大小寫。 • 許可權 ID 必須符合商業程序、XSLT 文件、Web 範本或資源的名稱。如果許可權 ID 與資源名稱沒有完全符合，您將無法鎖定資源。
許可權名稱	您正要建立的許可權其名稱。必要。 許可權名稱必須是唯一的。許可權名稱區分大小寫，例如，"Any document" 和 "Any Document" 是兩個不同的許可權名稱。
許可權類型	正要建立的許可權其「許可權類型」。 必要。許可權類型包括： • UI - 容許存取介面中的特定功能表項目。 • 信箱 - 容許存取系統中的特定信箱。 • 範本 - 容許存取特定的 Web 範本。 • BP - 容許存取特定的商業程序。 • 追蹤 - 容許存取特定的文件追蹤選項。 • 社群 - 容許存取特定的社群管理選項。 • Web 服務 • 服務 • 電子發票 • 其他 - 容許存取前述任何一種類型識別不出的資源。

如果要建立許可權：

程序

1. 從**管理功能表**中，選取**帳戶** > **許可權**。
2. 按一下**建立新許可權**旁的**執行！**
3. 在「許可權」頁面中，輸入**許可權 ID**。

4. 輸入**許可權名稱**。
5. 選取**許可權類型**。
6. 按**下一步**。
7. 檢閱許可權設定。
8. 按一下**完成**。

編輯許可權名稱

如果需要變更許可權名稱以更貼切反映許可權，您可以編輯許可權名稱。許可權名稱必須是唯一的且區分大小寫。您無法變更許可權 ID。如果需要編輯許可權 ID，您必須建立新的許可權。

關於這項作業

如果要編輯許可權名稱，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **許可權**。
2. 使用「許可權名稱搜尋」或「按字母順序排列的清單」來搜尋您要編輯的許可權，然後按一下**執行！**
3. 在您要編輯的「許可權」旁邊，按一下**編輯**。
4. 輸入新的**許可權名稱**。
5. 視需要更新許可權類型，然後按**下一步**。
6. 檢閱許可權設定資訊。
7. 按一下**完成**。

刪除許可權

您可以刪除與使用者帳戶相關聯的許可權。刪除許可權時，所有使用者帳戶將無法再使用它。

關於這項作業

如果您要刪除的許可權是唯一與使用者帳戶相關聯的許可權，您必須編輯使用者帳戶以關聯其他許可權。如果您未關聯至少一個新許可權至使用者帳戶，則使用者可以登入，但無權存取任何功能表項目。

如果要刪除許可權，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **許可權**。
2. 使用「許可權名稱搜尋」或「按字母排序的清單」，搜尋您要刪除的許可權，然後按一下**執行！**
3. 在「許可權」頁面中，對您要刪除的許可權按一下**刪除**。
4. 驗證許可權資訊符合您要刪除的許可權，然後按一下**刪除**。

   系統隨即刪除許可權並顯示訊息：

   已順利完成系統更新。

檢閱群組名稱和 ID

您可以從**管理**功能表檢閱許可權名稱和 ID。

關於這項作業

如果要檢閱許可權名稱和 ID：

程序

1. 從**管理功能表**中，選取**帳戶 > 許可權**。
2. 使用「許可權名稱搜尋」或「依英文字母順序列出」，然後按**執行！**，搜尋您要檢閱的許可權。
3. 選取許可權。 隨即顯示許可權名稱和 ID。

使用者帳戶

使用者帳戶依群組、許可權和密碼原則定義，可協助提供安全環境。此類型的使用者帳戶定義是定義為角色型安全模型。

您必須先決定您企業環境所需要的群組、許可權和密碼原則，然後才建立任何新的使用者帳戶。指派群組、許可權和密碼原則是選用性的。

只有具備建立許可權的帳戶可新建使用者帳戶。使用者帳戶作業包括：

- 建立使用者帳戶
- 搜尋使用者帳戶
- 編輯使用者帳戶
- 刪除使用者帳戶

預設使用者帳戶許可權

「我的帳戶」和「管理 Web 應用程式權限」會自動指派給使用者帳戶。

下列許可權會動態指派給使用者帳戶：

- 我的帳戶（許可權 ID PLTADM30）- 容許存取「我的帳戶」頁面（帳戶 > 我的帳戶）。
- 管理 Web 應用程式許可權（許可權 ID WebAppAdminPermission）- 用於存取其他的 Web 應用程式。

請勿從使用者帳戶移除這些許可權。如果意外移除它們，請編輯「使用者帳戶」並儲存。遺漏的許可權將會還原。

使用者帳戶鑑別

使用者帳戶鑑別可以是本端或外部。

使用者帳戶鑑別可以是：

- 本端 - 已針對資料庫完成鑑別。
- 外部 - 已針對 LDAP 伺服器完成鑑別。外部鑑別不需要 LDAP 配接器，它搭配商業程序使用，可透過「Java 命名和目錄介面 (JNDI)」，與本端或遠端 LDAP 伺服器進行通訊。如果您沒有單一登入或 LDAP 的授權，則您建立的所有使用者都是本

端使用者，並根據應用程式的資料庫來鑑別。如果要建立外部使用者帳戶，您必須具有單一登入或 LDAP 的應用程式授權。

使用者帳戶建立核對清單

您可以建立使用者帳戶。

請利用這個核對清單來建立使用者帳戶：

作業	角色型安全核對清單	您的附註
1	建立新的許可權或檢閱預先安裝且預先配置許可權。	
2	建立新群組或檢閱預先安裝的群組。	
3	建立自訂密碼原則以指派給使用者。	
4	如果您使用外部鑑別，請設定外部鑑別的環境。	
5	建立使用者帳戶並指派許可權、群組和密碼原則。	

設定「外部使用者帳戶鑑別」的環境

建立外部使用者時可以指定替代的鑑別方法（通常是 LDAP）。

關於這項作業

建立外部使用者帳戶之前，您必須：

程序

1. 停止 Sterling B2B Integrator。
2. 指定替代的鑑別方法，方法是在 authentication_policy.properties.ini 檔案中新增或修改鑑別配置。 內容必須遵循此格式：authentication_4.*xxx*=*xxx*_value。
3. 輸入 `setupfiles.sh`。
4. 啟動 Sterling B2B Integrator。

搜尋使用者帳戶

您可以從**管理**功能表搜尋使用者帳戶。

關於這項作業

如果要搜尋使用者帳戶，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **使用者帳戶**。
2. 完成下列其中一項動作：
   - 在**帳戶名稱**欄位的「搜尋」之下，輸入要搜尋的部分名稱或完整使用者帳戶名稱，然後按一下**執行！**「帳戶」頁面會列出符合搜尋準則的所有使用者帳戶。

- 在**依英文字母順序**欄位的「列出」之下，選取**全部**或要搜尋的使用者帳戶的名稱的第一個字母，然後按一下**執行！**「帳戶」頁面會列出符合搜尋準則的所有使用者帳戶。

建立使用者帳戶

您可以從**管理**功能表建立新的使用者帳戶。

關於這項作業

在您開始之前，您必須知道您是在使用本端或外部鑑別：

- 本端 - 對應用程式的資料庫完成鑑別。預設值。
- 外部 - 已針對 LDAP 伺服器完成鑑別。外部鑑別不需要 LDAP 配接器，LDAP 配接器用於商業程序，可讓系統使用「Java 命名和目錄介面 (JNDI)」，與本端或遠端 LDAP 伺服器進行通訊。

如果您指派一或多個「授權使用者金鑰」給此帳戶，金鑰必須從交易夥伴取得，並在建立使用者帳戶之前移入。

註：支援多種外國語言時，一個使用者帳戶不應搭配使用一種以上的特定語言，以避免發生使用者介面顯示問題。

您也必須知道下列資訊：

欄位	說明
使用者 ID	您正要建立之使用者帳戶的使用者 ID。使用者 ID 長度至少必須有五個英數字元。不容許特殊字元或標點符號。必要。 僅針對 MySQL 資料庫而言，登入不區分大小寫。您應該一律使用唯一拼字 ID，這樣某位使用者便不會意外使用其他使用者的 ID。
密碼（僅限本端鑑別）	您正要建立之使用者帳戶的密碼。密碼長度至少必須有六個英數字元。容許特殊字元。對於本端使用者，此為必要欄位。此欄位不對外部使用者顯示。
確認密碼（僅限本端鑑別）	第二次輸入密碼。對於本端使用者，此為必要欄位。此欄位不對外部使用者顯示。
原則（僅限本端鑑別）	與此使用者帳戶相關聯的密碼原則。從清單選取您要關聯的原則。選用。此欄位不對外部使用者顯示。 系統從使用者使用此密碼登入的第一天計算到期日。
鑑別主機（僅限外部鑑別）	在其中鑑別使用者的輕量型目錄存取通訊協定 (LDAP) 伺服器。此欄位中所列的伺服器指定於 authentication_policy.properties.ini 檔。
階段作業逾時值	在您必須再次登入之前，容許的非作用中時間量（分鐘）。時間單位為分鐘。必要。

欄位	說明
可存取性	使用者帳戶有權存取的儀表板使用者介面部分。選用。 下列是可存取性選項： • 管理 UI - 僅限存取儀表板中的「管理主控台」窗格。 • AS2 UI - 僅限存取 AS2 Edition 介面。 • 儀表板 UI - 存取儀表板介面。可選擇「儀表板佈景主題」進行調整。
儀表板佈景主題	使用者帳戶有權存取的預先定義儀表板。如果可存取性設為「儀表板 UI」，則此為必要欄位。 下列是儀表板佈景主題選項： • 預設值 • 操作員 • 參與者 • 參與贊助者 • 贊助者 • AFT
名字	使用者的名字。必要。
姓氏	使用者的姓氏。必要。
電子郵件	使用者的電子郵件位址。
呼叫器	使用者的呼叫器號碼。
偏好的語言	將值設為**使用用戶端應用程式設定**。 **註：**此值引導 Sterling B2B Integrator 採用使用者瀏覽器中的指定語言和/或用戶端作業系統的語言環境。 **註：** 這是預設值。
管理者 ID	使用者的管理者其使用者 ID。
身分	與使用者帳戶相關聯的交易夥伴身分。一個交易夥伴僅能與一個使用者帳戶相關聯。使用者帳戶可以與許多群組相關聯，而每一個群組都具有自己的交易夥伴身分關聯。這樣可讓使用者帳戶與一個以上的交易夥伴相關聯。「身分」欄位用於遞送「信箱」中的訊息。從清單選取交易夥伴身分。 預設值為「中心組織」。

如果要建立使用者帳戶，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶 > 使用者帳戶**。
2. 按一下**建立新帳戶**旁的**執行！**
3. 在「新帳戶」頁面中，選取**鑑別類型**。
4. 輸入**使用者 ID**。
5. 輸入**密碼**。

6. 確認密碼。
7. 選取**原則**。
8. 輸入**階段作業逾時值**。
9. 選取**可存取性**。
10. 選取**儀表板佈景主題**。
11. 按**下一步**。
12. 在「SSH 授權使用者金鑰」頁面中，指派一或多個公開金鑰。將金鑰從**可用**窗格移動至**已指派**窗格，然後按**下一步**。
13. 在「群組」頁面中，指派許可權群組。將群組名稱從**可用**窗格移動至**已指派**窗格，然後按**下一步**。
14. 在「許可權」頁面中，指派個別許可權。將許可權從**可用**窗格移動至**已指派**窗格，然後按**下一步**。 依預設，與獲指派此使用者之群組相關聯的許可權已選取。必要許可權為「管理 Web 應用程式許可權」與「我的帳戶」。
15. 在「使用者資訊」頁面中，輸入**名字**。
16. 輸入**姓氏**。
17. 輸入**電子郵件位址**。
18. 輸入**呼叫器號碼**。
19. 選取**偏好語言**。選取值**使用用戶端應用程式設定**。

    註：此值引導 Sterling B2B Integrator 採用使用者瀏覽器中的指定語言和/或用戶端作業系統的語言環境。
20. 輸入**管理者 ID**。
21. 選取**身分**。
22. 按**下一步**
23. 檢閱使用者帳戶設定。
24. 按一下**完成**。 隨即建立使用者帳戶並顯示此訊息：

    已順利完成系統更新。

    如果您已建立外部使用者，請登出系統，然後再使用外部使用者 ID 或帳戶登入。系統將在外部 LDAP 伺服器上鑑別外部使用者 ID。

編輯使用者帳戶

您可以從**管理**功能表編輯使用者帳戶。

關於這項作業

註：支援多種外國語言時，一個使用者帳戶不應搭配使用一種以上的特定語言，以避免發生使用者介面顯示問題。

如果要編輯使用者帳戶，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶 > 使用者帳戶**。
2. 使用「搜尋」或「列示」選項，尋找您要編輯的使用者帳戶。
3. 針對您要編輯的使用者帳戶，按一下**編輯**。

4. 對這個使用者的鑑別類型進行任何變更。

   如果將鑑別類型從外部變更為本端，則需要建立用使用者的密碼。如果將鑑別類型從本端變更為外部，則無法變更使用者的密碼或密碼原則。
5. 對**新密碼**進行任何變更，並確認新密碼。
6. 對**原則**進行任何變更。
7. 對**階段作業逾時值**進行任何變更，然後按**下一步**。
8. 對 **SSH 授權使用者金鑰**進行任何變更，然後按**下一步**。
9. 進行任何群組變更，然後按**下一步**。
10. 進行任何許可權變更，然後按**下一步**。

    您無法移除 Admin Web App Permission 或 MyAccount。
11. 對使用者資訊進行任何變更，然後按**下一步**。

    註：如果是以受支援外國語言顯示使用者介面的使用者帳戶，請驗證「偏好的語言」值設定為**使用用戶端應用程式設定**。此值引導 Sterling B2B Integrator 採用使用者瀏覽器中的指定語言和/或用戶端作業系統的語言環境。
12. 檢閱使用者帳戶設定。
13. 按一下**完成**。

刪除使用者帳戶

您可以從**管理**功能表刪除使用者帳戶。

關於這項作業

如果要刪除使用者帳戶，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶 > 使用者帳戶**。
2. 使用「搜尋」或「列出」選項，尋找您要刪除的使用者帳戶。
3. 對您要刪除的使用者帳戶按一下**刪除**。
4. 按一下**確定**。
5. 檢閱使用者帳戶設定。
6. 按一下**刪除**。 隨即刪除選取的使用者帳戶並顯示此訊息：

   已順利完成系統更新。

更新我的帳戶資訊

「我的帳戶」資訊與使用者名稱和密碼相關聯，因此，當您登入時，您的個人資訊會顯示在「我的帳戶」頁面。您可以編輯您自己的帳戶資訊，以及變更登入系統時的初始頁面。

關於這項作業

有許多實例需要您編輯您的帳戶資訊來變更個人帳戶資訊。此外，您可能需要因安全起見變更密碼。

註：支援多種外國語言時，一個使用者帳戶不應搭配使用一種以上的特定語言，以避免發生使用者介面顯示問題。

如果要更新帳戶資訊：

程序

1. 從**管理功能表**中，選取**帳戶 > 我的帳戶**。
2. 如果要更新帳戶密碼，請在**舊密碼**欄位輸入您的現行密碼，然後在**新密碼**欄位輸入新密碼。於**確認新密碼**欄位再一次輸入新密碼。
3. 在**名字**、**姓氏**、**電子郵件**或**呼叫器**欄位中輸入任何變更。
4. 如果要變更指派給此帳戶的 **SSH 授權使用者金鑰**，請將金鑰從「可用的」移至「已指派」窗格。
5. 如果要變更**偏好的語言**，請選取語言。

   註：若是以支援的外國語言顯示使用者介面的使用者帳戶，請驗證該值是設定為**使用用戶端應用程式設定**。此值引導 Sterling B2B Integrator 採用使用者瀏覽器中的指定語言和/或用戶端作業系統的語言環境。
6. 如果要變更登入時顯示的**歡迎使用頁面**（管理主控台首頁），請從清單中選取。
7. 如果要同時變更「現行處理程序」頁面上顯示的處理程序數目，請為**現行處理程序頁面大小**選取新值。
8. 如果要同時變更「現行文件」頁面上顯示的文件數目，請為**現行文件頁面大小**選取新值。
9. 如果要重複使用瀏覽器視窗以啟動捷徑，請選取**重複使用視窗以啟動捷徑**。
10. 如果您希望系統以先前輸入的字串為基礎，自動完成搜尋，則選取**自動完成搜尋**。
11. 如果您希望系統記住搜尋依據值，請選取**記住搜尋依據值**。 這個選項會儲存您在每一個「搜尋」欄位中輸入的最後值。
12. 按一下**儲存**。 儲存新帳戶資訊並顯示下列訊息：

    已順利完成您的更新。

登入用的使用者帳戶使用者結束程式（5.2.5 版或更新版本）

Sterling B2B Integrator 提供 Active Directory 同步使用者結束程式，可讓您利用 Active Directory 而非 Sterling B2B Integrator 使用者介面，來管理您的使用者帳戶。在「IBM 服務客戶約定」期間，可以透過「IBM 服務」來配置這些使用者結束程式。如需相關資訊，請聯絡您的「IBM 業務代表」。

使用者結束程式	說明
IUserLoginUserExit_preAuthenticate	用來在鑑別之前插入自訂程式碼。
IUserLoginUserExit_postAuthenticateFail	用來在鑑別成功之後插入自訂程式碼。
IUserLoginUserExit_postAuthenticateSuccess	用來在鑑別失敗之後插入自訂程式碼。

用於登出的使用者帳戶使用者結束程式（5.2.6 版或更新版本）

Sterling B2B Integrator 提供 Active Directory 同步使用者結束程式，可讓您利用 Active Directory 而非 Sterling B2B Integrator 使用者介面，來管理您的使用者帳戶。

在「IBM 服務客戶約定」期間，可以透過「IBM 服務」來配置這些使用者結束程式。如需相關資訊，請聯絡您的「IBM 業務代表」。

使用者結束程式	說明
ILogoutUserExit_OnSessionInvalidate	用來在階段作業失效之前插入自訂程式碼。

單一登入

單一登入

單一登入 (SSO) 是一種鑑別處理程序，可讓使用者只需輸入一個使用者名稱和密碼，即可存取數個應用程式。以往，登入每一個應用程式的使用者必須管理許多使用者名稱和密碼。

SSO 的使用者鑑別不需要 LDAP 配接器，它搭配商業程序使用，透過「Java 命名和目錄介面 (JNDI)」，與本端或遠端 LDAP 伺服器進行通訊。

Sterling B2B Integrator 容許 SSO 與 Netegrity SiteMinder 整合，或與其他單一登入應用程式和伺服器上的 SSO 外掛程式的自訂實作類別整合。

單一登入僅限下列元件：

- 管理介面
- Mailboxing 介面
- 儀表板介面
- 進階檔案傳送 (AFT) 介面
- MyAFT 介面

單一登入提供者預設類別

所有介面的 SSO 登入 URL 類似一般登入介面，儀表板除外。儀表板介面 URL 為 http:Host:port/dashboard/sso.jsp。儀表板介面的要求標頭必須具有值 SM_USER=SSO 使用者名稱（或可在 SSO_USER_HEADER 下的 security.properties 檔中配置的值）。

SSOProviderDefault 介面容許單一登入 (SSO) 外掛程式以處理 Netegrity SiteMinder 的單一登入功能。

使用者從 SSO 階段作業登出後，您可以配置 SSO 以重新導向至外部 HTTP 頁面（代替 Sterling B2B Integrator 登出頁面）。SSO 伺服器的外部頁面可以是登入或登出頁面。

下面的範例顯示 SSOProviderDefault.java 類別：

```
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)
}
}
```

單一登入外掛程式元件

Sterling B2B Integrator 容許在其他單一登入應用程式和伺服器上，自訂單一登入 (SSO) 外掛程式的實作類別。您必須在 security.properties 檔中新增實作類別 SSO_AUTHENTICATION_CLASS.<n>=<新類別項目>，以實作 SSO 外掛程式。

您可以根據下列 ISSOProvider.java 介面類別，為 SSO 外掛程式寫入自訂實作類別。

SSOProvider.java 介面類別

```
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 類別

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

SSOAuthenticationException 類別

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

使用者鑑別方法

鑑別方法已在登入期間起始設定。鑑別方法會在成功鑑別後傳回使用者 ID。鑑別失敗會擲出 SSOAuthenticationException。如果存在 SSO 標頭，異常狀況應包含適當的原因碼和要處理的重新導向頁面。如果 SSO 標頭不存在，便會將控制項傳回系統登入畫面。

頁面鑑別方法

authenticatePage 方法會在每一個頁面上起始設定。頁面從 SSO 伺服器轉移期間的任何其他驗證都是以這個方法處理。例如，您可以連線測試 SSO 伺服器，檢查 SSO 階段作業是否已逾時。若鑑別失敗，應該會擲出異常狀況，包含適當的原因碼和重新導向頁面。

SSO 的要求無效

使用者登出、無法鑑別登入或頁面，或階段作業到期時，便會起始設定失效方法。為了讓 SSO 要求失效，應該執行 HTTP 重新導向方法。系統會針對失敗的鑑別，對下列方法進行起始設定：

- 如果 SSO 伺服器鑑別成功，但 Sterling B2B Integrator 鑑別失敗，則搭配原因碼起始設定 REASON_GIS_AUTHENTICATION_FAILURE 方法。
- 如果 SSO 伺服器鑑別失敗，則搭配原因碼起始設定 REASON_SSO_AUTHENTICATION_FAILURE 方法。
- 如果使用者登出，則搭配原因碼起始設定 REASON_LOGOUT 方法。
- 如果 HTTP 階段作業到期，則搭配原因碼起始設定 REASON_HTTP_SESSION_EXPIRED 方法。
- 如果使用者的 SSO 階段作業到期，則搭配原因碼起始設定 REASON_SSO_SESSION_EXPIRED 方法。

以 Netegrity SiteMinder 核對清單單一登入

您必須瞭解單一登入 (SSO) 和 Netegrity SiteMinder 才可配置 SSO。

請利用這個核對清單來配置 SSO 與 Netegrity SiteMinder：

作業	以 Netegrity SiteMinder 核對清單單一登入	附註
1	安裝 Netegrity SiteMinder 並搭配反向 Proxy 伺服器予以配置。	
2	配置「內容檔」以搭配 Netegrity SiteMinder 使用。	
3	配置「Netegrity 安全 Proxy 伺服器」。	
4	建立「Netegrity 伺服器安全領域」。	

如需其他單一登入應用程式和伺服器的 SSO 外掛程式的自訂實作資訊，請參閱「單一登入外掛程式元件」。

使用 IBM Global High Availability Mailbox 進行單一登入（5.2.6 版或更新版本）

具備適當許可權的 Sterling B2B Integrator 使用者可以直接存取 IBM® Global High Availability Mailbox 管理工具，作法是從 Sterling B2B Integrator 進行單一登入來管理 Global Mailbox。

開始之前

Sterling B2B Integrator 使用者必須屬於下列其中一個群組，才能從 Sterling B2B Integrator 直接存取 Global Mailbox 管理工具：

- *MAILBOX*
- *Deployment*
- *Mailbox Administrators*
- *Sterling B2B Integrator Admin*

關於這項作業

當您選擇藉由單一登入來存取 Global Mailbox 管理工具時，會在新的 Web 瀏覽器標籤中開啟新的 Global Mailbox 階段作業，而您的 Sterling B2B Integrator 階段作業仍維持可用。

您只需從 Sterling B2B Integrator 進行單一登入，就能存取 Global Mailbox。如果您登出 Global Mailbox 管理工具，並不會登出 Sterling B2B Integrator 階段作業。

如果您想變更 Global Mailbox 管理者密碼，必須直接登入 Global Mailbox 管理工具。

限制：如果您藉由單一登入來登入 Global Mailbox 管理工具，則無法變更 Global Mailbox 管理者密碼，且**管理者**功能表中的**變更密碼**無法使用。

如果要藉由單一登入來存取 Global Mailbox 管理工具，請執行下列動作：

程序

1. 從「管理主控台」頁面，展開「管理功能表」中的**部署**。
2. 展開 **Global Mailbox**。
3. 選取**信箱管理**。
4. 按一下**啟動 Global Mailbox 管理工具**超鏈結，以便在 Global Mailbox 管理工具中開啟新的階段作業。

   記住：當您按一下**啟動 Global Mailbox 管理工具**超鏈結時，會在新的 Web 瀏覽器標籤中開啟新的 Global Mailbox 階段作業。

為 Netegrity SiteMinder 配置單一登入的內容檔

您可以為 Netegrity SiteMinder 單一登入配置內容檔。

關於這項作業

如果要編輯 neo-ui.properties 檔與 security.properties 檔：

程序

1. 停止 Sterling B2B Integrator。
2. 導覽至 */install_dir*/install/properties。
3. 開啟 neo-ui.properties 檔。
4. 為每一個介面新增關聯的 SSO 項目。下列程式碼範例顯示相同 HTTP 網站的關聯項目：

```
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. 儲存並關閉 neo-ui.properties 檔。
6. 在文字編輯器中開啟 */install_dir*/install/properties/security.properties 檔。
7. 在 security.properties 中，尋找 ## SSO 鑑別配置參數，如下列程式碼範例所示：

```
## 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. 在 ##SSO 鑑別配置項目下方，變更下列 SSO 參數：

參數	說明	隨附值	新建值
SSO_AUTHENTICATION_ ENABLED	啟用或停用 SSO。	False	True
SSO_USER_HEADER	來自 Netegrity SiteMinder 或您 SSO 應用程式配置的使用者標頭名稱。	SM_USER 此為 Netegrity SiteMinder 中的值。	必須符合 Netegrity SiteMinder 或您 SSO 應用程式中的項目。
SSO_PAGE_ AUTHENTICATION_ ENABLED	在每一個頁面上啟用或停用 SSO 鑑別	False	True - 在每一個頁面上鑑別 SSO。 僅在提供「SSO 提供者類別」時變更。

參數	說明	隨附值	新建值
SSO_AUTHENTICATION_CLASS.n	提供鑑別支援的實作類別。	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	從所提供的 SSOProvider 類別選取清單。
SSO_FORWARD_URL URL	當您從「信箱」登出時，顯示所提供的頁面。否則顯示預設值。	Commented 顯示預設頁面。	提供 URL。

9. 儲存並關閉 security.properties 檔。
10. 啟動 Sterling B2B Integrator。

配置 Netegrity Secure Proxy Server

您可以將轉遞規則新增至 proxyrules.xml 檔，以配置 Netegrity Secure Proxy Server。

關於這項作業

配置 Netegrity Secure Proxy Server 之前，您必須：

- 在 acme.si.com 之類的伺服器上安裝 Sterling B2B Integrator。
- 知道安裝 Mailbox Browser Interface (MBI) 的埠號。您必須在適當的轉遞規則中使用此資訊。
- 知道安裝 Sterling B2B Integrator Dashboard 使用介面的埠號。您必須在適當的轉遞規則中使用此資訊。

如果要配置 Netegrity Secure Proxy Server：

程序

1. 將 Sterling B2B Integrator 的必要轉遞規則新增至 /opt/netegrity/proxy-engine/conf/proxyrules.xml 檔。

   下列範例顯示在您新增轉遞規則以存取 Sterling B2B Integrator 元件後，完整 proxyrules.xml 檔應該呈現的樣子：

```
<?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. 新增下列內容至 proxyrules.xml 檔的資料行，以關閉 Cross Server Scripting 移入安全 Proxy 伺服器，因為Sterling B2B Integrator 不支援 Netegrity Cross Server Scripting 原則執行。

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

3. 儲存並關閉 proxyrules.xml 檔。

建立 Netegrity Policy Server 安全領域

Netegrity Policy Server 管理者必須針對由 Secure Proxy Server 轉遞的每一個 URL 型樣建立「安全領域」。這些安全領域需要有指派用於鑑別與授權的必要規則。

關於這項作業

此外，Secure Proxy Server 中的 Web 代理程式必須配置為與 Policy Server 通訊。

為所列每一個 URL 型樣建立安全領域：

URL 型樣	可存取：
/mbi/*	應用程式信箱介面
/dashboard/*	應用程式儀表板介面，使用 http://host:port/dashboard 格式

URL 型樣	可存取：
/datastore/*	資料儲存庫元件
/portlets/*	儀表板介面中的應用程式 Portlet 元件
/help/*	環境定義相關說明元件
/webxtools/*	Web 延伸公用程式
/gbm/*	「圖形程序建模器」元件

密碼

密碼原則

密碼原則是安全決策集，讓您可以根據公司的安全原則，製作與套用不同的使用者帳戶。這些選擇包括下列項目：密碼的有效天數、密碼的上限長度與下限長度。

您可以在新增使用者時使用密碼原則來簡化安全作業。您可以建立一個密碼原則，並將它套用到需要相同存取權的所有使用者，而不是為每一位個別使用者新增個別原則。

建立密碼原則後，您可以只將它套用到內部使用者帳戶。這提供您在維護安全原則時擁有最大的彈性。如果您使用 LDAP，您無法將密碼原則套用到外部帳戶。

密碼原則的預設值為：

參數	預設值
原則 ID	default_user
原則名稱	預設使用者原則
有效天數	60
長度下限	6
長度上限	28
保留在歷程中的密碼數目	5
密碼需要包含特殊字元	已選取
第一次試圖登入時需要變更密碼	已選取

密碼原則作業包括：

- 建立密碼原則
- 搜尋密碼原則
- 編輯密碼原則
- 刪除密碼原則
- 編輯鎖定參數
- 編輯密碼到期訊息

自訂密碼原則

Sterling B2B Integrator「自訂密碼原則」是一種可新增更多密碼原則規則的安全特性。這些附加的密碼規則可協助您避免使用強度弱且容易被駭的密碼，同時拒絕不符合規定的密碼。

如果要啟用此功能，您必須：

- 透過插入點實作某種自訂 Java 程式碼。一旦啟用，插入點可用於與密碼原則相關聯之系統的所有使用者（此為廣域設定）。
- 新增 passwordPolicyExtensionImpl 內容至 customer_overrides.properties 檔。
- 套用自訂密碼原則至「使用者帳戶」。

自訂密碼原則延伸規格會比預設密碼原則優先套用。如果密碼違反一個以上的原則需求（一個由延伸類別施行，另一個由預設實作施行），則僅會對使用者顯示從延伸類別傳回的錯誤訊息。

範例：密碼原則範例

這個範例顯示密碼原則的可能設定。

例如，名稱為 Test 的密碼原則可能會有下列密碼設定：

- 有效期 10 天
- 長度下限 10 個字元
- 長度上限 20 個字元
- 至少必須有兩個特殊字元
- 使用者必須在起始登入期間變更預設密碼
- 保留在歷程中的密碼數目

利用前述範例，系統管理者將使用者名稱和密碼提供給使用者。使用者利用提供的使用者名稱和密碼登入，系統會提示使用者變更密碼。如果使用者提供的密碼不足 10 個字元、超過 20 個字元或沒有至少兩個特殊字元，系統會提示使用者進行更正。一旦使用者變更密碼使其符合密碼原則中設定的所有條件後，系統便會儲存新密碼並允許使用者存取。每一個使用者帳戶只能有一個相關聯的密碼原則，但您可以將一個密碼原則套用到多個使用者帳戶。

除了介面中的密碼原則變更之外，您還可以變更容許使用者未正確登入的次數，超過這個次數後，系統即會鎖定嘗試登入之使用者的使用者帳戶。

比方說，如果連續登入嘗試失敗次數設定為三，且您輸入錯誤密碼三次，您就無法利用該特定電腦進行登入。您可以利用具有系統存取權的任何其他電腦來進行登入。

安裝密碼或通行詞組

在安裝期間，您可以建立 Sterling B2B Integrator 安裝的系統通行詞組。通行詞組是長度超過 16 個字元的高度複雜字串。啟動系統及存取受保護的系統資訊時，需要系統通行詞組。

唯一可以更新或變更通行詞組的人，就是建立/安裝軟體的人。如果遺失或忘記通行詞組，您將無法啟動系統。唯一可以更新系統通行詞組的使用者，就是執行安裝的使用者。

系統不會儲存系統通行詞組，但 Windows 安裝除外，為了方便系統作為非互動式服務執行，會將通行詞組以混淆編碼形式儲存在 security.properties 中。在其他平台上，通行詞組會以明文方式儲存在 security.properties 中，所以您在啟動系統時不需要在指令行中輸入它。不過，系統通行詞組只受作業系統檔案存取控制的保護。

自訂原則密碼核對清單

您可以實作自訂原則密碼。

請使用下列核對清單來實作自訂密碼原則：

作業	自訂原則密碼核對清單
1	在 <SI_Install_Dir> 內建立目錄結構，以用於測試、原則和延伸。
2	在延伸目錄內建立 java 類別。
3	指定 customer_overrides.properties 檔中實作密碼原則（passwordPolicyExtensionImpl 內容）的 Java 類別。
4	將實作類別 Jar 新增至類別路徑。
5	定義錯誤訊息。

範例 - 自訂原則密碼

這個範例顯示自訂原則密碼延伸。

這是自訂原則密碼延伸的範例。

介面 com.sterlingcommerce.woodstock.security.PasswordPolicyExtension 已新增至系統中，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);
}
```

從方法傳回空值表示已接受密碼。傳回任何其他值表示密碼無效。

範例實作

```
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";
      }

}
```

搜尋密碼原則

您可以從**管理**功能表搜尋密碼原則。

關於這項作業

如果要搜尋密碼原則：

程序

1. 從**管理功能表**中，選取**帳戶** > **密碼原則**。
2. 在「密碼原則」頁面中，完成下列其中一項動作：
   - 在**密碼原則名稱**欄位的「搜尋」之下，輸入要搜尋的部分名稱或完整密碼原則名稱，然後按一下**執行！**「密碼原則」頁面會列出符合搜尋準則的所有許可權。
   - 在**依英文字母順序**欄位的「列出」之下，選取**全部**或要搜尋的密碼原則的名稱的第一個字母，然後按一下**執行！**「密碼原則」頁面會列出符合搜尋準則的所有許可權。

建立密碼原則

您可以建立密碼原則，以指派原則給使用者帳戶。您不需要將密碼原則與使用者帳戶相關聯，不過這樣確實有助於管理您的安全。

關於這項作業

在您開始之前，您必須知道下列資訊：

欄位	說明
原則 ID	可在資料庫中識別密碼原則的 ID。
原則名稱	密碼原則被參照時，顯示於使用者介面的原則名稱。
有效天數	使用者密碼的有效天數。預設值為 0，表示密碼永遠不會到期。 如果您提供 1 到 999 之間的值，當此時段到期時，系統會提示使用者變更密碼。在指派密碼給使用者帳戶之後，從使用者第一次登入起算，有效期限便開始倒數。

欄位	說明
長度下限	密碼必須符合的長度下限。必要。有效值為任何數字。此數字必須至少設定為 6。預設值是 6。如果未套用任何原則，系統會強制設定為長度下限 6。
長度上限	密碼可以達到的長度上限。必要。有效值為任何數字。此數字必須至少設定為與長度下限相同。預設值為 28。
保留在歷程中的密碼數目	使用者在資料庫 PWD_HISTORY 表格中保留的密碼數目。在此密碼數目已超出時，最舊密碼便會從表格中移除，並且可以再度由使用者使用。預設值為 0。
密碼需要包含特殊字元	指定密碼至少必須包含一個特殊字元。有效值包括數字、大寫字母、!、@、#、$、%、^、& 或 *。
需要在第一次嘗試登入時變更密碼	指定使用者必須在起始登入後變更預設密碼。這會在使用者第一次登入後，提示他們變更密碼。

如果要建立密碼原則：

程序

1. 從**管理功能表**中，選取**帳戶** > **密碼原則**。
2. 按一下**建立新密碼原則**旁的**執行！**
3. 在「密碼原則」頁面中，輸入**原則 ID**。
4. 輸入**原則名稱**。
5. 輸入**有效天數**。
6. 輸入**長度下限**。
7. 輸入**長度上限**。
8. 輸入**保留在歷程中的密碼數目**。
9. 如果要求密碼包含特殊字元，請選取此勾選框。
10. 如果要求使用者在第一次嘗試登入時變更密碼，請選取此勾選框。
11. 按**下一步**。
12. 檢閱密碼原則設定。
13. 按一下**完成**。

編輯密碼原則

您可以從**管理**功能表編輯密碼原則。

關於這項作業

如果要編輯密碼原則，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **密碼原則**。
2. 使用「搜尋」或「列示」選項，尋找您要編輯的密碼原則。
3. 針對您要編輯的密碼原則，按一下**編輯**。
4. 在「密碼原則設定」頁面中，進行適當的變更，然後按**下一步**。
5. 檢閱密碼原則設定。

6. 按一下**完成**。

   隨即顯示下列訊息：

   已順利完成系統更新。

刪除密碼原則

如果您刪除密碼原則，與該特定密碼原則相關聯的使用者帳戶仍然可以登入，但該使用者不會被迫變更密碼。如果使用者真的變更密碼，系統並不會針對新密碼完成任何驗證。

關於這項作業

如果要刪除密碼原則：

程序

1. 從**管理功能表**中，選取**帳戶** > **密碼原則**。
2. 使用「搜尋」或「列示」選項，尋找您要刪除的群組。
3. 對您要刪除的密碼原則按一下**刪除**。
4. 在「確認」頁面中，按一下**刪除**。

   隨即顯示下列訊息：

   已順利完成系統更新。

變更使用者密碼有效期限的天數

系統會在管理主控台首頁的「系統警示」區段中放置訊息，以通知您密碼即將到期。系統管理者可以變更在到期之前幾天通知使用者。

關於這項作業

訊息指出您的密碼將在某具體天數內到期。系統每一天都會提示您變更密碼；天數會每天減 1，直到密碼到期當天為止。

系統管理者可以在 ui.properties.ini 檔中變更到期前天數。您應該在 ui.properties.ini 檔中進行所有變更，而不是 ui.properties 檔。如果您在 ui.properties 檔中進行變更，然後重新啟動系統，您對 ui.properties 檔所做的變更將會被 ui.properties.ini 檔改寫。

如果要變更密碼有效期限的天數：

程序

1. 停止 Sterling B2B Integrator。
2. 導覽至 /*install_dir*/install/properties。
3. 開啟 ui.properties.ini 檔。
4. 尋找 MsgPwdExpires= 15 項目。
5. 將 15 變更為使用者密碼有效期限的新天數。
6. 儲存檔案。
7. 導覽至 /*install_dir*/install/bin。
8. 輸入 **setupfiles.sh**。

9. 重新啟動 Sterling B2B Integrator。 您在 ui.properties.ini 檔中所做的變更會套用至 ui.properties 檔，並對所有使用者帳戶生效。

封鎖後重設您自己的密碼

如果您遭到封鎖，您可以利用其他任何電腦登入、等待 30 分鐘讓鎖定到期，或聯絡系統管理者來移除鎖定。

關於這項作業

如果您遭到封鎖：

- 使用已存取系統的任何其他電腦登入。
- 等待 30 分鐘，鎖定到期後將容許您使用遭到鎖定的電腦重新嘗試登入。
- 聯絡系統管理者透過「鎖定管理程式」頁面移除鎖定。這容許您使用遭到鎖定的電腦重新嘗試登入。

定義自訂密碼原則的錯誤訊息

您可以定義自訂密碼原則延伸規格的錯誤訊息。

關於這項作業

錯誤訊息會將密碼規則告知使用者，並列出拒絕密碼變更的原因。自訂密碼錯誤訊息定義於 Login_*language_dir*.properties_*uniqueID*_ext 檔。如果未提供自訂專用文字，將傳送預設錯誤訊息給使用者。Login_*language_dir*.properties_*uniqueID*_ext 檔不屬於預設的系統程式碼。該檔必須在起始系統安裝後建立及移入，以符合您的環境。

如果要定義自訂密碼原則延伸規格的錯誤訊息：

程序

1. 導覽至 */install_dir*/install/properties/lang/*language_dir*目錄。 其中 *language_dir* 是客戶語言環境（例如英文、日文、法文）的語言集。
2. 編輯 Login_*language_dir*.properties_*uniqueID*_ext 檔。 其中 language_dir 是客戶語言環境的語言集，而 <filename> 是新自訂密碼延伸的唯一 ID。例如：Login_en.properties_custompasswd_ext。
3. 在自訂延伸檔中，新增項目至錯誤狀況集的檔案，然後定義傳回給使用者的敘述字串。 例如，nogood = 密碼必須包含至少一個小寫字元，一個大寫字元，以及一個數字或特殊字元。
4. 儲存並關閉檔案。

在 customer_overrides.property 檔案中指定自訂密碼原則延伸規格

您可以指定實作密碼原則延伸規格的 Java 類別。

關於這項作業

如果要外掛自訂實作，必須在 customer_overrides.properties 檔的 passwordPolicyExtensionImpl 內容中指定 Java 類別名稱。

如果要指定實作密碼原則延伸規格的 Java 類別：

程序

1. 導覽至安裝目錄。
2. 導覽至 properties 目錄。
3. 編輯 customer_overrides.properties 檔。
4. 在檔案的最後新增 passwordPolicyExtensionImpl 內容，並輸入實作密碼延伸驗證的 Java 類別。 例如，security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl。
5. 儲存並關閉檔案。

新增實作類別 JAR 至自訂密碼原則的類別路徑

若為自訂密碼原則，您必須將實作類別 JAR 新增至類別路徑。

關於這項作業

延伸實作類別必須如下編譯及打包成 Jar：

程序

1. 導覽至 *SI_Install_Dir*。
2. 輸入下列指令，以編譯自訂類別檔：

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

3. 從 *SI_Install_Dir* 執行下列指令，以建立 jar 檔：

   jar cf *any_filename*.jar *absolute_path_to_custom_class_file*.class 其中 *any_filename*.jar 是要建立之新 jar 檔的名稱，*absolute_path_to_custom_class_file*.class 是自訂實作 Java 類別檔的名稱。例如：jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class

4. 導覽至 *SI_Install_Dir*/bin 目錄。
5. 輸入下列指令，將新建的 jar 新增至類別路徑：

   ```
   ./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 鑑別

輕量型目錄存取通訊協定 (LDAP) 作為 Sterling B2B Integrator 的鑑別工具

輕量型目錄存取通訊協定 (LDAP) 是一組通訊協定，用來存取儲存於資訊目錄（也就是 LDAP 目錄）中的資訊。

LDAP 目錄是一種資料庫，而不是關聯式資料庫，用來管理分散於網路上多個伺服器且已針對讀取效能最佳化的資訊。

您可以使用 LDAP 將外部使用者帳戶的鑑別委派給 LDAP 目錄，以及使用公司中其他應用程式所用的相同安全資訊來提供鑑別。如果公司已採用 LDAP，您就可以使用現有的 LDAP 目錄。

使用者帳戶鑑別不需要 LDAP 配接器，它是和商業程序一起用來透過「Java 命名和目錄介面 (JNDI)」與本端或遠端 LDAP 伺服器進行通訊。

如果您的 LDAP 伺服器未運作，具有內部帳戶的使用者仍然可以存取；不過，具有外部帳戶的使用者必須等到 LDAP 伺服器運作後才能存取。

在您可以使用 Sterling B2B Integrator 配置 LDAP 之前，必須具有：

- LDAP 知識
- 對含有使用者資訊且已安裝和配置之 LDAP 伺服器的存取權
- LDAP 伺服器的位置
- （適用於 SSL）金鑰儲存庫和信任儲存庫中已安裝的安全憑證
- 已建立將透過 LDAP 伺服器鑑別之每個使用者的外部使用者帳戶
- （適用於 SSL）金鑰儲存庫和信任儲存庫的位置

範例：LDAP 鑑別配置參數

這個範例顯示 LDAP 鑑別配置參數。

下列範例顯示 LDAP 鑑別配置參數：

```
## 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 鑑別配置核對清單

您可以使用 Sterling B2B Integrator 配置 LDAP。

請使用此核對清單來使用 Sterling B2B Integrator 配置 LDAP：

作業	**LDAP 配置核對清單**
1	使用下列其中一種方法來配置 LDAP： • 密碼比較模式 • 密碼二進位模式
2	使用 Sterling B2B Integrator 配置 LDAP
3	驗證 LDAP 配置
4	選用。將 LDAP 密碼加密。

以密碼連結模式配置 LDAP

您可以輸入外部帳戶的**使用者 ID** 和**密碼**，以便於密碼連結模式下配置 LDAP。

關於這項作業

如果要以密碼連結模式配置 LDAP：

程序

輸入您外部使用者帳戶的**使用者 ID** 與**密碼**。 系統：

- 嘗試透過認證連結至 LDAP 儲存庫，便可執行必要查詢。
- 搜尋 LDAP 目錄中，具有適當使用者 ID的使用者。
- 從 LDAP 目錄擷取使用者的識別名稱 (DN)。
- 使用使用者 DN 與密碼嘗試連結至 LDAP 儲存庫。
- 成功 - 系統以使用者身分連結至 LDAP 儲存庫。
- 失敗 - 系統無法以使用者身分連結至 LDAP 儲存庫。

以密碼比較模式配置 LDAP

您可以在密碼比較模式下配置 LDAP。

關於這項作業

如果要以密碼比較模式配置 LDAP：

程序

1. 輸入您外部使用者帳戶的**使用者 ID** 與**密碼**。
2. 系統透過認證嘗試連結至 LDAP 儲存庫，便可執行必要查詢。
3. 系統會在 LDAP 目錄中，搜尋具有適當使用者 ID 的使用者。
4. 系統從 LDAP 目錄擷取使用者密碼。
5. 系統比較使用者提供的密碼與從 LDAP 目錄擷取的密碼。如果密碼符合，您便透過鑑別並獲准存取系統。如果密碼不符合，您便無法透過鑑別也不准存取。

使用 Sterling B2B Integrator 配置 LDAP

如果要將 Sterling B2B Integrator 配置為使用 LDAP，您必須編輯 authentication_policy.properties.ini 檔。您也可以使用 customer_overrides.properties 檔來設定內容值，這些內容值無法被修補程式安裝改寫。

關於這項作業

如果配置 LDAP 鑑別：

程序

1. 停止 Sterling B2B Integrator。
2. 導覽至安裝目錄。
3. 導覽至 properties 目錄。
4. 開啟 authentication_policy.properties.ini 檔。
5. 在 authentication_policy.properties.ini 中尋找 ## GIS/LDAP 鑑別配置項目。
6. 在 ##GIS/LDAP 鑑別配置項目下方，變更下列 LDAP 參數：

參數	說明	隨附值	變更為
#LDAP_SECURITY_TRUSTSTORE	本端信任儲存庫的路徑。您必須在信任儲存庫中儲存 LDAP 所需的憑證。您無法使用來自交易夥伴的憑證。選用。僅在使用 SSL 時使用。	非作用中路徑	本端信任儲存庫的完整路徑。
#LDAP_SECURITY_TRUSTSTORE_PASSWORD	容許存取信任儲存庫的密碼。選用。僅在使用 SSL 時使用。	changeit	容許存取本端信任儲存庫的密碼。

參數	說明	隨附值	變更為
#LDAP_SECURITY_ KEYSTORE	本端金鑰儲存庫的路徑。您必須在金鑰儲存庫中儲存 LDAP 所需的憑證。您無法使用來自交易夥伴的憑證。選用。僅在使用 SSL 時使用。	非作用中路徑	本端金鑰儲存庫的完整路徑。
#LDAP_SECURITY_ KEYSTORE_ PASSWORD	容許存取金鑰儲存庫的密碼。選用。僅在使用 SSL 時使用。	password	容許存取金鑰儲存庫的密碼。
#authentication_ <number>. enabled	啟用或停用 LDAP。 False - 將停用從此鑑別主機建立的所有使用者（無法登入）。 True - 只能從內部或外部（不能同時）存取每一個使用者，因為每一個使用者 ID 都是唯一的。用於內部鑑別時，不會勾選此值。	False	True
#authentication_<number> .jndi_factory	為 LDAP 服務提供者建立起始環境定義之 Factory 類別的類別名稱。這是隨附於 JDK 的標準環境定義 Factory。	com.sun. jndi.ldap. LdapCtx Factory	不變
#authentication_ <number>.server	指定 LDAP 伺服器之主機名稱的 URL。	非作用中路徑	本端 LDAP 主機 URL。
#authentication_ <number>.port	LDAP 伺服器的埠號。		
#authentication_ <number>. security_type	供提供者使用的鑑別方法。系統僅支援簡式鑑別。	simple	不變
#authentication_ <number>. principle	要鑑別之原則（可讓系統執行查詢）的身分。此參數是 LDAP ASN.1 連結要求中的名稱元件。	cn=Manager, dc=amr, dc=stercomm, dc=com	本端命名資訊。
#authentication_ <number>. credentials	在 LDAP 儲存庫中，針對 LDAP 原則設定的密碼，可讓系統執行查詢。	SecretPassword	搭配您本端原則的本端密碼。
#authentication_ <number>. security_protocol	指定提供者使用何種安全通訊的物件。	SSL	不變。如果您選擇不使用 SSL，將看不見此參數。

參數	說明	隨附值	變更為
#authentication_ <number>. password_attribute	包含使用者密碼的 LDAP 屬性名稱。 此參數僅使用於 #LDAP_ AUTHENTICATE_ WITH_USER_BIND 設為 False 時。	userPassword	包含密碼的本端屬性。
#authentication_ <number>. search_root	指定使用者查詢所依據之來源根目錄的物件。	dc=amr, dc=stercomm, dc=com	本端搜尋路徑。
#authentication_ <number>.search_filter	指定搜尋時所使用範本的物件。<userid> 值會在要求時動態取代為使用者要求鑑別的使用者 ID。	(uid=<userid>)	Windows Active Directory 伺服器可以使用的項目，例如： (sAMAccount Name=<userid>)
#authentication_ <number>. with_user_bind	指定是否要根據成功連結鑑別使用者。 False - 系統從 LDAP 伺服器擷取使用者密碼的值，然後對所提供的使用者認證執行比較。 True - 系統運用使用者的識別名稱與所提供的認證，連結至 LDAP 伺服器。成功連結表示成功鑑別。	false	如果您想要使用使用者連結進行鑑別，請變更為 True。

7. 儲存 authentication_policy.properties.ini 檔。
8. 輸入 /*install_dir*/install/bin/setupfiles.sh (UNIX) 或 *install_dir*\install\bin\setupfiles.cmd (Windows)，以將 LDAP 項目從 authentication_policy.properties.ini 檔更新為 authentication_policy.properties 檔。
9. 啟動 Sterling B2B Integrator。

   已套用 authentication_policy.properties 檔的變更，您可以立即使用 LDAP 伺服器來鑑別使用者。

   啟動後，系統會從 authentication_policy.properties 檔識別 LDAP 伺服器。系統會在使用者登入時鑑別外部使用者。

驗證 LDAP 配置

如果要驗證您已使用 Sterling B2B Integrator 正確配置 LDAP，請檢閱「使用者鑑別」之下的 Authentication.log 檔案，以確定系統已接受 LDAP 配置。

關於這項作業

如果連接至 LDAP 目錄發生問題，或 LDAP 鑑別失敗，請檢查 Authentication.log 檔案中的 DEBUG 日誌陳述式以疑難排解問題。Authentication.log 檔案記錄所有登入嘗試，不論其成功或失敗。

將 LDAP 密碼加密

您可以在 customer_overrides.property 檔中將 LDAP 相關密碼加密，以在內容檔中隱藏這些密碼。

關於這項作業

下列參數（內容）可用來在 customer_overrides.properties 檔中將 LDAP 密碼加密：

參數/內容	說明
authentication_policy.authentication _1.credentials	此參數或內容可控管存取 LDAP 實例所需的主體密碼。這樣應該是安全的，因為不會以純文字顯示任何用於控管安全和存取權的密碼。
authentication_policy. LDAP_SECURITY_ TRUSTSTORE_PASSWORD	此參數或內容可控管用於保護 LDAP 連線安全的信任儲存庫（JKS 格式）密碼。您必須提供此 JKS 的通行詞組，才能存取信任儲存庫，因為它是加密檔。
authentication_policy. LDAP_SECURITY_KEYSTORE_PASSWORD	如果使用用戶端型 SSL 鑑別來保護給定的 LDAP 實例連線安全，此參數或內容可控管密碼。

如果要將 LDAP 密碼加密，請執行下列動作：

程序

1. 導覽至 bin 目錄。
2. 使用 encrypt_string.[sh/cmd] 來判定所要加密之內容/參數的實際值。
3. 更新 customer_overrides.properties 檔中的參數/內容，使其包含下列項目。使用 bin/encrypt_string.sh（或 .cmd），將所有 <ENCVAL> 取代為該內容註銷的非加密字串的加密值。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
```

使用者新聞

使用者新聞

「使用者新聞」特性可讓您將訊息公佈至「管理主控台」首頁。使用者新聞可通知使用者變更內容或提醒使用者重要事件和作業。

可公佈訊息：

- 給所有使用者
- 給特定使用者
- 給多位使用者

根據有效日期和到期日來顯示新聞項目。您也可以將訊息設定為：

訊息類型	符號	說明
注意		提供一般或低優先順序的公告資訊。
警示		提供高優先順序的公告資訊。

您必須具備帳戶的寫入權，才可建立使用者新聞訊息。刪除舊訊息減少儲存需求和所需的時間以擷取特定訊息。

使用者新聞作業包括：

- 為特定使用者建立「使用者新聞訊息」
- 為所有使用者建立「使用者新聞訊息」
- 搜尋「使用者新聞訊息」
- 編輯「使用者新聞訊息」
- 刪除「使用者新聞訊息」

建立所有使用者適用的使用者新聞訊息

您可以從**管理**功能表，為所有使用者建立使用者新聞訊息。

關於這項作業

在您開始之前，您必須知道下列資訊：

欄位	說明
類型	您正要建立的訊息類型。有效值為 Notice 及 Alert。
主旨	您正要建立的訊息其主旨。
訊息	您正要建立的訊息其主體。

程序

1. 從**管理功能表**中，選取**帳戶** > **使用者新聞**。
2. 按一下**新訊息**旁的**執行！**
3. 輸入**類型**。
4. 輸入**主旨**。
5. 輸入**訊息**。
6. 按**下一步**。
7. 選取**全部使用者**，然後按**下一步**。
8. 輸入訊息的**有效日期** (yyyy-mm-dd)。
9. 輸入訊息的**到期日** (yyyy-mm-dd)。
10. 按**下一步**。
11. 檢閱「新聞訊息設定」。
12. 按一下**完成**。

建立特定使用者適用的使用者新聞訊息

您可以從**管理**功能表，為特定使用者建立使用者新聞訊息。

關於這項作業

在您開始之前，您必須知道下列資訊：

欄位	說明
類型	您正要建立的訊息類型。有效值為 Notice 及 Alert。
主旨	您正要建立的訊息其主旨。
訊息	您正要建立的訊息其主體。

程序

1. 從**管理功能表**中，選取**帳戶** > **使用者新聞**。
2. 按一下**新訊息**旁的**執行！**
3. 輸入**類型**。
4. 輸入**主旨**。
5. 輸入**訊息**。
6. 按**下一步**。
7. 選取**選取的使用者**。
8. 選取每一個您希望其收到此訊息的使用者名稱。
9. 按**下一步**。
10. 輸入訊息的**有效日期** (yyyy-mm-dd)。
11. 輸入訊息的**到期日** (yyyy-mm-dd)。
12. 按**下一步**。
13. 檢閱「新聞訊息設定」。
14. 按一下**完成**。

搜尋使用者新聞訊息

您可以從**管理**功能表搜尋使用者新聞訊息。

關於這項作業

如果要搜尋使用者新聞訊息：

程序

1. 從**管理功能表**中，選取**帳戶** > **使用者新聞**。
2. 請使用下列其中一個搜尋選項：

使用者新聞搜尋選項	動作
依使用者 ID	請選取「全部」或從清單中選取特定使用者。
依主旨	輸入部分訊息文字。
依有效日期範圍	輸入日期範圍 (mm/dd/yyyy)。

3. 按一下**執行！** 「使用者新聞」頁面會列出符合搜尋準則的所有訊息。

編輯使用者新聞訊息

您可以從**管理**功能表編輯使用者新聞訊息。

關於這項作業

如果要編輯使用者新聞訊息，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **使用者新聞**。
2. 搜尋您要編輯的使用者新聞訊息。
3. 針對您要編輯的使用者新聞訊息，按一下「編輯」。
4. 視需要更新訊息類型、主旨或訊息。
5. 按**下一步**。
6. 視需要更新接收此訊息的使用者，然後按**下一步**。
7. 視需要更新訊息的**有效日期** (yyyy-mm-dd)。
8. 視需要更新訊息的**到期日** (yyyy-mm-dd)。
9. 按**下一步**。
10. 檢閱「新聞訊息設定」。
11. 按一下**完成**。

刪除使用者新聞訊息

您可以從**管理**功能表刪除使用者新聞訊息。

關於這項作業

如果要刪除使用者新聞訊息，請執行下列動作：

程序

1. 從**管理功能表**中，選取**帳戶** > **使用者新聞**。
2. 搜尋您要刪除的使用者新聞訊息。
3. 對您要移除的新聞訊息按一下**刪除**。
4. 檢閱「新聞訊息設定」。
5. 按一下**刪除**。 隨即顯示下列訊息：
   已順利完成系統更新。

文件加密

文件加密特性概觀

文件加密是 Sterling B2B Integrator 隨附的一項特性，可在傳統的檔案與資料庫許可權之外，再多配置一層安全性。如果您整合 Sterling File Gateway 與 Sterling B2B Integrator，則可使用相同的文件加密特性來保護存放資料。

Sterling File Gateway 是利用不同通訊協定、檔案命名慣例及檔案格式，在夥伴之間安全傳送檔案的一種應用程式。

文件加密特性預期用來保護存放資料以免遭到探查。此功能可讓您為儲存於資料庫和/或檔案系統的有效負載資料加密。此功能也設計用來預防系統外部人士直接存取資料庫或檔案系統，使其無法檢視有效負載資料。

文件加密的重要層面：

- 安裝時的預設配置為無加密。如果您想要加密文件，您必須開啟此功能。
- 您可以隨時開啟此特性，但唯有開啟加密後收到的文件才會進行加密。
- 一旦您開啟此功能，整個系統上的所有有效負載都會加密。
- 唯有文件有效負載資料會加密，meta 資料**不**會加密。
- 加密與解密使用相同的加密金鑰。
- 系統使用預先定義的憑證 (doccrypto) 來加密文件。您可以建立不同的系統憑證。如果要這麼做，您必須在 customer_overrides.properties 檔中，更新 CERT_NAME 的值。

效能會因啟用加密而受影響，每個客戶都將看到不同的效能影響，這些影響取決於硬體、處理文件的數目與大小，以及執行文件持續性與擷取以及其他活動時，給定伺服器耗費在其上的相對處理時間量。

文件加密的加密金鑰

使用相同金鑰來加密與解密資料庫或檔案系統文件。數位憑證用於產生及加密金鑰，系統通行詞組則用於加密數位憑證。

文件加密為每份文件建立一個金鑰，此金鑰會隨文件一起儲存在 meta 資料之中。數位憑證的儲存方式如同其他的系統憑證。

系統使用預先定義憑證 (doccrypto) 來產生及加密用於加密文件的金鑰。您可以建立不同的系統憑證。如果要這麼做，您必須在 customer_overrides.properties 檔中，更新 CERT_NAME 的值。

為文件加密指派不同的憑證

系統使用預先定義的憑證 (doccrypto) 來加密文件。您可以建立不同的系統憑證用來加密文件，例如，前一個憑證即將到期。如果這麼做，您必須在 customer_overrides.properties 檔中更新 CERT_NAME 的值。

關於這項作業

注意：請勿刪除或重新命名前一個系統憑證。您需要前一個憑證來解密先前用它來加密的文件。新的系統憑證從未用來加密這些文件，因此無法解密這些文件。

執行這項程序之前，您需要：

- 產生新的憑證
- 知道憑證的名稱

如果要更新 CERT_NAME 的值：

程序

1. 導覽至 install 目錄。
2. 導覽至 properties 目錄。
3. 開啟 customer_overrides.properties 檔。
4. 在檔案中加入下面這一行：

   ```
   security.CERT_NAME=name_of_new_system_certificate
   ```

5. 儲存並關閉 customer_overrides.properties 檔。
6. 停止並重新啟動 Sterling B2B Integrator。

對檔案系統和資料庫文件啟用文件加密

您可以從 properties 目錄將檔案系統文件和資料庫文件加密。

關於這項作業

如果要將檔案系統和資料庫文件加密，請執行下列動作：

程序

1. 導覽至 install 目錄。
2. 導覽至 properties 目錄。
3. 開啟 customer_overrides.properties 檔。
4. 將下列字行新增至檔案：

   ```
   security.ENC_DECR_DOCS=ENC_ALL
   ```

5. 儲存並關閉 customer_overrides.properties 檔。
6. 停止並重新啟動 Sterling B2B Integrator。

對資料庫文件啟用文件加密

您可以從 install 目錄將資料庫文件加密。

關於這項作業

如果要將資料庫文件加密，請執行下列動作：

程序

1. 導覽至 install 目錄。
2. 導覽至 properties 目錄。
3. 開啟 customer_overrides.properties 檔。
4. 將下列字行新增至檔案：

   ```
   security.ENC_DECR_DOCS=ENC_DB
   ```
5. 儲存並關閉 customer_overrides.properties 檔。
6. 停止並重新啟動 Sterling B2B Integrator。

對檔案系統文件啟用文件加密

您可以從 install 目錄將檔案系統文件加密。

關於這項作業

如果要將檔案系統文件加密，請執行下列動作：

程序

1. 導覽至 install 目錄。
2. 導覽至 properties 目錄。
3. 開啟 customer_overrides.properties 檔。
4. 將下列字行新增至檔案：

   ```
   security.ENC_DECR_DOCS=ENC_FS
   ```
5. 儲存並關閉 customer_overrides.properties 檔。
6. 停止並重新啟動 Sterling B2B Integrator。

停用文件的文件加密

您可以從 properties 目錄停用文件加密。

關於這項作業

安裝時的預設配置為無加密。

如果要停用文件加密：

程序

1. 導覽至 install 目錄。
2. 導覽至 properties 目錄。
3. 開啟 customer_overrides.properties 檔。
4. 將 ENC_DECR_DOCS 的值更新為 NONE。 例如：

   ```
   security.ENC_DECR_DOCS=NONE
   ```
5. 儲存並關閉 customer_overrides.properties 檔。
6. 停止並重新啟動 Sterling B2B Integrator。

憑證

數位憑證

使用「IBM 金鑰管理公用程式 (iKeyman)」協助您管理數位憑證。

系統使用下列數位憑證類型：

- CA 與授信憑證 - 系統沒有其私密金鑰的數位憑證。這些憑證使用標準 DER 格式儲存。
- 系統憑證 - 其私密金鑰交由系統維護的數位憑證。這些憑證使用安全格式與私密金鑰儲存在一起。

下列是部分有關如何使用數位憑證的基本資訊：

- 每一個會交換安全文件的組織都必須擁有憑證。使用 iKeyman 來產生憑證，或者從外部產生。如需 iKeyman 的相關資訊，請參閱第 58 頁的『IBM 金鑰管理公用程式 (iKeyman)』。
- 您會與對方交換簽署與加密文件的交易夥伴，其每一個交易設定檔都必須擁有憑證。
- 組織或交易設定檔一次只能有一個作用中憑證。在雙重憑證案例中，組織可以有一對作用中憑證；一個用於簽章，一個用於加密。
- 組織或交易設定檔必須擁有作用中憑證，才能順利交換簽署與加密文件。
- 組織或交易設定檔可以多個有效憑證。
- 所有的傳輸方法都可以使用憑證來簽署您傳輸的文件。
- 憑證的金鑰長度不一定要與交易夥伴憑證的金鑰長度完全相同。
- 在設定憑證有效期限之前，建議您先閱讀並套用 Microsoft PKI Quick Guide 中的最佳作法建議。如需使用憑證的最佳作法建議相關資訊，請參閱 http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

支援的數位憑證

Sterling B2B Integrator 支援第 3 版 X.509 數位憑證。數位憑證可以是自簽或 CA 簽署。

- 自簽憑證是使用對應於憑證中公開金鑰之私密金鑰簽署的數位憑證，這表示發證者擁有對應於憑證中公開金鑰的私密金鑰。
- CA 簽署的憑證是使用由憑證管理中心維護之金鑰簽署的數位憑證。在發出憑證之前，CA 通常會評估憑證申請者，以判斷申請者是否確實是憑證中參照的憑證持有者。

CA 憑證

CA 憑證是憑證管理中心 (CA) 發出的數位憑證。CA 會針對授信主要憑證來驗證授信憑證。授信主要憑證是在憑證中建立授信鏈所依據的基礎。

信任 CA 主要憑證代表您信任該 CA 發出的所有憑證。如果您選擇不信任 CA 主要憑證，則 Sterling B2B Integrator 不會信任該 CA 發出的任何憑證。

CA 憑證包含對應於私密金鑰的公開金鑰。CA 擁有私密金鑰並用以簽署其所發出的憑證。如要驗證授信憑證，您必須先移入 CA 憑證。

一般 CA 的主要憑證內含於 Sterling B2B Integrator 所隨附 JVM 的 Java 金鑰儲存庫 (JKS) 中。如此一來，可讓使用者在建立某些權限型信任關係時，會比他們必須從 CA 網站搜尋及取得憑證來得更為容易。

在本產品中，CA 憑證與授信憑證分開儲存。

您可以透過使用者介面，移入源自下列任何來源的 CA 主要憑證：

- JKS 金鑰儲存庫中的一般 CA 主要憑證（隨附於 Sterling B2B Integrator）。
- 系統僅能辨識憑證與授信憑證。在 UI 中看不到憑證與私密金鑰。
- 從交易夥伴匯入的 SSL 憑證。
- 從外部取得的其他憑證。

視您網站的安全原則而定，也可以透過主控台移入 JKS 金鑰儲存庫中的 CA 憑證。雖然 CA 憑證是公開文件，但您必須仔細思考誰有權新增它們。別人可以惡意新增錯誤 CA 憑證，以便驗證錯誤的一般使用者憑證。

CA 憑證名稱

憑證內容不含 CA 憑證名稱。 CA 憑證名稱是從發證者相對識別名稱 (RDN) 和憑證序號建置。不過，JKS 金鑰儲存庫的憑證使用任意字串命名。

由於憑證名稱儲存在系統資料庫中，而且用來做為在 GUI 中參照憑證的別名，您可能會希望根據自己的檔案命名慣例，使用比較簡短或比較有意義的方式重新命名 CA 憑證。您可以在移入或編輯時重新命名憑證。

自簽與 CA 簽署數位憑證的優點

自簽與 CA 簽署數位憑證各有優缺點，視您的需求而定。

當您與您的交易夥伴在決定是要產生自簽憑證，還是購買 CA 簽署的憑證時，請考慮下列幾點：

- 您可以使用 Sterling B2B Integrator 輕鬆建立自簽憑證。不過，這些自簽憑證欠缺具公信力第三者的驗證。
- 使用 CA 憑證的主要優點是，憑證持有者的身分經過具公信力第三者的驗證。缺點是會有額外成本與管理工作。如果您決定使用第三者憑證，請從 CA 取得憑證。
- CA 提供集中式來源以發佈與取得憑證相關資訊，包括撤銷憑證的相關資訊。

依預設，系統信任所有 CA 憑證與應用程式產生的自簽憑證。不過，您可以指定應該信任所有或部分特定 CA 發出的憑證。您也無法明確信任交易夥伴的自簽憑證。

憑證的到期日

如果配接器與 Servlet 是用於入埠通訊，您必須監視系統憑證的到期日，以確保憑證有效。在憑證到期之前，必須以有效憑證取代它們。

系統憑證參數定義

如果配接器與 Servlet 是用於入埠通訊，您必須監視系統憑證的到期日，以確保憑證有效。在憑證到期之前，必須以有效憑證取代它們。

參數	說明
alias	儲存於 HSM 中的金鑰名稱。僅使用包含字元 a-z、A-Z、0-9 或連字號 (-)，且總長度不能大於系統 GUID 長度的別名。
certname	在資料庫中指派給系統憑證的名稱。
Certtype	要匯入的憑證類型。支援四種憑證檔類型：pkcs12、pkcs8、pem 與 keystore。Sterling B2B Integrator 僅支援使用 DES 或 3DES 加密的 pem 金鑰。 使金鑰儲存庫來列出或匯入金鑰儲存庫。
file	要匯入的檔案名稱。
keypass	Eracom 裝置其屬性的 PIN。
keystoretype	要匯入的金鑰儲存庫類型。有效值為 CRYPTOKI。
keystoreprovider	提供者類型。Eracom 是 HSM 唯一支援的提供者類型。 有效值為： • ERACOM • ERACOM.n（如果要將憑證匯入第一個位置以外的屬性）
password	憑證檔的儲存庫通行詞組。
pkcs12file	要匯入的 PKCS12 檔名。
pkcs12storepass	用來產生 PKCS12 檔的儲存庫通行詞組。
pkcs12keypass	PKCS12 檔的有效通行詞組。
storepass	金鑰儲存庫所在之 Eracom 裝置其屬性的 PIN。
systempass	系統通行詞組。

IBM 金鑰管理公用程式 (iKeyman)

IBM 金鑰管理公用程式 (iKeyman) 是 IBM SDK 中的一個元件，會產生金鑰、憑證要求，以及自簽憑證。

您可以利用 iKeyman，來建立安全通訊用的憑證，以及用來加密和解密資料。在使用 SSL 的安全傳送中，憑證可提供附加的安全等級。

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

- 憑證簽署要求 (CSR) - 透過電子郵件傳給憑證管理中心以要求 X.509 憑證的檔案。
- 金鑰憑證 - 結合 ASCII 編碼憑證和 ASCII 編碼 PKCS12 加密私密金鑰的組合。如果您使用標準格式（預設值）產生含有特定密碼的金鑰憑證，其輸出憑證在匯入至 Sterling B2B Integrator 時會發生錯誤。PKCS12 是建議的金鑰憑證格式。

如需配置和使用 iKeyman 的相關資訊，請參閱適用於 IBM SDK, Java Technology Edition 7.0.0 的 iKeyman 概觀

憑證作業

建立自簽憑證

您可以從**管理**功能表建立自簽憑證。

關於這項作業

如果要建立自簽憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**建立自簽憑證**旁的**執行！**
3. 輸入自簽憑證的**名稱**。
4. 輸入原始**組織**的名稱。
5. 選取自簽憑證的**國家/地區**或出處。
6. 針對組織中的憑證負責人，輸入聯絡**電子郵件**位址，然後按**下一步**。
7. 輸入憑證的**序號**。 序號是您想要指派給自簽憑證的號碼。
8. 輸入自簽憑證的有效天數（**持續時間**）。

   註：在 5.2.6.2 版或更新版本中，最晚到期日為 *2080* 年 *1* 月 *1* 日。輸入的任何持續時間如果導致到期日超過 2080 年 1 月 1 日，將預設為 *2080* 年 *1* 月 *1* 日。舊版中沒有上限。
9. 就您想要當做 SubjectAltName 欄位與憑證相關聯的網路介面，輸入其 **IP 位址**。
10. 就您想要當作 SubjectAltName 欄位與憑證相關聯的網路介面，輸入其 **DNS 名稱**。
11. 選取**金鑰長度**。選取下列其中一個金鑰長度：
    - 512
    - 1024
    - 2048

    註：金鑰長度 1024 提供安全性、交互作業能力與效率之間的最佳平衡。金鑰長度 2048 最安全，但也最慢，且部分應用程式可能不適用。

    註：如果您選取金鑰長度 512，也必須使用 JDK 7 SR5。JDK 7 SR7 FP1 不支援低於 1024 的金鑰長度。
12. 選取**簽署演算法**。
13. 選取**使用時驗證**選項。驗證選項如下：
    - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
    - 鑑別鏈 - 針對未自行簽署的憑證建構信任的鏈結。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
14. 選取勾選框，藉此設定**憑證簽署位元**。
15. 按**下一步**。
16. 檢閱自簽憑證相關資訊。
17. 按一下**完成**。

從交易夥伴自動取得授信憑證

「憑證擷取公用程式」會將從交易夥伴取得 SSL 憑證的程序自動化。這個取得憑證資訊的方法可讓夥伴輕易連接及儲存憑證。

關於這項作業

如果需要，可以在憑證移入系統作為 CA 或「授信」憑證之前，進行頻外安全檢查。

開始之前：

- 驗證夥伴的主機系統已啟用 SSL。
- 取得交易夥伴伺服器的主機和埠資訊。
- 如果將使用 FTPS 模式，請判定模式會是明確或隱含的。
- 配置預設 SSLCertGrabberAdapter 服務實例，以使用適當的周邊伺服器及（僅限 HTTPS）Proxy 伺服器。如需詳細資料，請參閱配接器說明文件。

如果要從交易夥伴自動取得 SSL 憑證，請執行下列動作：

程序

1. 從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 憑證擷取公用程式**。
2. 按一下**擷取夥伴憑證**旁的**執行！**
3. 選取伺服器的連線類型，然後按**下一步**。
   - FTPS
   - HTTPS
4. 輸入**主機名稱**或 **IP 位址**。
5. 輸入**埠號**。
6. 選取 FTPS 連線模式（如果您使用 HTTPS，請跳過此步驟）：
   - 明確 - 建立 FTP 連線之後進行 SSL 協議。預設值。
   - 隱含 - 建立 FTP 連線之前進行 SSL 協議。
7. 按**下一步**。 系統會嘗試連接並擷取憑證。
8. 擷取完成之後，請檢閱摘要資訊並決定要儲存哪些憑證。
9. 選取每一個憑證的編碼方法，然後按一下**儲存**。編碼格式如下：
   - BASE64 - 在標準 DER 憑證上使用 BASE64 編碼。預設值。
   - DER - 大部分應用程式接受的數位憑證標準格式。
10. 按一下**儲存**，並瀏覽至您要儲存檔案的位置。
11. 接受預設檔名，或根據您的檔案命名慣例來編輯檔名，然後按一下**儲存**。
12. 儲存之後，可以將憑證移入系統中。如果您決定將憑證移入系統中，請執行下列動作：
    a. 驗證每一個憑證是否有效且已授信。
    b. 視功能而定，將憑證移入作為 CA 或「授信」憑證。若為「憑證管理中心型信任」，您可能需要移入憑證鏈，不含一般使用者憑證。若為「直接信任」，請移入一般使用者憑證。

配置憑證摘要上的狀態資訊

依預設，當選取加上超鏈結的憑證名稱時，在摘要蹦現視窗底端會提供憑證狀態資訊。您可以併入或排除狀態資訊。由於狀態資訊為即時編譯，您可能不想併入它。

關於這項作業

VerificationOnPopupInfo 內容控制在憑證摘要中是否要顯示狀態資訊。此內容位在 ui.properties 檔中。VerificationOnPopupInfo 內容的值如下：

- True - 併入驗證資訊（預設值）
- False - 在蹦現視窗中不要編譯或顯示驗證資訊
- （任何其他值）- 併入驗證資訊

如果要避免編譯與顯示狀態資訊：

程序

1. 開啟 ui.properties 檔。
2. 將 VerificationOnPopupInfo 的值更新為 False。例如：

   ```
   VerificationOnPopupInfo=false
   ```
3. 儲存並關閉檔案。
4. 重新啟動 Sterling B2B Integrator。

配置指模顯示

除了預先計算的 SHA1 雜湊外，還可以在憑證顯示畫面、確認畫面與摘要畫面中併入額外憑證指模。雜湊計算可在產生顯示畫面時隨需應變執行。

關於這項作業

在 GUI 畫面上會顯示附加指模，但不會對訊息處理或系統通訊產生任何影響。

如果要配置系統計算及顯示附加憑證指模：

程序

1. 在 ui.properties 檔中修改這一行：

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   如果要顯示一個以上的附加雜湊，請使用逗點來分隔所有的值。例如：

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

參數	說明
hash_algorithm	要套用至憑證指模的雜湊演算法名稱。有效值為： • SHA-256 • SHA-384 • SHA-512

2. 儲存並關閉 ui.properties 檔。
3. 重新啟動 Sterling B2B Integrator。

搜尋 CA 憑證

您可以從**管理**功能表搜尋 CA 憑證。

關於這項作業

如果要搜尋 CA 憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > CA**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 完成下列其中一項，然後按一下**執行！**
   - 在**依憑證名稱**欄位的「搜尋」之下，輸入要搜尋的部分名稱或完整 CA 憑證名稱。「CA 數位憑證」頁面會列出符合搜尋準則的所有 CA 憑證。
   - 在**依英文字母順序**欄位的「列出」之下，選取**全部**或要搜尋的 CA 憑證的名稱的第一個字母。選取「全部」列出全部的 CA 憑證。「CA 數位憑證」頁面會列出符合搜尋準則的所有 CA 憑證。

檢視 CA 憑證摘要資訊

顯示憑證清單時，您可以按一下憑證名稱以檢視該憑證的摘要資訊。您可以配置系統名稱、指模及狀態。

關於這項作業

下列欄位在系統中是可以配置的。

憑證摘要欄位	說明
系統名稱	「憑證名稱」為資料庫標籤。它用於在 GUI 中參照此憑證，並將此名稱儲存在其資料庫中。 來自 JKS 金鑰儲存庫的憑證的預設名稱為任意字串。其他憑證的名稱會從發證者相對識別名稱 (RDN) 和憑證序號中建置。 移入或編輯憑證時，您可以將憑證名稱變更成更短或更容易辨識的名稱。
指模	依預設，會包含 SHA1 雜湊的資訊。如果要配置計算和顯示其他雜湊的指模資訊，請編輯 ui.properties 檔。
狀態	現行狀態的即時檢查說明憑證日期是否有效，以及憑證是否經過驗證。如果要配置該資訊在顯示時是否已計算，請編輯 ui.properties 檔。

雖然此資訊會套用至 CA 憑證的摘要資訊，但類似欄位仍然會出現在其他憑證類型的摘要與確認畫面中。

從使用者介面移入 CA 憑證

您可以從使用者介面的**管理**功能表下移入 CA 憑證。

關於這項作業

視您網站的安全原則而定，也可以透過主控台移入 JKS 金鑰儲存庫中的 CA 憑證。

開始之前，請將您從外部取得的 CA 憑證儲存至本端檔案。

如果要移入 CA 憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > CA**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**移入新憑證**旁的**執行！**
3. 選取憑證匯入方法：

匯入方法	下一步
從 JVM 匯入 - 從 JKS 金鑰儲存庫匯入	1. 從 **JVM** 按一下**匯入**。 2. 接受出現在密碼欄位中的預設密碼，然後按**下一步**。 預設金鑰儲存庫密碼是由 Sun Microsystems 提供。如果密碼欄位是空的，系統仍會使用預設密碼。
從檔案中匯入 - 匯入另存為本端磁碟機檔案的憑證	1. 從**檔案**按一下**匯入**。 2. 輸入檔名或按一下**瀏覽**以選取 CA 憑證檔。按「下一步」。 您可以忽略出現在密碼欄位中的密碼。不需要消除項目。

   可用憑證會與識別資訊摘要一起列出。依預設會選取所有的憑證。
4. 按一下每一個項目左側的勾選框，以選取或取消選取要匯入的憑證。
5. 對於每一個選取憑證，接受建議的憑證名稱，或根據您的檔案命名慣例編輯憑證名稱。
6. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證，嘗試建構上達根目錄的信任鏈。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
7. 如果您收到指出憑證與資料庫中已有憑證發生重複現象的訊息，請輸入 Y 或 N 以指示是否要匯入複製。

   此勾選僅能在單一憑證上執行。移入某個檔案的一或多個憑證時，無法執行此勾選。

由 SHA1 雜湊識別憑證，目的是判斷複製。在資料庫中可以存在一個以上的憑證副本，因為每一個副本都會移入不同的一列，並且擁有特定的物件 ID。現有憑證不會被改寫。

8. 檢閱 CA 憑證資訊。
9. 按一下**完成**。

從主控台移入 CA 憑證

將任何 CA 憑證儲存至本端檔案之後，您可以在主控台從安裝目錄移入 CA 憑證。

關於這項作業

一般 CA 憑證內含在隨附 Sterling B2B Integrator 之 JVM 裡面的 JKS 金鑰儲存庫。JKS 金鑰儲存庫位在 /install_dir/jdk/jre/lib/security/cacerts。您也可以從外部取得憑證。

如果要將憑證匯入 Sterling B2B Integrator 授信儲存庫，請修改以下指令： /install_dir/install/bin/ImportCACerts.sh (UNIX) 或 \install_dir\install\bin\ImportCACerts.cmd (Windows) 的指令。

開始之前，請將從外部取得的 CA 憑證儲存至本端檔案。

如果要在主控台移入 CA 憑證：

程序

1. 導覽至安裝目錄。
2. 導覽至 bin 目錄。
3. 輸入以下指令：

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   檔案中的所有憑證都會列出，一次一個，但下列狀況例外：
   - 未處理或列出包含對稱或私密金鑰的項目。
   - 僅處理及列出 DER 格式檔案中的第一個憑證。
4. 遵循提示，針對要匯入的任何憑證輸入 Y（不區分大小寫）。
5. 對於每一個已接受憑證，接受建議的憑證名稱，或根據您的檔案命名慣例編輯憑證名稱。
6. 如果憑證標籤與資料庫中已有標籤發生重複現象，請輸入 Y 或 N（不區分大小寫），以指出您是否要變更標籤。 雖然憑證一般不是經由標籤識別，而且資料庫容許標籤複製，但部分服務會依標籤查閱憑證。避免重複標籤，以免發生非預期的行為。
7. 如果憑證與資料庫中已有憑證發生重複現象（如憑證的 SHA1 雜湊所示），請透過 Y 或 N 指定您是否要匯入複製。

   由 SHA1 雜湊識別憑證，目的是判斷複製。在資料庫中可以存在一個以上的憑證副本，因為每一個副本都會移入不同的一列，並且擁有特定的物件 ID。現有憑證不會被改寫。

編輯 CA 憑證

您可以從**管理**功能表編輯 CA 憑證。

關於這項作業

如果要編輯 CA 憑證，請執行下列動作：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > CA**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 使用「搜尋」或「清單」來尋找您要編輯的 CA 憑證，然後按一下**執行！**
3. 在您要編輯的 **CA 憑證**旁邊，按一下**編輯**。
4. 輸入「憑證名稱」。
5. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證建構信任的鏈結。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
6. 檢閱 CA 憑證資訊。
7. 按一下**完成**。

刪除 CA 憑證

您可以從**管理**功能表刪除 CA 憑證。

關於這項作業

如果要刪除 CA 憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > CA**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**依字母順序列出**旁邊的**執行！**
3. 按一下您要刪除之 CA 憑證旁的**刪除**。

搜尋系統憑證

您可以從**管理**功能表搜尋系統憑證。

關於這項作業

如果要搜尋系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 在系統憑證中，完成下列其中一項動作，然後按一下**執行！**
   - 在**依憑證名稱**欄位的「搜尋」之下，輸入要搜尋的部分名稱或完整系統憑證名稱。「系統憑證」頁面列出包含您輸入的完整名稱或局部名稱的所有系統憑證。
   - 在**依英文字母順序**欄位的**列出**之下，選取**全部**或要搜尋的 CA 憑證的名稱的第一個字母。選取「全部」列出全部的系統憑證。「系統憑證」頁面會列出符合搜尋準則的所有系統憑證。

編輯系統憑證

您可以從**管理**功能表編輯系統憑證。

關於這項作業

如果要編輯系統憑證，請執行下列動作：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 使用「搜尋」或「清單」來尋找您要編輯的**系統憑證**，然後按一下**執行！**
3. 在您要編輯的系統憑證旁邊，按一下**編輯**。
4. 輸入**憑證名稱**。
5. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證建構信任的鏈結。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
6. 檢閱系統憑證資訊。
7. 按一下**完成**。

識別 Sterling B2B Integrator 中的系統憑證

您可以從**管理**功能表識別系統憑證。

關於這項作業

如果要識別系統憑證，請執行下列動作：

程序

1. 從**管理功能表**中，選取**部署 > 服務 > 配置**。

2. 在「清單」區段中，從**依服務類型**清單中選取適用的服務或配接器類型，然後按一下**執行！**
3. 從配置清單中，選擇配置。
4. 按一下**服務名稱**，以檢視配置資訊。
5. 檢閱憑證摘要資訊。

檢查系統憑證的到期日

如果配接器與 Servlet 是用於入埠通訊，您必須監視系統憑證的到期日，以確保憑證有效。

關於這項作業

如果要檢查系統憑證的到期日：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 如果要檢視所有的系統憑證，從按字母順序的下拉清單選取**全部**，然後按一下**執行！**
3. 選取要檢視的系統憑證名稱。 隨即顯示「憑證摘要」。
4. 在「憑證摘要」的**說明**區段中，檢閱**有效日期**欄位中提供的資訊。
5. 檢閱**狀態**區段中提供的資訊，以查看日期是否有效，以及憑證是否已驗證。

匯出 Sterling B2B Integrator 中的系統憑證

此匯出指令只適用於 Sterling B2B Integrator 系統憑證。您無法使用此指令來匯出 HSM 中的系統憑證。

關於這項作業

如果要匯出系統憑證，請輸入下列指令以及適當的參數：

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

參數	說明
keyname	所要匯出系統金鑰的索引鍵名稱。
pkcs12filename	包含所匯出資訊的檔案名稱。
pkcs12storepass	保護儲存庫的儲存庫密碼。
pkcs12keypass	保護金鑰的金鑰密碼。

刪除 Sterling B2B Integrator 中的系統憑證。

在您刪除系統憑證之前，您可以先將系統憑證的副本匯出至本端磁碟。OpsDrv、OpsKey 與 UIKey 是無法刪除的系統憑證。

關於這項作業

如果要刪除系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**依字母順序列出**旁邊的**執行！**
3. 按一下您要刪除之系統憑證旁的**刪除**。
4. 在「確認」頁面中按一下**刪除**。

移出系統憑證

如果要匯出系統憑證，您必須移出憑證。此程序僅會匯出公用憑證，不會匯出私密金鑰，提供您公用憑證以傳送給交易夥伴。

關於這項作業

如果要移出系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 使用「搜尋」或「列出」來尋找您要移出的系統憑證。
3. 針對您要移出的系統憑證，按一下其旁邊的**移出**。
4. 在**移出系統憑證**對話框中選取憑證格式，然後按一下**執行！**：
   - PKCS12 - 此選項會將數位憑證格式化為 PKCS12 檔。您也可以選擇輸入私密金鑰密碼和金鑰儲存庫密碼。
   - BASE64 - 此選項會在標準 DER 憑證上使用 BASE64 編碼。
   - DER - 大部分應用程式都接受這種數位憑證標準格式。
5. 在**檔案下載**對話框中，按一下**儲存**。
6. 在**另存新檔**對話框中，選取您要儲存憑證的位置，然後按一下**儲存**。 不支援開啟憑證的選項。您必須在作業系統中開啟憑證。如果您收到錯誤訊息：「這是無效的安全憑證檔案」，請在文字編輯器中開啟該檔案，然後刪除 -----BEGIN CERTIFICATE----- 之前的任何空白行。儲存編輯過的檔案，然後嘗試開啟檔案。
7. 在「移出系統憑證」對話框中，按一下**關閉**。 隨即顯示「系統憑證」頁面。

搜尋授信憑證

您可以從**管理**功能表搜尋授信憑證。

關於這項作業

如果要搜尋授信憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 授信**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 在「授信數位憑證」中，完成下列其中一項動作，然後按一下**執行！**：
   - 在**依憑證名稱**欄位的「搜尋」之下，輸入要搜尋的部分名稱或整個授信憑證名稱。「授信數位憑證」頁面會列出符合搜尋準則的所有授信憑證。
   - 在**依英文字母順序**欄位中「列出」之下，選取**全部**或要搜尋的授信憑證的名稱的第一個字母。「授信數位憑證」頁面會列出符合搜尋準則的所有授信憑證。

移入授信系統憑證

您可以移入授信憑證，例如從交易夥伴匯入的 SSL 憑證，或其他外部憑證。

關於這項作業

授信憑證可能產生自下列來源：

- 從交易夥伴匯入的 SSL 憑證
- 從外部取得的其他憑證

開始之前，請將授信系統憑證儲存至您本端電腦上的檔案。

如果要移入授信系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 授信**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**移入新憑證**旁的**執行！**
3. 輸入**檔名**或按一下**瀏覽**以選取授信憑證的檔案名稱，然後按**下一步**。
4. 輸入**憑證名稱**。
5. 驗證您要移入的授信憑證名稱。 對於每一個您選取的憑證，「憑證名稱」欄位都會顯示建議名稱，並於其後提供憑證中的識別資訊摘要。您可以根據檔案命名慣例變更名稱。
6. 如果您選取的檔案中擁有一個以上的授信憑證，請選取每一個憑證左側的勾選框以移入每一個憑證。
7. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證，嘗試建構上達根目錄的信任鏈。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
   - CRL 快取 - 控制是否在每次使用系統憑證時查閱「CRL 快取」。
8. 檢閱授信憑證資訊。

9. 按一下**完成**。

編輯授信憑證

您可以從**管理**功能表編輯授信憑證。

關於這項作業

如果要編輯授信憑證，請執行下列動作：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 授信**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 使用「搜尋」或「清單」來尋找您要編輯的授信憑證，然後按一下**執行！**
3. 按一下您要編輯之授信憑證旁邊的**編輯**。
4. 輸入**憑證名稱**。
5. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證，嘗試建構上達根目錄的信任鏈。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
   - CRL 快取 - 控制是否在每次使用系統憑證時查閱「CRL 快取」。
6. 檢閱憑證資訊。
7. 按一下**完成**。

刪除授信系統憑證

您可以從**管理**功能表下刪除授信系統憑證。

關於這項作業

如果要刪除授信系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 授信**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**依字母順序列出**旁邊的**執行！**
3. 按一下您要刪除之授信憑證旁的**刪除**。

匯入 PKCS12 系統憑證

您可以匯入 PKCS12 系統憑證。

關於這項作業

如果要匯入 PKCS12 系統憑證，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入：

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

移入 PKCS12 系統憑證

將 PKCS12 系統憑證儲存至本端電腦上的檔案之後，您可以從**管理**功能表下移入 PKCS12 系統憑證。

關於這項作業

開始之前，您必須將 PKCS12 系統憑證儲存至您本端電腦上的檔案。

如果要移入 PKCS12 系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 在「系統憑證」頁面中，按一下 **PKCS12 憑證**旁邊「移入」之下的**執行！**
3. 輸入 PKCS12 **憑證名稱**。
4. 輸入**私密金鑰密碼**。 這是用來加密 PKCS12 憑證的密碼。
5. 輸入**金鑰儲存庫密碼**。 這是 PKCS12 物件的密碼。它可能與私密金鑰密碼相同。
6. 輸入**檔名**或按一下**瀏覽**以選取 PKCS12 憑證的檔案名稱，然後按**下一步**。
7. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證建構信任的鏈結。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
8. 檢閱 PKCS12 系統憑證資訊。
9. 按一下**完成**。

匯入 Pem 系統憑證

您可以匯入使用 DES 或 3DES 加密的 pem 系統憑證。

關於這項作業

僅支援 DES 或 3DES 加密的 pem 金鑰。

如果要匯入 pem 系統憑證，請執行下列動作：

程序

1. 導覽至 /*install_dir*/install/bin。
2. 輸入：

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

匯入金鑰系統憑證

您可以匯入金鑰系統憑證。

關於這項作業

如果要匯入金鑰系統憑證，請執行下列動作：

程序

1. 導覽至 /*install_dir*/install/bin。
2. 輸入：

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

匯入金鑰儲存庫系統憑證

您可以在 HSM 上產生金鑰儲存庫系統憑證。

關於這項作業

如果要在 HSM 上產生金鑰儲存庫系統憑證，請執行下列動作：

程序

1. 導覽至 /*install_dir*/install/bin。
2. 輸入：

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

移入金鑰系統憑證

將金鑰系統憑證儲存至本端電腦上的檔案之後，您可以從**管理**功能表下移入金鑰系統憑證。

關於這項作業

開始之前，請將金鑰系統憑證儲存至您本端電腦上的檔案。

如果要移入金鑰系統憑證：

程序

1. 請選擇下列其中一種方式：
   - 如果您使用 Sterling B2B Integrator，請從**管理功能表**中，選取**交易夥伴 > 數位憑證 > 系統**。
   - 如果您使用 AS2 Edition，請從 **AS2 管理**功能表中，選取**憑證**。
2. 按一下**金鑰憑證**旁邊的**執行！**
3. 輸入**憑證名稱**。

4. 輸入**私密金鑰密碼**。 這是用來加密私密金鑰的密碼。
5. 輸入**檔名**或按一下**瀏覽**以選取金鑰憑證的檔案名稱，然後按**下一步**。
6. 選取**使用時驗證**選項，然後按**下一步**。驗證選項如下：
   - 有效性 - 驗證憑證有效期限中的日期是否仍有效。如果日期無效，則不會使用該憑證。
   - 鑑別鏈 - 針對未自行簽署的憑證建構信任的鏈結。如果無法使用有效的憑證來建構信任的鏈結，則不會使用該憑證。如果憑證已自行簽署，此選項只會驗證憑證簽章。
7. 檢閱金鑰憑證資訊。
8. 按一下**完成**。

線上憑證狀態通訊協定 (OCSP)

Sterling B2B Integrator 中的線上憑證狀態通訊協定 (OCSP) 支援

「線上憑證狀態通訊協定 (OCSP)」是一組 ASN.1 定義的資料結構，用於要求及接收憑證撤銷狀態的相關資訊。這些資料結構可由原則中的許多傳輸通訊協定傳送及接收。實際上使用 HTTP。

OCSP 用戶端可傳送問題及處理回應。OCSP 回應者可回答問題及產生回應。

OCSP 用戶端功能

OCSP 用戶端實作包含用於管理 OCSP 回應者相關資訊的資料結構、用於產生 OCSP 要求的功能、用於處理 OCSP 回應的功能，以及用於傳輸 OCSP 要求和接收 OCSP 回應的功能。

OCSP 用戶端實作包含：

- 用於管理 OCSP 回應者相關資訊的資料結構
- 用於產生 OCSP 要求的功能
- 用於處理 OCSP 回應的功能
- 用於傳輸 OCSP 要求及接收 OCSP 回應的功能

Sterling B2B Integrator 如何執行 OCSP 檢查

Sterling B2B Integrator 中憑證的 OCSP 檢查是在 Sterling B2B Integrator 中的 OCSP 檢查實作為內部系統 API 一部分時決定的，這些 API 供服務用來從資料庫中取得憑證和金鑰。

關於這項作業

當呼叫方法來從資料庫中封裝憑證和金鑰的物件取得這些憑證和金鑰時，Sterling B2B Integrator 會執行 OCSP 檢查。

下列步驟說明如何在 Sterling B2B Integrator 中實作 OCSP 檢查：

程序

1. 系統會檢查封裝憑證的物件，以判定是否啟用 OCSP 檢查。這可讓系統在沒有其他資料庫呼叫的情況下，決定是否嘗試 OCSP 檢查。
2. 如果已啟用 OCSP 檢查，系統會從憑證取得已編碼的發證者名稱。

3. 系統會使用 SHA1 將已編碼的發證者名稱進行雜湊運算。
4. 系統會嘗試尋找系統中所配置，且有一個名稱其雜湊符合憑證雜湊的憑證管理中心。
5. 如果找不到憑證管理中心，則不會執行檢查。
6. 如果找到憑證管理中心，系統會檢查該憑證管理中心的 OCSP 原則。如果原則允許或需要 OCSP 檢查，請參閱 CERT_AUTHORITY 表格，以取得相關資訊。系統會嘗試尋找憑證管理中心的 OCSP 回應者。
7. 如果找不到憑證管理中心的 OCSP 回應者，則會發生下列其中一種情況：
   - 如果憑證管理中心原則設為一律檢查，則會擲出異常狀況且檢查會失敗。
   - 如果憑證管理中心原則設為只在配置回應者時檢查，則不會執行檢查。
   - 如果找到憑證管理中心的 OCSP 回應者，則會嘗試 OCSP 檢查。

資料庫表格

新增 CERT_AUTHORITY 和 OCSP_RESPONDER 以管理 OCSP 相關資訊。

已新增兩個資料庫表格，以管理 OCSP 相關資訊：

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

CERT_AUTHORITY 表格維護憑證管理中心相關資訊。

直欄	類型	說明
OBJECT_ID	VARCHAR (255)	這是構成記錄唯一 ID 的 GUID。此為主要索引鍵。不能是空值。
NAME	VARCHAR (255)	記錄的名稱。接受空值。
CREATE_DATE	DATETIME	記錄的建立日期。
MODIFIED_DATE	DATETIME	記錄的前次修改日期。
MODIFIED_BY	VARCHAR(255)	記錄修改者相關資訊。
ISSUER_NAME	BLOB	從其憑證取得之憑證管理中心的 RDN。
HASH_ALG	VARCHAR(128)	用於計算名稱與金鑰雜湊的雜湊演算法。僅支援 SHA1。
RDN_HASH	VARCHAR(255)	從憑證管理中心的憑證取得之 DER 編碼發證者 RDN 的 BASE64 編碼 SHA1。此欄已索引化。
KEY_HASH	VARCHAR(255)	在發證者憑證中，已編碼公開金鑰的 BASE64 編碼 SHA1 雜湊
CERT_OID	VARCHAR(255)	在 CA_CERT_INFO 表格中，憑證管理中心其憑證的 OBJECT_ID。在資料庫中每一個憑證管理中心都必須具有 CA 憑證。不接受空值。

直欄	類型	說明
OCSP_POLICY	VARCHAR(128)	憑證管理中心的 OCSP 原則。這由兩個使用逗點分隔的值所組成。這些值說明何時使用 OCSP 與檢查哪些內容。 可能值如下： **OCSP_When** • never - 永不使用 OCSP • resp - 如果在提出要求時已配置回應者，僅限使用 OCSP • always - 提出要求時一律使用 OCSP。這需要配置回應者，如果未配置回應者，將導致憑證檢查失敗 **OCSP_What** • none - 永不檢查任何憑證 • end-user - 只檢查一般使用者憑證 • both - 同時檢查一般使用者與中繼憑證。目前不支援 • 此直欄不接受空值
CRL_POLICY	VARCHAR(128)	目前未使用。

OCSP_RESPONDER

OCSP_RESPONDER 表格維護 OCSP 回應者的相關資訊。

直欄	類型	說明
OBJECT_ID	VARCHAR (255)	這是構成記錄唯一 ID 的 GUID。此為主要索引鍵。不能是空值。
NAME	VARCHAR (255)	記錄的名稱。接受空值。
CREATE_DATE	DATETIME	記錄的建立日期。
MODIFIED_DATE	DATETIME	記錄的前次修改日期。
MODIFIED_BY	VARCHAR(255)	記錄修改者相關資訊。
ISSUER_NAME	BLOB	從其憑證取得之憑證管理中心的 RDN。
HASH_ALG	VARCHAR(128)	用於計算名稱與金鑰雜湊的雜湊演算法。僅支援 SHA1。
RDN_HASH	VARCHAR(255)	從憑證管理中心的憑證取得之 DER 編碼發證者 RDN 的 BASE64 編碼 SHA1。此欄已索引化。
KEY_HASH	VARCHAR(255)	在發證者憑證中，已編碼公開金鑰的 BASE64 編碼 SHA1 雜湊
CERT_OID	VARCHAR(255)	在 CA_CERT_INFO 表格中，憑證管理中心其憑證的 OBJECT_ID。在資料庫中每一個憑證管理中心都必須具有 CA 憑證。不接受空值。

直欄	類型	說明
CACHE_TTL	VARCHAR(64)	接受 OCSP 回應在內部回應快取中的存活時間（以秒為單位） 如果此欄為空值，OCSP 回應將只能快取 1 秒，這在實際上完全沒意義。
TRANS_PROF_OID	VARCHAR(255)	在 GIS 資料庫中，設定檔的 OBJECT_ID。您必須為 OCSP 回應者建立設定檔，其中包括回應者的正確 URL。
COMM_BP	VARCHAR(255)	用來與 OCSP 回應者進行通訊的商業程序名稱。這必須是執行 HTTP 通訊的商業程序。商業程序中的服務，必須分別配置成在傳送與接收時，都不需要或不呈現 HTTP 標頭。可以使用，也建議使用系統隨附的處理程序 HTTPClientSend。
COMM_WAIT	VARCHAR(24)	在推斷發生錯誤之前等待與 OCSP 回應者進行通訊的秒數。

OCSP 配置

當您配置系統來使用 OCSP 時，您可以建立不限數量的憑證管理中心與回應者。

關於這項作業

配置系統時，您可以建立任意數目的憑證管理中心與回應者。

如果要配置系統使用 OCSP：

程序

1. 針對發出你所需要之憑證以便透過 OCSP 移入 Sterling B2B Integrator 的憑證管理中心，檢查其憑證以驗證是否為 CA 憑證。
2. 列出系統中的 CA 憑證，並針對您剛安裝的憑證取得其物件 ID。
3. 如果憑證管理中心的 OCSP 回應簽署憑證，不同於憑證管理中心的發出憑證，請將憑證管理中心的 OCSP 回應簽署憑證，當作授信憑證移入 Sterling B2B Integrator。

   註：在 5.2.4.2 及更高版本中，您可以將發出回應端憑證的主要憑證當作 CA 移入，而不是將回應端憑證當作「授信憑證」移入。因為回應端憑證經常變更，在更換為有效的憑證之前，視 CA 而定，可能會造成 OCSP 失敗。從現在起，最好的作法是您應該一律移入主要憑證，因為它們很少變更。不過，仍會繼續容許這兩種類型。
4. 如果您已移入其他的 OCSP 簽署憑證，請列出系統中的 CA 憑證，並針對您剛安裝的憑證取得其物件 ID。
5. 跳至 Sterling B2B Integrator 安裝的 bin 目錄。
6. 必要時請啟動資料庫。
7. 啟動 bash 或 sh shell。
8. 尋找檔案 tmp.sh

9. 使用類別 com.sterlingcommerce.security.ocsp.SCICertAuthority 中的公用程式來建立憑證管理中心。
10. 使用類別 com.sterlingcommerce.security.ocsp.SCIOCSPResponder 中的公用程式來建立 OCSP 回應者
11. 更新憑證管理中心的憑證或個別憑證以啟用 OCSP。公用程式 com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo 會為管理中心配置所有的授信與系統憑證。公用程式 com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo 會配置 1 個系統憑證。公用程式 com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo 會配置 1 個授信憑證。

OCSP 配置 Script

OCSP 緊急修復程式已隨附下列 Script 來執行 OCSP 配置公用程式。每一個 Script 都有 UNIX/Linux 和 Windows 版本。這些 Script 採用相同的指令行引數作為其呼叫的公用程式。這些 Script 位於產品安裝的 bin 目錄中。基本上，本節只是重複說明 Script 的指令行引數的相關資訊。

ManageCertAuthority.sh 和 ManageCertAuthority.cmd

引數	說明
-a、-r、-d	要執行的作業： -a add -l list -d delete -l 選項不使用其他引數。 -d 選項使用單一引數：所要刪除記錄的物件 ID
名稱	憑證管理中心的名稱。需要與 -a 搭配使用。
Modified_by	修改或建立身分的使用者。需要與 -a 搭配使用。
Hash_alg	憑證管理中心的雜湊演算法。僅支援 "SHA1" 值。需要與 -a 搭配使用。
Certificate_id	與憑證管理中心相關聯之 CA 憑證的物件 ID。需要與 -a 搭配使用。

OCSP_policy	憑證管理中心的 OCSP 原則字串。這是有關 CERT_AUTHORITY 表格的一節中所說明的逗點區隔字串。需要與 -a 搭配使用。 如果是字串的第一個元素，允許下列項目： • never - 永不使用 OCSP • resp - 只有在提出要求時配置了回應者的情況下才使用 OCSP • always - 提出要求時一律使用 OCSP。這需要配置回應者，如果未配置回應者，將會導致憑證檢查失敗 如果是字串的第二個元素，允許下列項目： **OCSP 內容** • none - 永不檢查任何憑證 • end-user - 只檢查一般使用者憑證 • both - 同時檢查一般使用者與中繼憑證。目前不支援。 範例： • never,none • always,end-user
Crl_policy	憑證管理中心的 CRL 原則字串。需要與 -a 搭配使用。需要提供此引數的值，但目前並未使用。可接受 "None"。
Object_ID	建立此記錄時所要使用的物件 ID。選擇性與 -a 搭配使用。

ManageOCSPResponder.sh 和 ManageOCSPResponder.cmd

引數	說明
-l	取得目前配置的 OCSP 回應者清單。 此選項不使用其他引數。
-d	以針對回應者配置資料提供的物件 ID，刪除所配置的 OCSP 回應者。 此選項使用 object_id 作為其他引數。
-u2	以憑證管理中心憑證的公開金鑰及憑證管理中心憑證的主旨 DN 之相關正確資訊，更新資料庫中的現有記錄。 這必須針對「憑證管理中心」和「OCSP 回應者」的所有現有記錄執行，或者您需要刪除並重建記錄，以在資料庫取得適當資訊。 此選項使用 object_id 作為其他引數。

-a	針對要用於檢查所提供憑證管理中心發出之憑證狀態的新「OCSP 回應者」，新增配置資料。 其他引數為 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	（需要與 -a 搭配使用）憑證管理中心的名稱。
modified_by	（需要與 -a 搭配使用）修改或建立身分的使用者。
hash_alg	（需要與 -a 搭配使用）憑證管理中心的雜湊演算法。僅支援 "SHA1" 值。
authority_cert_oid	（需要與 -a 搭配使用）與憑證管理中心相關聯之 CA 憑證的物件 ID。
response_signing_cert_oid	（需要與 -a 搭配使用）OCSP 服務提供者用來簽署提供憑證狀態的回應之憑證的物件 ID。此憑證必須新增至「CA 數位憑證」儲存庫或「授信數位憑證」儲存庫中。這是憑證出現在儲存庫中的「系統憑證 ID」。
resp_signing_cert_in_ca_store	（需要與 -a 搭配使用）旗標，指出是否在 Sterling B2B Integrator 的「CA 數位憑證儲存庫」中找到 response_signing_cert_oid 引數的前一個值。
cache_ttl	（需要與 -a 搭配使用）內部快取中 OCSP 回應的存活時間（秒）。
trans_prof_oid	（需要與 -a 搭配使用）配置來與 OCSP 回應者通訊之傳輸的物件 ID。
comm_bp	（需要與 -a 搭配使用）用來與 OCSP 回應者通訊的商業程序名稱。這必須是執行 HTTP 通訊的商業程序。商業程序中的服務，必須分別配置成在傳送與接收時，都不需要或不呈現 HTTP 標頭。建議使用系統提供的 HTTPClientSend 程序。
comm_wait	（需要與 -a 搭配使用）在推斷發生錯誤前，等待與回應者通訊的秒數。
send_nonce	（需要與 -a 搭配使用）指出 NONCE 值是否傳送給 OCSP 服務。NONCE 值用來防止受到部分 OCSP 提供者的重播攻擊。
require_nonce	（需要與 -a 搭配使用）指出伺服器是否應要求 OCSP 服務在回應中提供 NONCE 值。
object_id	（選擇性與 -a 搭配使用）建立此記錄時所要使用的物件 ID。

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

此公用程式會在資料庫中設定單一系統憑證的 OCSP 資訊

引數	說明
-o、-n	如何解譯第二個引數： -o object_ID -n name
Object_ID/Name	由引數 1 所決定之憑證管理中心的物件 ID 或名稱。

SetSystemCertOCSPInfo.sh 和 SetTrustedCertOCSPInfo.cmd

此公用程式會在資料庫中設定單一系統憑證的 OCSP 資訊

引數	說明
-o、-n	如何解譯第二個引數： -o object_ID -n name
Object_ID/Name	由引數 1 所決定之憑證管理中心的物件 ID 或名稱。

執行 OCSP Script

下列範例顯示如何執行 OCSP 配置 Script。這些 Script 假設您已移入憑證管理中心的 CA 憑證、已啟動資料庫、已位於 Sterling B2B Integrator 安裝架構的 bin 目錄中，並且已取得 bin 目錄中的 tmp.sh 檔。

關於這項作業

從憑證管理中心取得 CA 憑證的物件 ID 之後，請在 Sterling B2B Integrator 的**管理功能表**中，選取**交易夥伴 > 數位憑證-CA**。選取憑證。這時會出現含有憑證資訊的「憑證摘要」對話框，包括其物件 ID。

請完成下列步驟來執行 OCSP Script。如需 OCSP Script 指令的完整清單，請參閱 第 77 頁的『OCSP 配置 Script』。

程序

1. 執行類似如下的指令，以在系統中建立憑證管理中心：

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

2. 在建立憑證管理中心及建立與 OCSP 回應者通訊的設定檔之後，請執行類似如下的指令，以在系統中建立 OCSP 回應者：

   ```
   ./ManageOCSPResponder.sh -a CertAuth_TestOCSP admin SHA1
   "kenny:node1:13727b3f8e4:29762" "kenny:node1:13727275fd9:40698" false （使用
   true，表示移入的簽署憑證
   與回應憑證相同，亦即，在步驟 3 中移入
   憑證管理中心） "2400" "14ffd4a0:1371823040d:-77c8"
   HTTPClientSend 3600 false false
   ```

3. 執行類似如下的指令，以列出系統中的所有憑證管理中心：

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

傳回每一個憑證管理中心顯示的輸出：

```
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. 使用類似如下的指令，以對憑證管理中心發出的所有授信憑證和系統憑證啟用 OCSP：

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

OCSP 檢查邏輯

下列步驟說明 Sterling B2B Integrator 中的 OCSP 檢查邏輯。如果憑證狀態為正常，表示 OCSP 檢查成功。否則，表示失敗。

程序

1. 如果找到存活時間未過期的現有回應，則會使用該回應作為 OCSP 回應。
2. 如果在快取中找不到現有回應或快取中回應的存活時間已過期，則會建立 OCSP 要求。
3. 如果系統建立 OCSP 要求，它會啟動針對 OCSP 回應者配置的商業程序來傳送要求及取得回應。如果回應者是配置為要傳送一個 Nonce 值，則要求將包括 Nonce 值。
4. 如果商業程序順利完成，系統會嘗試將其主要文件剖析為 OCSP 回應。用來傳送 OCSP 要求及接收 OCSP 回應的商業程序，會從回應中除去 HTTP 標頭。
5. 如果主要文件可以剖析為 OCSP 回應，系統會檢查回應的狀態。
6. 如果回應狀態指出要求產生有效的回應，系統會嘗試使用配置給 OCSP 回應者的憑證，來驗證 OCSP 回應中的簽章。
7. 如果已驗證簽章且回應者配置為需要 Nonce，系統會嘗試從回應中取得並檢查 Nonce。
8. 如果已透過其他所有驗證，系統會尋找建構及傳送要求的憑證之憑證狀態資訊。
9. 如果找到狀態資訊，表示系統已針對憑證的現有 OCSP 回應更新內部快取。

聯邦資訊存取安全標準 (FIPS)

美國聯邦資訊處理標準 (FIPS) 140-2

為符合 FIPS 200 安全需求，應用程式必須使用「加密模組驗證程式」所認證的加密模組，並且符合 FIPS 140-1 或 140-2。

以下是應用程式使用已驗證的加密法之最低需求：

- 所有加密作業（包括金鑰產生）都必須由已驗證的加密模組執行。
- 僅允許已核准的安全功能。
- 僅允許已核准的金鑰建立技術。

FIPS 140-2 與 Sterling B2B Integrator

Certicom Government Service Edition (GSE) 是 Sterling B2B Integrator 隨附的 FIPS 140-2 Level 1 認證的加密模組。GSE 是以 Java 撰寫的低階加密工具箱，實作各種安全功能，包括未核准的安全功能。

當在 FIPS 模式中時，請執行下列作業：

- 啟用 GSE FIPS 狀態機器並呼叫開機自我測試。
- 將核心系統的加密函數呼叫集中到 GSE。

在安裝期間啟用 FIPS

在新的安裝期間，當詢問您是否要以 FIPS 模式執行時，請選取 TRUE。

手動啟用 FIPS 模式

在安裝 Sterling B2B Integrator 之後，您可以手動啟用 FIPS 模式。在開始之前，請先驗證您擁有在 FIPS 模式下作業的授權，然後才啟用它。啟動時會檢查您的授權，如果 FIPS 模式已啟用但未獲授權，則不會啟動。

關於這項作業

如果要手動啟用 FIPS 模式，請執行下列動作：

程序

1. 導覽至 /*install_dir*/properties/。
2. 尋找 security.properties 檔。
3. 在文字編輯器中開啟 security.properties 檔。 如果您變更了 security.properties 檔，請務必對 security.properties.ini 檔進行相同的變更。這可防止您的自訂設定遭到改寫。您應該使用安全內容檔來自訂 FIPS，而不是直接編輯內容檔。
4. 指定下列配置：FIPSMode=true
5. 儲存並關閉 security.properties 檔。
6. 重新啟動 Sterling B2B Integrator。必須如此系統才能辨識這些變更。

停用 FIPS 模式

您可以手動停用 FIPS 模式。

關於這項作業

如果要手動停用 FIPS 模式：

程序

1. 導覽至 /*install_dir*/properties/。
2. 尋找 security.properties 檔。
3. 在文字編輯器中開啟 security.properties 檔。
4. 指定下列配置：FIPSMode=false
5. 儲存並關閉 security.properties 檔。
6. 重新啟動 Sterling B2B Integrator。 必須如此系統才能辨識這些變更。

Proxy 伺服器

Proxy 伺服器

Proxy 伺服器加強系統安全。

配置 HTTP Proxy 伺服器

您可以從**管理**功能表配置 HTTP Proxy 伺服器。

關於這項作業

如果要配置 HTTP Proxy 伺服器：

程序

1. 從**管理功能表**中，選取**作業** > **Proxy 伺服器**。
2. 按一下**新增**。
3. 輸入 Proxy 伺服器的**名稱**。
4. 選取 **HTTP** 為 **類型**。
5. 輸入**主機**名稱。 IPV6 位址應以方括弧括住。
6. 輸入**埠號**。
7. 輸入**重試次數**。
8. 按**下一步**。
9. 如果您想要求使用者進行基本鑑別 (BA)：
   - 選取**是**，然後按**下一步**。
   - 如果「否」（預設值），按一下**下一步**，然後跳至步驟 13。
10. 輸入**授權使用者 ID**。
11. 輸入**授權密碼**。
12. 按**下一步**。
13. 檢閱「Proxy 伺服器設定」。
14. 按一下**完成**。

配置 SSP Proxy 伺服器

您可以從**管理**功能表配置 SSP Proxy 伺服器。

關於這項作業

如果要配置 SSP Proxy 伺服器：

程序

1. 從**管理功能表**中，選取**作業** > **Proxy 伺服器**。
2. 按一下**新增**。
3. 輸入 Proxy 伺服器的**名稱**。
4. 選取 **SSP** 為 **類型**。
5. 輸入**主機**名稱。 IPV6 位址應以方括弧括住。
6. 輸入**埠號**。
7. 輸入**重試次數**。
8. 按**下一步**。
9. 在「需要對使用者進行基本鑑別 (BA) 嗎？」選取「是」或「否」。
10. 在「需要 SSL 嗎？」選取「是」或「否」。
11. 按**下一步**。
12. 如果您為此使用者選取基本授權，您必須輸入**授權使用者 ID** 與**授權密碼**，然後按**下一步**。 如果不需要此授權，此頁面便不會顯示。
13. 如果您在需要 SSL 方面選取「是」，則您必須選取**密碼強度**、**CA 憑證**與**金鑰憑證**，然後按**下一步**。 如果不需要 SSL，此頁面便不會顯示。
14. 按**下一步**。
15. 檢閱「Proxy 伺服器設定」。
16. 按一下**完成**。

配置 Proxy 伺服器以使用 SSL

您可以建立或匯入 SSL 憑證，並於適當的配接器配置中，將**使用 SSL** 欄位設定成**必須**，以搭配使用 SSL 與 SSP Proxy 伺服器配置。

關於這項作業

如果您決定搭配使用 SSL 與 SSP Proxy 伺服器配置，您必須：

程序

1. 建立 SSL 憑證或從您在 Sterling B2B Integrator 中的憑證管理中心匯入憑證。
2. 在適當的配接器配置中，將**使用 SSL** 欄位設定成**必須**。

編輯 Proxy 伺服器

您可以從**管理**功能表編輯 Proxy 伺服器配置。

關於這項作業

如果要編輯 Proxy 伺服器配置，請執行下列動作：

程序

1. 從**管理功能表**中，選取**作業** > **Proxy 伺服器**。
2. 針對您要編輯的 Proxy 伺服器，按一下**編輯**。

3. 依照需要來更新欄位。
4. 按**下一步**。
5. 檢閱「Proxy 伺服器設定」。
6. 按一下**完成**。

刪除 Proxy 伺服器

關於這項作業

刪除 Proxy 伺服器配置可能會造成 Sterling B2B Integrator 部分功能發生錯誤。在沒有特定的 Proxy 伺服器配置時，您可能需要重新配置特定的配接器與服務以使其適當運作。

如果要編輯 Proxy 伺服器配置，請執行下列動作：

程序

1. 從**管理功能表**中，選取**作業** > **Proxy 伺服器**。
2. 對您要編輯的 Proxy 伺服器按一下**刪除**。
3. 檢閱「Proxy 伺服器設定」。
4. 按一下**刪除**。

SSL

關於在 Sterling B2B Integrator 中實作 SSL

Secure Sockets Layer (SSL) 提供經由網際網路的安全通訊。它同時使用對稱和非對稱加密法。

SSL 安全通訊協定在 Sterling B2B Integrator 中提供伺服器鑑別和用戶端鑑別：

- 伺服器鑑別在用戶端連接至伺服器時執行。起始信號交換後，伺服器會將其數位憑證傳送給用戶端。用戶端驗證伺服器憑證或憑證鏈。
- 用戶端鑑別會在伺服器於信號交換期間將憑證申請傳送給用戶端時執行。如果用戶端憑證或憑證鏈已驗證，且憑證驗證訊息已驗證，則信號交換會進一步繼續進行。
- 執行選擇性的其他鑑別，方法如下：從可取得伺服器的完整網域名稱的反向網域名稱伺服器 (DNS) 查閱中，針對伺服器的完整網域名稱檢查憑證中的通用名稱。

信任類型

Sterling B2B Integrator 對於 SSL 憑證支援兩種信任類型：

- CA 信任 - 以主要憑證為基處的階層式信任，用來發行其他憑證。這是標準的 SSL 憑證信任模型。
- 直接信任 - 自簽憑證的直接信任假設透過安全頻外機制配送。直接信任和自簽憑證不屬於 SSL 標準，但常用於某些交易社群。

SSL 憑證

如果要使用 SSL 進行通訊，請配置相關系統以支援伺服器鑑別或主從式鑑別。如果要針對伺服器執行鑑別，您必須具備主要憑證管理中心 (CA) 的憑證，以及在憑證鏈中的中繼憑證集，如果伺服器使用自簽憑證，則需一份自簽憑證。

如果要支援主從式鑑別，您需要 CA 或自簽憑證及系統憑證。

您可以將憑證簽署要求 (CSR) 提供給 CA，從授信的 CA 取得 SSL 憑證。SSL 憑證連結公開金鑰和 SSL 伺服器或用戶端。

如果您計劃使用主從式鑑別，請配置系統憑證。您可以使用下列方法來建立系統憑證：

- 移入現有的金鑰憑證檔案或 PKCS12 檔案
- 產生自簽系統憑證
- 使用「金鑰管理公用程式 (iKeyman)」來產生 CSR，並從 CA 取得憑證。如需 iKeyman 的相關資訊，請參閱第 58 頁的『IBM 金鑰管理公用程式 (iKeyman)』。

密碼組合

使用 Sterling B2B Integrator 之前，應先檢閱預先定義的可用密碼清單，並根據您公司的安全需求加以自訂。

IBM SDK, Java Technology Edition 第 7 版密碼組合可在這裡找到：http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html。如需 Sterling B2B Integrator 所支援的其他 JDK，請參閱 JDK 供應商說明文件，以取得支援的密碼組合清單。

密碼強度是在 `security.properties` 或 `customer_overrides.properties` 中配置。可用的密碼組合層次如下：

- AllCipherSuite（使用者介面選項是**全部**）- 包含「弱」和「強」中所列的每一項。
- WeakCipherSuite（使用者介面選項是**弱**）- 新增您想與 Sterling B2B Integrator 搭配使用之支援的弱密碼組合
- StrongCipherSuite（使用者介面選項是**強**）- 新增您想與 Sterling B2B Integrator 搭配使用之支援的強密碼組合
- CipherSuiteDefault（5.2.6 版和更新版本所提供）- 依預設，含有一部分的 IBM JDK7 支援密碼。如果 WeakCipherSuite 和 StrongCipherSuite 是空的，會使用此項。

用於 SSL 的用戶端配接器

FTP 用戶端配接器、HTTP 用戶端配接器及 Sterling Connect:Direct® FTP+ 要求端配接器（搭配 Secure+ 選項）都支援 SSL。

下列用戶端配接器支援 SSL：

- FTP 用戶端配接器
- HTTP 用戶端配接器
- Sterling Connect:Direct FTP+ 要求端配接器（搭配 Secure+ 選項）

可在交易夥伴設定檔中或針對配接器設定 SSL 的參數。若是 FTP 用戶端配接器，這些參數是設定在「FTP 用戶端開始階段作業」服務中。若是 HTTP 用戶端配接器，這些參數是設定在「HTTP 用戶端開始階段作業」服務中。設定在「開始階段作業」服務中的參數會置換交易夥伴設定檔中的設定。

下表中的參數從用戶端視景控制 SSL。請參閱您配置的特定配接器或服務的說明文件。

參數	說明
SSL	決定 SSL Socket 協議。
CACertificateId (trusted_root)	授信 CA 公用憑證的清單。在程序資料中，此參數是顯示為物件 ID。
CipherStrength	對於流經 Socket 連線的資料套用的加密層次。
SystemCertificateId	請從可用的系統憑證清單中選取。此憑證向伺服器確認用戶端身分。

用於 SSL 的伺服器配接器

FTP 伺服器配接器、HTTP 伺服器配接器、Sterling Connect:Direct 伺服器配接器（搭配 Secure+ 選項）及 SMTP 傳送配接器都支援 SSL。

下列伺服器配接器支援 SSL：

- FTP 伺服器配接器
- HTTP 伺服器配接器
- Sterling Connect:Direct 伺服器配接器（搭配 Secure+ 選項）
- SMTP 傳送配接器

下表中的參數從伺服器視景控制 SSL。請參閱您配置的特定配接器或服務的說明文件。

參數	說明
SSL	SSL 是否作用中。
金鑰憑證通行詞組	保護伺服器金鑰憑證的密碼。此通行詞組由內部系統使用，以起始設定 SSL 程式庫。
CipherStrength	用來加密資料的演算法強度。
金鑰憑證（系統儲存庫）	用於伺服器鑑別的私密金鑰和憑證。
CA 憑證	使用的憑證（若有的話），以驗證用戶端憑證。

移入憑證

如果要支援主從式鑑別，您需要 CA 或自簽憑證及系統憑證。

關於這項作業

您可以在 CA 憑證儲存庫移入 CA 憑證或自簽憑證，方法如下：從**管理功能表**中，選取**交易夥伴** > **數位憑證** > **CA** > **移入新憑證**。

建立測試用的自簽憑證

針對測試，您可以使用自簽憑證。可在 Sterling B2B Integrator 中產生和管理自簽憑證。

關於這項作業

如果要建立自簽憑證：

程序

1. 選取**交易夥伴** > **數位憑證** > **系統憑證** > **建立自簽憑證**。
2. 建立之後，尋找它並將其移出至檔案。
3. 將憑證移回 Sterling B2B Integrator 作為 CA 憑證，方法如下：選取**交易夥伴** > **數位憑證** > **CA** > **移入新憑證**。

SSL/TLS 重新協議（5.2.6 版或更新版本）

Sterling B2B Integrator 利用 IBM JSSE 參數來控制 SSL/TLS 重新協議的限制性。在 `security.properties` 檔中，可以更新下列參數。

參數名稱	定義	有效值
com.ibm.jsse2.extended.renegotiation.indicator	請利用這個內容，強制所有協議都需要 RFC 5746，而不只是重新協議。只有在所有必要的通訊夥伴都已實作 RFC 5746 之後，這個協議才實際可行。預設值是 OPTIONAL。	有效值為： • BOTH - 只有在指示的同層級支援 RFC 5746 重新協議時，「IBM JSSE2 伺服器」或 IBM JSSE2 用戶端才能夠進行連線。附註：將內容設為 BOTH，會使未更新為支援 RFC 5746 的用戶端或伺服器，交互作業能力發生問題。 • CLIENT - 只有在指示的伺服器支援 RFC 5746 重新協議時，IBM JSSE2 用戶端才能夠進行連線。附註：將內容設為 CLIENT，會使未更新為支援 RFC 5746 的伺服器，交互作業能力發生問題。 • OPTIONAL - 這個設定是預設值。使用這個選項表示在起始信號交換期間，「IBM JSSE2 伺服器」或「IBM JSSE2 用戶端」不需要重新協議指示器。 • SERVER - 只有在指示的用戶端支援 RFC 5746 重新協議時，「IBM JSSE2 伺服器」才能夠進行連線。附註：將內容設為 SERVER，會使未更新為支援 RFC 5746 的用戶端，交互作業能力發生問題。

參數名稱	定義	有效值
com.ibm.jsse2.renegotiate	請利用這個內容來變更 IBM JSSE2 重新協議的能力。預設值是 NONE。	有效值為： • ABBREVIATED - 這個設定會在階段作業連續性獲證明時，在重新協議期間，置換及接受未受保護的簡要信號交換。接受 RFC 5746 重新協議。 • ALL - 這個設定會在重新協議期間，置換及接受未受保護的完整信號交換，以及未受保護的簡要信號交換。接受 RFC 5746 重新協議。 • DISABLED - 這個設定會置換及停用所有不安全的重新協議及 RFC 5746 重新協議。 • NONE - 這個設定是預設值。不接受任何未受保護的信號交換重新協議。只接受 RFC 5746 重新協議。
com.ibm.jsse2.renegotiation.peer.cert.check	請利用這個內容來變更 IBM JSSE2 重新協議的能力，要求 RFC 5746 所指定的同層級支援。只有在所有必要的通訊夥伴都已實作 RFC 5746 之後，這個需求才實際可行。預設值是 OFF。	有效值為： • OFF - 這個設定是預設值。它會停止「IBM JSSE2 用戶端」或「IBM JSSE2 伺服器」針對同層級的憑證來執行識別檢查。結果是容許在重新協議期間變更同層級憑證。 • ON - 這個設定會使「IBM JSSE2 用戶端」或「IBM JSSE2 伺服器」對照同層級的憑證來進行比較。原因是為了確保在重新協議期間，憑證沒有改變。這項比較適用於安全及未受保護的重新協議。

疑難排解 SSL

如果收到錯誤訊息，您可以對 SSL 進行疑難排解。

毀損或無法使用的憑證錯誤訊息

如果您收到下列錯誤訊息：

嚴重警示：BAD_CERTIFICATE - 收到毀損或無法使用的憑證。

來自 Perimeter 日誌的資訊如下所示：

```
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)
```

移入憑證時，Sterling B2B Integrator 會在命名畫面上顯示「簽章無效」的「狀態」值。如果執行出埠 HTTP POST 搭配 SSL 的商業程序，在「HTTP 方法」服務上失敗並發生錯誤，則會顯示下列訊息：

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

為交易夥伴取得適當的 CA 憑證。如果交易夥伴使用自簽憑證，則憑證本身可作為 CA 憑證使用。

CA 和直接信任

Sterling B2B Integrator 為用戶端時，如果伺服器擁有由 CA 發行的憑證，並且該憑證在主旨「相對識別名稱 (RDN)」中具有伺服器的 DNS 名稱，您可以將主要 CA 憑證放置在 CA 儲存區中並信任它。如果 SSL 仍然無效，請嘗試直接信任。將伺服器憑證放置在 CA 存放區中並信任它。

如果伺服器使用自簽憑證，請將它放置在 CA 存放區中並信任它。您同樣會在此情況下執行直接信任。

使用不含憑證的 SSL

您無法在沒有必要憑證或系統憑證時，使用已啟用 SSL 的配接器。

使用 CBC 型密碼組合時，SSL 沒有作用

如果您選取 CBC 模式密碼組合，且 SSL 沒有作用，您必須關閉 CBC 保護。

若為 5.2.5 版和更舊版本，請執行下列步驟：

1. 開啟 tmp.sh 檔來編輯。
2. 尋找您正在配置之作業系統的伺服器旗標，並新增下列值：

   ```
   -DDisableSSLEmptyRecords=true
   ```

3. 儲存並關閉檔案。

若為 5.2.6 和更新版本，請執行下列步驟：

1. 在 *<B2Bi Install>*/bin 目錄中，若為 Windows，請找出 InstallNoappsWindowsService.cmd.in 和 InstallContainerWindowsService.cmd.in；若為其他所有作業系統，請找出 tmp.sh_platform_ifcresources_ext.in。
2. 編輯檔案，將下列內容的所有實例變更為 false：

   ```
   jsse.enableCBCProtection=true
   ```

3. 執行 setupfiles Script。

GPM 的 HTTPS 配置

在基本 HTTP 埠 + 1 上，Sterling B2B Integrator 中的大部分 Web 應用程式都已支援透過 SSL 的安全 HTTP 存取。

此 SSL 加強功能：

- 啟用「圖形程序建模器 (GPM)」的 HTTPS（HTTP 含 SSL 加密）
- 在基本 HTTP 埠上啟用 Web 應用程式的停用和重新導向至不同的埠（使用 HTTPS）
- 透過在安全 HTTP 伺服器配接器實例上部署 Web 應用程式，支援對 Web 應用程式的安全存取
- 減少安全風險

如果您使用此功能，您必須配置「圖形程序建模器 (GPM)」，以便和使用 HTTPS 而非 HTTP 的儀表板 Web 應用程式通訊。存取透過安全 HTTP 伺服器配接器部署的 Web 應用程式，可能會比在基本埠上存取慢。

註：在 5.2.6 版和更新版本中，預設安全通訊協定是 TLS 1.2（若為基本 HTTP 埠 + 1）。必要的話，您可以更新 properties_platform_ifcresources_ext 中的 **jsseProtocol** 參數，以變更為 TLS 1.1 或 TLS 1.0。有效值包括下列參數：

- **TLS1-TLS1.1** - 表示 TLS1.0 和 TLS1.1
- **TLS1.1-TLS1.2** - 表示 TLS1.1 和 TLS1.2
- **TLS1** - 表示僅限 TLS1.0
- **TLS1.1** - 表示僅限 TLS1.1
- **TLS1.2** - 表示僅限 TLS1.2

新 SSL 參數

新增數個新參數以加強 SSL 功能。您需要配置這些參數，讓「圖形程序建模器 (GPM)」與伺服器之間的 SSL 通訊更便利。這些新參數必須定義在其各自的內容檔中。

環境的所有自訂內容都應設定在 customer_overrides.properties 檔中，如此就不會在升級或修補程式安裝期間被置換。定義在 sandbox.cfg 檔案內的內容不可定義在 customer_overrides.properties 中，因為這些內容在 customer_overrides.properties 中會被忽略。這些內容僅限未定義在 customer_overrides.properties 中者。

下表說明新 SSL 參數並提供內容檔的名稱，您可以在這裡可找到參數。

參數名稱	定義	內容檔
WEBAPP_LIST_PORT	識別 GPM 用戶端應該用來與伺服器通訊的埠。在安裝期間預設為基本埠。 如果已將「儀表板」和 GPM Web 應用程式部署為安全 HTTP 伺服器配接器實例，則應修改此參數以符合安全 HTTP 伺服器配接器實例的埠。 如果基本 SSL 埠（基本 HTTP 埠 +1）已用於 GPM 和「儀表板」的安全部署，則應修改此參數以符合基本 SSL 埠（sandbox.cfg 中的 SSL_PORT）。	sandbox.cfg 檔案
WEBAPP_PROTOCOL	識別用來與「儀表板」Web 應用程式 (http/https) 通訊的通訊協定。	sandbox.cfg 檔案
SKIP_BASEPORT_ DEPLOYMENT_WARS	指出在基本埠上 WAR 部署期間應該跳過的 Web 應用程式。WAR 清單以逗點區隔，區分大小寫且沒有 .war 字尾。 預設值為不跳過任何 WAR。「儀表板」和 GPM Web 應用程式已順利部署在安全 HTTP 伺服器配接器之後，此參數可設定為 =admin,dashboard,gbm，以移除對基本埠上的 Web 應用程式的存取權。Web 應用程式的完整清單包括： • myaft • Portlet 值 ALL 可當作萬用字元使用，以指示部署在基本 HTTP 埠上的所有 WAR 都應該跳過。如果已對外部存取封鎖基本埠，則無此必要。值 ALL 不可搭配任何其他值使用。	customer_overrides.properties
HTTPS_REDIRECT_WARS	指出自動從基本 HTTP 埠，重新導向至安全 HTTP 伺服器配接器或基本 SSL 埠的 WAR。 值 ALL 可用於將基本 HTTP 埠上所有略過的 WAR，重新導向至 HTTPS_LIST_PORT（安全 HTTP 伺服器配接器或基本 SSL 埠）。 值 ALL 不可搭配任何其他值使用。	customer_overrides.properties
HTTPS_LIST_PORT	指出針對基本 HTTP 埠所做要求的重新導向目的地埠。應該設定為安全 HTTP 伺服器配接器或基本 SSL 埠的值。	customer_overrides.properties

參數名稱	定義	內容檔
HTTPS_CLIENT_CERTS	以逗點區隔的系統憑證清單，其公開金鑰必須新增至預設信任儲存庫。當 HTTPS 呼叫從應用程式伺服器分離 (ASI) 伺服器進行起始設定，然後返回本身時，這些憑證會在 SSL 信號交換期間用於用戶端驗證。 此參數需要具有 **SubjectAltName** 的伺服器憑證金鑰。如果您使用現有金鑰但未搭配此參數，此功能將失效，且訊息非常不明顯。 **註：**在 baseport+1 (sslCert) 上為 HTTPS 配置的憑證會自動新增至信任儲存庫，不需要新增至此清單。	customer_overrides.properties

配置此功能時，如果只定義 SKIP_BASEPORT_DEPLOYMENT_WARS，沒有定義 HTTPS_REDIRECT_WARS 和 HTTPS_LIST_PORT，則無法在基本埠上存取 Web 應用程式，也不會將使用者自動重新導向至 HTTPS 埠。如果使用者因安全起見不願自動重新導向，則此為合理狀況。在安全「HTTP 伺服器」配接器或基本 SSL 埠上存取時，Web 應用程式仍然可用。

啟用自動重新導向至 HTTPS

您可以啟用自動重新導向至 HTTPS。

關於這項作業

新增支援以容許自動重新導向至要針對 Web 應用程式配置的 HTTPS，這些 Web 應用程式都部署在安全埠（HTTP 伺服器配接器或基本 SSL 埠），而在基本埠上都會予以略過。這是選用項目，但強烈建議配置。

註：環境的所有自訂內容都應設定在 customer_overrides.properties 檔中，如此就不會在升級或修補程式安裝期間被置換。

如果要啟用自動重新導向至 HTTPS：

程序

1. 導覽至 /<install_dir>/install/properties。
2. 開啟 customer_overrides.properties 檔，並如下設定下列參數值：

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

   這些參數會配置為自動將使用者重新導向至 Web 應用程式的 HTTPS 實例。

   註：customer_overrides.properties 檔不是預設系統程式碼的一部分。該檔必須在起始系統安裝後建立及移入，以符合您的環境。
3. 儲存並關閉檔案。

範例實作

customer_overrides.properties 檔中的範例實作：

```
 ## 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>
```

註：如果使用「安全 HTTP 伺服器」配接器實例，該配置會要求所有指定為 HTTPS_REDIRECT_WARS 的 WAR，都必須部署在相同的「HTTP 伺服器」配接器實例上。

HTTPS_CLIENT_CERTS

如果已使用「安全 HTTP 伺服器」配接器實例，則必須將用於配置「安全 HTTP 伺服器」配接器實例的 SSL 憑證，新增至授信憑證清單。

這是必要步驟，因為部分「儀表板」畫面會讓 https 回呼至 ASI 伺服器。 為了讓這些呼叫成功完成 SSL 信號交換，憑證必須配置在 ASI 伺服器的信任儲存庫中。在 HTTPS_CLIENT_CERTS 清單中指定憑證名稱即可完成這項作業。

建立系統憑證時，這些系統憑證必須將 DNS 名稱和 IP 位址指定為替代名稱。由 JDK 提供的預設 SSL 主機名稱驗證，會要求該 SSL 伺服器呈現的憑證名稱，必須符合 http url 中所使用的主機名稱，或符合憑證的 "SubjectAltName" 屬性的其中一個字串。儀表板上的部分畫面需有 "SubjectAltName" 配置才會運作。

替代名稱是透過系統憑證建立精靈（**交易夥伴** > **數位憑證** > **系統**）中的「以逗點區隔的 IP 位址清單」和「以逗點區隔的 DNS 名稱清單」欄位，來加以配置。

HTTPS 支援 GPM

Java Web Start (JavaWS) 用於透過 HTTP 啟動「圖形程序建模器 (GPM)」。它支援 HTTPS 和類似瀏覽器的憑證動態匯入。

SSL 信號交換期間，伺服器提供其憑證，JavaWS 則處理信任驗證。如果 JavaWS 無法驗證憑證，系統會提示使用者接受或拒絕憑證。JavaWS 無法自動驗證 SSL 憑證，它必須由使用者驗證。

為 Java Web Start 匯入憑證

如果要避免 Java Web Start (JavaWS) 作業期間出現未信任的憑證提示，您可以先將憑證匯入本端電腦儲存庫，然後再啟動「圖形程序建模器 (GPM)」。

關於這項作業

如果使用者的本端電腦，未信任與安全 HTTP 伺服器配接器或基本 SSL 埠相關聯的 SSL 憑證，這樣做可減少使用者的混淆。

如果要將授信主要憑證匯入 JavaWS：

程序

1. 將授信主要憑證儲存至本端電腦的檔案上。
2. 在您的本端電腦上開啟 **Java 控制台**（jre\bin 之下的 javaws.exe）。

3. 開啟**安全**標籤並按一下**憑證**。
4. 按一下**匯入**，瀏覽至授信主要憑證並選取它。
5. 按一下**開啟**以匯入新的授信主要憑證。 移入授信主要憑證之後，JavaWS 會在 SSL 信號交換期間將它當作信任驗證。

使用基本 SSL 埠從 HTTP 切換為 HTTPS

您可以使用基本 SSL 埠從 HTTP 切換為 HTTPS。

關於這項作業

如果要使用基本 SSL 埠從 HTTP 切換為 HTTPS：

程序

1. 導覽至 /install_dir/install/properties。
2. 開啟 sandbox.cfg 檔。
3. 修改下列參數：

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

   這些參數由「圖形程序建模器 (GPM)」用於和伺服器通訊。
4. （選用項目，建議）如果要關閉基本埠上的儀表板和 GPM Web 應用程式的存取，以及配置自動重新導向至 HTTPS 埠，請在 customer_overrides.properties 檔中指定下列參數：

```
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. 儲存並關閉檔案。
6. 導覽至 /install_dir/install/bin。
7. 停止 Sterling B2B Integrator。
8. 套用配置變更。輸入 ./setupfiles.sh。
9. 部署新配置。輸入 ./deployer.sh。
10. 啟動 Sterling B2B Integrator。
11. （選用項目）如果要關閉基本埠上的儀表板和 GPM Web 應用程式的存取（步驟 4），請驗證所做的變更。例如，您可以驗證：

- 存取儀表板 Web 應用程式時，無法從 http://host:baseport/dashboard 進行存取，或者會自動重新導向至 https://host:<base_port + 1>/dashboard 加以存取。
- 存取 http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp 上的 GPM Web 應用程式時，會無法存取，或者會自動重新導向至 https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp。

使用安全 HTTP 伺服器配接器從 HTTP 切換為 HTTPS 模式

您可以使用「安全 HTTP 伺服器」配接器從 HTTP 切換為 HTTPS 模式。

關於這項作業

如果要從 HTTP 切換為 HTTPS 模式：

程序

1. 新建「HTTP 伺服器」配接器實例，並啟用 SSL。您必須配置下列指定的參數：
   - **需要使用者鑑別**設定為**否**
   - **使用 SSL** 設定為**必須**
2. 將必要的 WAR 檔部署至「HTTP 伺服器」配接器實例，並啟用 SSL。

   註：配置「HTTP 伺服器」配接器實例時，所有 WAR 檔都必須從 /install_dir/install/noapp/deploy 目錄挑選。此外，管理 Web 應用程式的環境定義名稱還必須與 /install_dir/install/properties/sandbox.cfg 檔中的 ADMIN_CONTEXT_PATH 參數相符。若是所有其他 Web 應用程式，環境定義名稱應該為副檔名不是 ".war" 的 WAR 檔之名稱。

   此為必要，以便透過修補程式和緊急修復程式所做的變更，會自動在「HTTP 伺服器」配接器部署中反映。

   所需的 WAR 檔包括：
   - admin.war
   - dashboard.war
   - gbm.war
   - myaft.war
   - portlets.war

   可能需要其他 WAR 檔以支援您新增至「儀表板」的新功能。
3. 開啟 sandbox.cfg 檔，並修改下列參數：

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

   這些參數由 GPM 用於和伺服器通訊。
4. （選用項目，建議）如果要關閉基本埠上的儀表板和 GPM Web 應用程式的部署，請在 customer_overrides.properties 檔中指定下列參數：

```
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. 如果您要在這項功能中使用不同憑證，請修改 /install_dir/install/properties/customer_overrides.properties，並新增下列一行：*noapp.sslCert={mention_name_of_your_own_cert}*。如果您未指定不同憑證，則這項功能會使用 ASISslCert。
6. （選用項目）如果要使用 HTTPS 之類的安全通訊協定從瀏覽器傳送 Cookie，請導覽至 /install_dir/install/properties，並在 customer_overrides.properties 檔案中指定下列參數：

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

7. 導覽至 /install_dir/install/bin。
8. 停止 Sterling B2B Integrator。
9. 套用配置變更。輸入 ./setupfiles.sh。
10. 部署新配置。輸入 ./deployer.sh。
11. 啟動 Sterling B2B Integrator。
12. 11. 存取 https://host:<*secure_http_server_adapter_port*>/dashboard，透過「HTTP 伺服器」配接器來驗證儀表板 Web 應用程式。
13. 藉由存取 https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp，來驗證透過安全「HTTP 伺服器」配接器可存取 GPM Web 應用程式。
14. 儲存並關閉檔案。
15. 如果您已關閉基本埠上的儀表板和 GPM Web 應用程式的部署（步驟 4），請驗證下列項目：
    - 如果要存取 http://host:baseport/dashboard 上的儀表板 Web 應用程式，則會自動重新導向至 https://host:<*secure_http_server_adapter_port*>/dashboard。
    - 存取 http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp 上的 GPM Web 應用程式時，會自動重新導向至 https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp。

從 HTTPS 切換為 HTTP 模式

您可以從 HTTPS 切換為 HTTP 模式。

關於這項作業

如果要從 HTTPS 切換為 HTTP 模式：

程序

1. 導覽至 /install_dir/install/properties。
2. 開啟 **sandbox.cfg** 檔案。
3. 修改下列參數：

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

4. 儲存並關閉檔案。
5. （選用項目）當切換為 HTTPS 模式時，如果基本埠上的儀表板和 GPM Web 應用程式的部署為關閉，則您必須開啟 customer_overrides.properties 檔，並註銷下列參數，以便它們不會被套用：

```
## 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. （選用項目）儲存並關閉檔案。
7. 導覽至 /install_dir/install/bin。
8. 停止 Sterling B2B Integrator。
9. 套用配置變更。輸入 ./setupfiles.sh。
10. 部署新配置。輸入 ./deployer.sh。
11. 啟動 Sterling B2B Integrator。
12. 請驗證下列項目：
    - 儀表板 Web 應用程式可從 http://host:baseport/dashboard 取得
    - GPM Web 應用程式可從 http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp 取得
13. （選用項目）從 SSL 已啟用的 HTTP 伺服器配接器實例中解除部署 Web 應用程式。

硬體安全模組 (HSM) 5.2.3 - 5.2.5 版

硬體安全模組 (HSM)

HSM 是一種用於產生、儲存及保護加密金鑰的硬體式安全裝置。您可以利用 Sterling B2B Integrator 將系統憑證儲存於資料庫中，或儲存於 HSM 中。

Sterling B2B Integrator 支援下列 HSM 裝置：

- SafeNet Eracom ProtectServer Orange External
- ProtectServer Gold PCI 裝置

您可以使用 HSM 來執行下列作業：

- 在 HSM 中建立系統憑證
- 從 Sterling B2B Integrator 匯入系統憑證

- 從 Sterling B2B Integrator 匯出系統憑證
- 從 HSM 中移除系統憑證
- 檢視 HSM 中憑證的系統憑證詳細資料

適用於 HSM 支援的 Sterling B2B Integrator 特性

Sterling B2B Integrator 會將代表每一個金鑰組和憑證的項目儲存在 CERTS_AND_PRI_KEY 表格中。

此項目包含下列相關資訊：

- 金鑰和憑證，包括使用者介面 (UI) 用來向使用者顯示的有效期限、序號、使用限制、發證者及主旨，而不需要實際存取金鑰或憑證。
- 將系統用於搜尋的識別名稱正規化
- 記錄修改。
- 憑證撤銷狀態資訊。
- 金鑰儲存庫類型。
- 儲存於 DATA_TABLE 中之二進位金鑰儲存庫物件的參照。當使用軟體金鑰儲存庫時，參照物件可能包含金鑰資料。如果是 HSM，則會包含參照資訊 (nCipher) 或位置保留元 (Eracom)。

HSM 系統憑證參數

下表提供 CreateSystemCert、ImportSystemCert 及 ExportSystemCert 指令的參數。

參數	說明
autogen	是否使用系統產生的資訊來控制金鑰和金鑰儲存庫的存取權。如果是 HSM 中的金鑰，則必須設為 false。
alias	儲存於 HSM 中的金鑰名稱。別名只包含字元 a-z、A-Z、0-9 或連字號 (-)，且其總長不超過系統 GUID 長度。
Certtype	要匯入的憑證類型。支援四種憑證檔類型：pkcs12、pkcs8、pem 與 keystore。 Sterling B2B Integrator 僅支援使用 DES 或 3DES 加密的 pem 金鑰。請使用 keystore 來列出或匯入金鑰儲存庫。
certname	要指派給 Sterling B2B Integrator 資料庫中憑證的名稱。
file	要匯入的 Keycert 或 PEM 檔案。
keyname	要建立的 Sterling B2B Integrator 系統金鑰名稱。
keypass	用於保護金鑰儲存庫所在的 SafeNet Eracom HSM 之記號的 PIN。
key passphrase	私密金鑰的通行詞組。此值在指令行中為選用項。如果您未提供此值，系統會提示您提供它。金鑰儲存庫所在之 SafeNet Eracom HSM 中記號的 PIN。
keysize	RSA 模數的長度（位元）。有效值為 768、1024、2048、3072 或 4096
keystoretype	要匯入的金鑰儲存庫類型。有效值為 CRYPTOKI。
keystoreprovider	提供者類型。SafeNet Eracom 是唯一支援的 HSM。如果您將憑證匯入預設插槽 0 以外的插槽，則為 ERACOM 或 ERACOM.n。
keytype	公開金鑰演算法。RSA 是唯一支援的演算法。
ObjectID	系統憑證的 ID。

參數	說明
pkcs12file	要匯入的 pkcs12 檔案。
password	keycert 或 PEM 檔案的儲存庫通行詞組。
pkcs12storepass	PKCS12 檔案的儲存庫通行詞組。
pkcs12keypass	用來加密 PKCS12 檔案中私密金鑰的金鑰通行詞組。
provider	金鑰儲存庫類型的提供者。如果您將憑證匯入預設插槽 0 以外的插槽，則為 ERACOM 或 ERACOM.n。
rfc1779rdnsequence	識別名稱字串欄位包含「有效值」直欄中識別的任何欄位。只需要 CN 欄位。請以逗點區隔每個欄位。有效資訊如下： • CN = 通用名稱 • O = 組織 • OU = 組織單位 • L = 位置 • ST = 狀態 • C = 國家/地區（提供雙字母 ISO3166-1 alpha-2 代碼）
storetype	金鑰儲存庫類型。CRYPTOKI 是唯一支援的金鑰儲存庫類型。
signingbit	設定自簽憑證的簽章金鑰使用位元。有效值為 true 或 false。
serial	憑證序號。
system passphrase	Sterling B2B Integrator 系統通行詞組。此值在指令行中為選用項。
store passphrase	存取金鑰儲存庫的通行詞組。金鑰儲存庫所在之 SafeNet Eracom HSM 中記號的 PIN。此值在指令行中為選用項。
systempass	Sterling B2B Integrator 系統通行詞組。
storepass	用於保護金鑰儲存庫所在的 SafeNet Eracom HSM 之記號的 PIN。
totrusttable	判斷憑證是否已新增至授信憑證表格中。有效值為 true 或 false。
validityindays	憑證的有效時間長度（天數）。

SafeNet Eracom HSM

搭配 Sterling B2B Integrator 使用 HSM 之前，您必須先設定 Sterling B2B Integrator，以便使用和辨識 SafeNet Eracom HSM。

如果要安裝和設定 SafeNet Eracom HSM，請遵循供應商提供的指示，並確定您安裝了 Java 執行時期。當您設定和使用公用程式時，請針對將儲存 Sterling B2B Integrator 金鑰的插槽，來使用提供者。針對 SafeNet Eracom 插槽建立了 PIN 後，請勿變更 PIN。如果變更 PIN，Sterling B2B Integrator 無法存取 HSM 的金鑰。

SafeNet Eracom 架構將 HSM 分成多個插槽。請依照供應商的指示安裝和配置卡或 HSM。每一個插槽都有關聯的安全提供者，並受到個別的個人識別號碼 (PIN) 保護。您可以為 Sterling B2B Integrator 建立個別的插槽，並以唯一的 PIN 保護插槽。預設插槽 0 的提供者為 ERACOM。其他插槽的提供者則命名為 ERACOM.*n*，其中，*n* 是插槽的號碼。請確定 Java 執行時期元件可用來與裝置互動。

配置 Sterling B2B Integrator 使用 SafeNet Eracom HSM

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

程序

1. 導覽至 */install_dir*/install/bin。
2. 新增下面幾行至 tmp.sh 與 tmp.sh.ini 檔：

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

   export LD_LIBRARY_PATH
   ```

3. 如果您正在配置網路型伺服器，新增下面幾行至 tmp.sh 與 tmp.sh.ini 檔，其中 *network_device_IP_OR_hostname* 是 SafeNet Eracom 網路型伺服器的 IP 位址或完整網域名稱：

   ```
   ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname

   export ET_HSM_NETCLIENT_SERVERLIST
   ```

4. 將 jprov.jar 從 /opt/Eracom/lib 目錄複製至 */install_dir*/install/jdk/jre/lib/ext 目錄。
5. 將每一個安全提供者的定義新增至 */install_dir*/install/bin/jdk/jre/lib/security/java.security 檔。如果要新增定義，請識別指派給 Certicom 提供者的數目，然後指派 n+1 給 SafeNet Eracom 提供者。對於在 SafeNet Eracom 提供者之後識別的所有其他提供者，請將 security.provider 數目加 1。

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

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

   如果您在 SafeNet Eracom HSM 上使用非零屬性，請如下指定屬性，其中 *x* 為屬性的數目：

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

6. 在 */install_dir*/install/properties/security.properties 檔中定義 TLSProviderPolicy。
   - 如果是在屬性 0 中定義提供者，請確定 TLSProviderPolicy 參數的唯一未註解行如下：

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

   - 如果是在 0 以外的屬性中定義提供者，請如下修改 TLSProviderPolicy 參數，其中 *x* 為您正要配置的屬性：

```
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 檔中定義 KeyStoreProviderKey 指令。
   - 如果是在屬性 0 中定義提供者，請確定 KeyStoreProviderMap 定義如下：

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

- 如果是在 0 以外的任何屬性中定義提供者，請如下修改 KeyStoreProviderMap 參數，其中 *x* 為您正要配置的屬性：

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

支援的 nCipher 和 SafeNet/Eracom 網路與 PCI 裝置

除 nCipher 之外，Sterling B2B Integrator 目前還支援 Safenet/Eracom ProtectServer Orange PCI 卡和 ProtectServer Orange External 網路裝置。

支援下列各項：

製造商	支援的裝置類型
nCipher	• nShield 系列 PCI 卡 • NetHSM 網路裝置
Safenet/Eracom	• ProtectServer Gold PCI 卡 • ProtectServer Orange PCI 卡 • ProtectServer Orange External 網路裝置

使用硬體安全模組

建立系統憑證以儲存在 HSM 中

您可以建立自簽系統憑證以儲存在 HSM 中。

開始之前

開始之前：

- 停止 Sterling B2B Integrator。
- 確定 Sterling B2B Integrator 資料庫執行中。

關於這項作業

如果要建立自簽系統憑證以儲存在 HSM 中：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays` [系統通行詞組] [儲存庫通行詞組] [金鑰通行詞組]
3. 如果您未在指令行中提供系統通行詞組、儲存庫通行詞組與金鑰通行詞組，系統會提示您輸入。

列出儲存於 HSM 中的系統憑證

您可以列出儲存於 HSM 中的系統憑證的相關資訊。

關於這項作業

如果要列出儲存於 HSM 中的系統憑證相關資訊，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

範例

以下是指令輸出的範例：

```
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
```

將 HSM 系統憑證匯入 Sterling B2B Integrator 資料庫

當金鑰和憑證存在於 HSM 且已新增至獨立於 Sterling B2B Integrator 之外的 HSM 中時，請使用這項程序。您必須先將儲存於 HSM 的系統憑證資訊匯入資料庫中，然後 Sterling B2B Integrator 才能使用它。

關於這項作業

根據用來將私密金鑰和憑證新增至 HSM 的方法，清單功能可能顯示單一金鑰和憑證配對的重複項目。

您必須先取得系統憑證別名，然後才能將系統憑證的相關資訊匯入資料庫中。

如果要匯入系統憑證，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

移除儲存在 HSM 中的系統憑證

您可以從 HSM 永久刪除系統憑證。其內含的私密金鑰無法回復。

關於這項作業

如果要移除儲存在 HSM 中的系統憑證：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./RemoveSystemCert.sh -r`*xxxx*

   其中，*xxxx* 是要移除的憑證的物件 ID。

匯出系統憑證

您可以從 Sterling B2B Integrator 匯出系統憑證，以便將它們匯入 HSM。

關於這項作業

您無法使用 ExportSystemCert.sh 來匯出 HSM 中的系統憑證。

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. 輸入您的通行詞組。

範例：HSM 系統憑證

您可以將系統憑證以 keycert、pkcs12 或 pem 格式匯入 HSM。匯入系統憑證會將金鑰和憑證新增至 HSM，並在 Sterling B2B Integrator 資料庫中建立對應項目。

如果您匯入 pem 類型的憑證和金鑰，請確定私密金鑰是以 DES 或三重 DES 演算法加密格式建立。

以下是以三重 DES 演算法格式建立的 pem 私密金鑰範例：

```
-----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/WynlVfRK1gEEg8MPa3B9veat7OET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

管理系統憑證公用程式

HSM 金鑰組和憑證簽章要求

GenCSR 公用程式會在 HSM 上產生金鑰組，並且使用該金鑰組中的公開金鑰建立 PKCS10 憑證簽署要求 (CSR)。然後，您可以將 CSR 提交給「憑證管理中心 (CA)」。

當您收到 CA 發出的憑證時，請使用 GenCSR 來更新憑證。系統憑證必須以 CA 發出的憑證更新後，才能在 Sterling B2B Integrator 中使用。

您也可以使用此公用程式來檢視 CSR 清單、將 CSR 相關資訊寫入檔案、刪除 CSR，或將儲存於 HSM 中 CA 發出的憑證的相關資訊寫入檔案。CSR 的相關資訊是在 Sterling B2B Integrator 資料庫中維護，而實際金鑰則是儲存在 HSM 中。

如果要使用此公用程式，請先決定所要執行的動作。然後，使用 GenCSR 公用程式並在指令行中識別動作。針對每一個動作，在內容檔中提供動作所需的引數。在 */install_dir*/install/properties 目錄中提供了一個稱為 csr.properties.sample 的範例內容檔。

您可以在 */install_dir*/install/bin 目錄中找到 GenCSR 公用程式。

指令語法如下：`GenCSR.sh -a ACTION -p PROPERTIES`

GenCSR 參數

下表提供執行 GenCSR Script 時所使用的參數。

參數	說明	有效值
-a ACTION	要執行的動作。	有效動作如下： • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	包含動作所需的其他參數的內容檔。您需要併入內容檔的路徑。	內容檔的名稱。 例如：`csr_create.properties`

以 CA 發行的憑證更新 HSM 金鑰儲存庫

使用 GenCSR 公用程式搭配更新引數，將 CA 發行的憑證資訊新增至 HSM 金鑰儲存庫。

程序

1. 請確定 csr_update.properties 檔已正確配置。

   下表針對更新引數說明 csr_update.properties 檔所需的參數。

參數	說明	有效值
provider	金鑰儲存庫提供者的名稱。	ERACOM 或 ERACOM.n
keystoretype	使用的金鑰儲存庫名稱。	CRYPTOKI
certificate.request.Name	要更新的 CSR 名稱。	指派給 CSR 的名稱
add.trusted	識別憑證資訊是否已新增至授信憑證表。	True | false
ca.cert.file	寫入 CA 發行的憑證相關資訊之檔案的路徑和檔名。	CA 發行的憑證檔案之有效路徑和檔名

2. 更新 HSM 金鑰儲存庫。

   指令語法為：`./GenCSR.sh -a update -p ../properties/csr_update.properties`

列出憑證簽章要求

搭配使用 GenCSR 公用程式和 list 引數，以顯示 HSM 資料庫中的 CSR。list 引數不需要內容檔配置。

關於這項作業

指令語法如下：`./GenCSR.sh -a list`

刪除憑證簽署要求

使用 GenCSR 公用程式與 delete 引數來刪除 CSR。此公用程式只會刪除 CSR。它不會刪除以 CA 發出憑證更新的系統憑證。

程序

1. 確定已適當配置 cacert.properties 檔。 在使用 delete 引數之前，您必須先配置內容檔。下列表格說明 cacert.properties 檔中 delete 引數的必要參數。

參數	說明	有效值
certificate.request.Name	要刪除的 CSR 名稱。	CSR 的名稱
keystoretype	使用的金鑰儲存庫名稱。	CRYPTOKI
provider	金鑰儲存庫提供者的名稱。	ERACOM[.N]

2. 刪除 CSR。 指令語法為 `./GenCSR.sh -a delete -p ../properties/cacert.properties`

將 CSR 資訊寫入 pkcs10 格式

使用 GenCSR 公用程式搭配 getpkcs10 引數，以 pkcs10 格式將 CSR 寫入指定的檔案。

程序

1. 請確定 csr_getpkcs10.properties 檔已正確配置。

   下表針對 getpkcs10 引數說明 csr_getpkcs10.properties 檔所需的參數。您必須先配置內容檔，才可使用 getpkcs10 引數。

參數	說明	有效值
certificate.request.Name	CSR 的名稱。	指派給 CSR 的名稱
keystoretype	使用的金鑰儲存庫名稱。	CRYPTOKI
csr.file	寫入 CSR 資訊之檔案的完整路徑。	寫入 CSR 資訊之檔案的路徑和檔名

2. 將 CSR 寫入檔案。

   指令語法為 `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

將系統憑證移至 HSM

您可以將自簽憑證或 CA 發出的憑證從資料庫移至 HSM。

關於這項作業

更安全的作法是利用 CreateSystemCert.sh 或 GenCSR.sh 來重新產生金鑰和憑證。

如果要將自簽憑證或 CA 發出的憑證從資料庫移至 HSM，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 停止 Sterling B2B Integrator。

3. 啟動資料庫。
4. 將系統憑證匯出至 PKCS12 檔：

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

5. 尋找要移除之系統憑證的物件 ID。輸入：

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

6. 從資料庫中移除系統憑證。輸入：

   `RemoveSystemCert.sh -r`*xxxx*，其中 *xxxx* 是所要移除憑證的物件 ID。

7. 如果要匯入您匯出至 HSM 的系統憑證並建立對應的資料庫項目，請執行下列指令：

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

   註：如果您將 OpsDrv、OpsKey 及 UIKey 移至 HSM，請使用確切名稱。否則，Sterling B2B Integrator 將無法適當地運作。如果是其他所有系統憑證，則名稱並不重要。當移動 OpsDrv、OpsKey 及 UIKey 以外的系統憑證時，會變更服務和配接器所用的物件 ID。請重新配置使用已移動之系統憑證的任何服務。

將 CA 發行的憑證寫入檔案

使用 GenCSR 公用程式搭配 getcacert 引數，將 CA 發行的憑證寫入檔案。

程序

1. 請確定 getcacert.properties 檔已正確配置。

   下表針對 getcacert 動作說明 getcacert.properties 檔所需的參數。您必須先配置 getcacert.properties 檔，才可使用 getcacert 引數。

參數	說明	有效值
certificate.request.Name	CSR 的名稱。	憑證名稱
keystoretype	使用的金鑰儲存庫名稱。	CRYPTOKI
ca.cert.file	寫入 CA 憑證資訊之檔案的完整路徑。	CA 憑證檔案的名稱和路徑

2. 將憑證寫入檔案。

   指令語法為 `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

在 HSM 上產生內部系統憑證（OpsDrv、OpsKey、UIKey）

三個系統憑證會隨 Sterling B2B Integrator 一起安裝來保護內部作業的安全。將它們移至 HSM 可以有益於增加少許的安全性。您的安全原則可能會要求將含有私密金鑰的所有憑證儲存在 HSM 中。

關於這項作業

當在 HSM 上產生稱為 OpsDrv、OpsKey 及 UIKey 的 Sterling B2B Integrator 內部系統憑證時，請使用確切名稱。否則，Sterling B2B Integrator 將無法適當地運作。

如果要產生內部系統憑證，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入 `./RemoveSystemCert.sh -l`，以檢視資料庫中的憑證。記下每一個系統憑證的物件 ID。
3. 針對每一個憑證執行下列指令，以從資料庫中刪除系統憑證：`./RemoveSystemCert.sh -r xxxx`，其中 *xxxx* 是所要移除憑證的物件 ID。
4. 針對每一個憑證輸入下列指令，以在 HSM 上產生系統憑證：

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

使用 nCipher 和 SafeNetEracom

金鑰儲存庫提供者對映

Sterling B2B Integrator 具有加密服務提供者中唯一的金鑰儲存庫類型；它能夠定義金鑰儲存庫類型與提供者之間的對映，實作金鑰儲存庫物件本身、簽章演算法及金鑰傳輸演算法時需要此對映。

金鑰和金鑰資訊摘要物件包含此資訊，以及 com.sterlingcommerce.security.PrivateKeyInfo 的參照。

這可讓 Sterling B2B Integrator 同時在 HSM 上及在資料庫的軟體儲存庫中使用金鑰組合，除了金鑰或金鑰資訊初次載入到資料庫之外，並不需要其他配置。對於 Sterling B2B Integrator 而言，不論金鑰儲存在何處，所有金鑰看起來全都一樣。

對映會實作為 security.properties 中稱為 KeyStoreProviderMap 的內容。它由一組以分號 (;) 區隔的項目所組成。每一個項目有六個元素（以逗點區隔）並且遵循下列格式：

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

下表說明這些元素：

元素	說明	其他資訊
KeyStoreType	金鑰儲存庫的字串類型	
KeyStoreProvider	實作金鑰儲存庫的加密服務提供者名稱	
DoesAliasMatter	此金鑰儲存庫類型的金鑰別名是否必須是唯一的	這可以是 true 或 false。在每個裝置只有一個金鑰儲存庫的情況下，金鑰必須具有唯一別名。
SignatureProvider	要用來利用金鑰儲存庫中的金鑰建立簽章的加密服務提供者名稱	
EncryptionProvider	使用金鑰儲存庫中的金鑰來解密資訊時，所要使用的加密服務提供者名稱	這主要用於 RSA 金鑰傳輸作業
KeyOnHSM	金鑰儲存庫是否位於 HSM	

字串空值為可接受的值，且將視為形同尚未指定提供者。項目至少必須有兩個值。不論在儲存金鑰、簽章提供者、加密提供者時別名是否重要，以及金鑰是否在適用於 KeyStore 類型的 HSM 上，如果項目包含的值不足六個，這些值將從左到右指派給金鑰儲存庫提供者。其他值將被視為空值，在執行該類型的金鑰作業時，將不會要求特定的提供者。

目前的預設 KeyStoreProviderMap 如下：

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

管理 HSM 金鑰和金鑰資訊

Sterling B2B Integrator 有數個用於管理 HSM 金鑰的 Java Script。

以下列出 Java 程式。

方案	用途
com.sterlingcommerce.db.RemoveSystemCert	列出並刪除 Sterling B2B Integrator 系統憑證。在刪除期間，此程式會盡力清除金鑰儲存庫中的金鑰，並改寫資料庫中的金鑰儲存庫物件。
com.sterlingcommerce.db.CreateCertEx	在 HSM 上產生金鑰組，以及含有該金鑰組之公開金鑰的自簽憑證。
com.sterlingcommerce.security.util. CertificateSigningRequest	在 HSM 上產生金鑰組，以及建立和管理關聯的 PKCS10 憑證簽章要求。您可以將 PKCS10 提供給某個憑證管理中心，以取得該憑證管理中心簽署的憑證。然後，可以使用此程式將該憑證載入金鑰儲存庫，並將它關聯於正確的金鑰組。
com.sterlingcommerce.db.ImportSystemCert	以支援的格式（PKCS12 或 PEM）將私密金鑰和憑證匯入 HSM 中的金鑰儲存庫。將 HSM 中私密金鑰和憑證的相關資訊匯入 Sterling B2B Integrator 資料庫。

適用於 nCipher HSM 支援的 JDK 變更

為了使 Sterling B2B Integrator 能夠使用 nCipher HSM，您必須安裝 nCipher Java 加密服務提供者。如果要執行安裝，請複製 JDK 內 jre/lib/ext 子目錄中的下列 jar 檔案。修改 java.security，以載入 nCipher 提供者。

nCipher 安裝程式會將下列檔案放置於 /opt/nfast/java/classes 中：

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

您應該在 IBM JCE 提供者的後面與 Certicom 提供者的前面新增 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 系統上，您應該將 nCipher 提供者置於 Sun JCA 和 JCE 提供者的後面，以及 Certicom 提供者的前面。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 中的範例來設定 TLSProvider 原則。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
```

適用於 Eracom HSM 支援的 JDK 變更

為了使 Sterling B2B Integrator 能夠使用 Eracom HSM，您必須安裝 Eracom Java 加密服務提供者。如果要執行安裝，請將適當的 .jar 檔案置於 JDK 的 jre/lib/ext 子目錄中，然後修改 java.security，以載入 nCipher 提供者。

nCipher 安裝程式會將下列檔案放置於 /opt/nfast/java/classes 中：

- jcprov.jar
- jprov.jar

您應該在 Certicom 提供者的後面新增 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
```

註：Eracom 具有可以為卡片上每一個插槽指定的提供者。如果是插槽 8 的提供者，請使用：

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

適用於 nCipher HSM 支援的 Linux 環境變更

nCipher 建議您建立特殊使用者帳戶來執行 nCipher hardserver。

您執行 Sterling B2B Integrator 的所在帳戶必須具有同等許可權，或者您必須從 nCipher 特殊帳戶或以 root 身分執行 Sterling B2B Integrator。如果您執行其中一項作業且使用 MySQL，則必須變更 MySQL 的許可權，或在呼叫 run.sh 之前從一般帳戶啟動 MySQL。

適用於 Eracom HSM 支援的 Linux 環境變更

如果要使用 Eracom 裝置，您必須將環境變數中的其他資訊提供給存取該裝置的階段作業。

以下是對於 PATH、LD_LIBRARY_PATH 及 MANPATH 的建議變更：

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

此外，如果您使用的是網路裝置而非本端 PCI 卡，則必須提供 ET_HSM_NETCLIENT_SERVERLIST，如下所示：

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

您應該匯出 tmp.sh 中的這些變數。

硬體安全模組 (HSM) 5.2.6 版或更新版本

硬體安全模組 (HSM)

HSM 是一種用於產生、儲存及保護加密金鑰的硬體式安全裝置。您可以利用 Sterling B2B Integrator 將系統憑證儲存於資料庫中，或儲存於 HSM 中。

Sterling B2B Integrator 支援下列 HSM 裝置：

- SafeNet Luna SA
- nCipher nShield Connect

您可以使用 HSM 來執行下列作業：

- 在 HSM 中建立系統憑證
- 從 Sterling B2B Integrator 匯入系統憑證
- 從 Sterling B2B Integrator 匯出系統憑證
- 從 HSM 中移除系統憑證
- 檢視 HSM 中憑證的系統憑證詳細資料

適用於 HSM 支援的 Sterling B2B Integrator 特性

Sterling B2B Integrator 會將代表每一個金鑰組和憑證的項目儲存在 CERTS_AND_PRI_KEY 表格中。

此項目包含下列相關資訊：

- 金鑰和憑證，包括使用者介面 (UI) 用來向使用者顯示的有效期限、序號、使用限制、發證者及主旨，而不需要實際存取金鑰或憑證。
- 將系統用於搜尋的識別名稱正規化
- 記錄修改。
- 憑證撤銷狀態資訊。

- 金鑰儲存庫類型。
- 儲存於 DATA_TABLE 中之二進位金鑰儲存庫物件的參照。當使用軟體金鑰儲存庫時，參照物件可能包含金鑰資料。如果是 HSM，則會包含參照資訊 (nCipher) 或位置保留元 (Luna)。

HSM 系統憑證參數

下表提供 CreateSystemCert、ImportSystemCert 及 ExportSystemCert 指令的參數。

參數	說明
autogen	是否使用系統產生的資訊來控制金鑰和金鑰儲存庫的存取權。如果是 HSM 中的金鑰，則必須設為 false。
alias	儲存於 HSM 中的金鑰名稱。別名只包含字元 a-z、A-Z、0-9 或連字號 (-)，且其總長不超過系統 GUID 長度。
Certtype	要匯入的憑證類型。支援四種憑證檔類型：pkcs12、pkcs8、pem 與 keystore。 Sterling B2B Integrator 僅支援使用 DES 或 3DES 加密的 pem 金鑰。請使用 keystore 來列出或匯入金鑰儲存庫。
certname	要指派給 Sterling B2B Integrator 資料庫中憑證的名稱。
file	要匯入的 Keycert 或 PEM 檔案。
keyname	要建立的 Sterling B2B Integrator 系統金鑰名稱。
keypass	用於保護金鑰儲存庫所在的 SafeNet 或 nCipher HSM 之記號的 PIN。
key passphrase	私密金鑰的通行詞組。此值在指令行中為選用項。如果您未提供此值，系統會提示您提供它。
keysize	RSA 模數的長度（位元）。有效值為 1024、2048、3072 或 4096
keystoretype	要匯入的金鑰儲存庫類型。有效值為 nCipher.sworld、Luna 及 PKCS11IMPLKS（從 5.2.6.2 起）。
keystoreprovider	提供者類型。有效值為 nCipherKM、LunaProvider 及 IBMPKCS11Impl（從 5.2.6.2 起）。
keytype	公開金鑰演算法。RSA 是唯一支援的演算法。
ObjectID	系統憑證的 ID。
pkcs12file	要匯入的 pkcs12 檔案。
password	keycert 或 PEM 檔案的儲存庫通行詞組。
pkcs12storepass	PKCS12 檔案的儲存庫通行詞組。
pkcs12keypass	用來加密 PKCS12 檔案中私密金鑰的金鑰通行詞組。
provider	金鑰儲存庫類型的提供者。有效值為 nCipherKM、LunaProvider 及 IBMPKCS11Impl（從 5.2.6.2 起）。
rfc1779rdnsequence	識別名稱字串欄位包含「有效值」直欄中識別的任何欄位。只需要 CN 欄位。請以逗點區隔每個欄位。有效資訊如下： • CN = 通用名稱 • O = 組織 • OU = 組織單位 • L = 位置 • ST = 狀態 • C = 國家/地區（提供雙字母 ISO3166-1 alpha-2 代碼）

參數	說明
storetype	金鑰儲存庫類型。有效值為 nCipher.sworld、Luna 及 PKCS11IMPLKS（從 5.2.6.2 起）。
signingbit	設定自簽憑證的簽章金鑰使用位元。有效值為 true 或 false。
serial	憑證序號。
system passphrase	Sterling B2B Integrator 系統通行詞組。此值在指令行中為選用項。
store passphrase	存取金鑰儲存庫的通行詞組。此值在指令行中為選用項。如果您未提供此值，系統會提示您提供它。
systempass	Sterling B2B Integrator 系統通行詞組。
storepass	用於保護金鑰儲存庫所在的 SafeNet 或 nCipher HSM 之記號的 PIN。
totrusttable	判斷憑證是否已新增至授信憑證表格中。有效值為 true 或 false。
validityindays	憑證的有效時間長度（天數）。

使用硬體安全模組

建立系統憑證以儲存在 HSM 中

您可以建立自簽系統憑證以儲存在 HSM 中。

開始之前

開始之前：

- 停止 Sterling B2B Integrator。
- 確定 Sterling B2B Integrator 資料庫執行中。

關於這項作業

如果要建立自簽系統憑證以儲存在 HSM 中：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays` [系統通行詞組] [儲存庫通行詞組] [金鑰通行詞組]
3. 如果您未在指令行中提供系統通行詞組、儲存庫通行詞組與金鑰通行詞組，系統會提示您輸入。

列出儲存於 HSM 中的系統憑證

您可以列出儲存於 HSM 中的系統憑證的相關資訊。

關於這項作業

如果要列出儲存於 HSM 中的系統憑證相關資訊，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。

2. 輸入： `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

範例

以下是指令輸出的範例：

```
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
```

註：從 5.2.6.2 版起，Keystoretype 的有效值為 PKCS11IMPLKS。

將 HSM 系統憑證匯入 Sterling B2B Integrator 資料庫

當金鑰和憑證存在於 HSM 且已新增至獨立於 Sterling B2B Integrator 之外的 HSM 中時，請使用這項程序。您必須先將儲存於 HSM 的系統憑證資訊匯入資料庫中，然後 Sterling B2B Integrator 才能使用它。

關於這項作業

根據用來將私密金鑰和憑證新增至 HSM 的方法，清單功能可能顯示單一金鑰和憑證配對的重複項目。

您必須先取得系統憑證別名，然後才能將系統憑證的相關資訊匯入資料庫中。

如果要匯入系統憑證，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

移除儲存在 HSM 中的系統憑證

關於這項作業

此程序會永久刪除 HSM 中的系統憑證。其內含的私密金鑰無法回復。

如果要移除儲存在 HSM 中的系統憑證：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./RemoveSystemCert.sh -r`*xxxx*

   其中，*xxxx* 是要移除的憑證的物件 ID。

匯出系統憑證

您可以從 Sterling B2B Integrator 匯出系統憑證，以便將它們匯入 HSM。

關於這項作業

您無法使用 ExportSystemCert.sh 來匯出 HSM 中的系統憑證。

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入： `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. 輸入您的通行詞組。

範例：HSM 系統憑證

您可以將系統憑證以 keycert、pkcs12 或 pem 格式匯入 HSM。匯入系統憑證會將金鑰和憑證新增至 HSM，並在 Sterling B2B Integrator 資料庫中建立對應項目。

如果您匯入 pem 類型的憑證和金鑰，請確定私密金鑰是以 DES 或三重 DES 演算法加密格式建立。

以下是以三重 DES 演算法格式建立的 pem 私密金鑰範例：

```
-----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
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszRJjvPvM8zL1EwxO
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----END RSA PRIVATE KEY-----
```

管理系統憑證公用程式

HSM 金鑰組和憑證簽章要求

GenCSR 公用程式會在 HSM 上產生金鑰組，並且使用該金鑰組中的公開金鑰建立 PKCS10 憑證簽署要求 (CSR)。然後，您可以將 CSR 提交給「憑證管理中心 (CA)」。

當您收到 CA 發出的憑證時，請使用 GenCSR 來更新憑證。系統憑證必須以 CA 發出的憑證更新後，才能在 Sterling B2B Integrator 中使用。

您也可以使用此公用程式來檢視 CSR 清單、將 CSR 相關資訊寫入檔案、刪除 CSR，或將儲存於 HSM 中 CA 發出的憑證的相關資訊寫入檔案。CSR 的相關資訊是在 Sterling B2B Integrator 資料庫中維護，而實際金鑰則是儲存在 HSM 中。

如果要使用此公用程式，請先決定所要執行的動作。然後，使用 GenCSR 公用程式並在指令行中識別動作。針對每一個動作，在內容檔中提供動作所需的引數。在 */install_dir*/install/properties 目錄中提供了一個稱為 csr.properties.sample 的範例內容檔。

您可以在 */install_dir*/install/bin 目錄中找到 GenCSR 公用程式。

指令語法如下：`GenCSR.sh -a ACTION -p PROPERTIES`

GenCSR 參數

下表提供執行 GenCSR Script 時所使用的參數。

參數	說明	有效值
-a ACTION	要執行的動作。	有效動作如下： • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	包含動作所需的其他參數的內容檔。您需要併入內容檔的路徑。	內容檔的名稱。 例如：`csr_create.properties`

以 CA 發行的憑證更新 HSM 金鑰儲存庫

關於這項作業

使用 GenCSR 公用程式搭配更新引數，將 CA 發行的憑證資訊新增至 HSM 金鑰儲存庫。

程序

1. 請確定 csr_update.properties 檔已正確配置。

   下表針對更新引數說明 csr_update.properties 檔所需的參數。

參數	說明	有效值
provider	金鑰儲存庫提供者的名稱。	IBMPKCS11IMPL（從 5.2.6.2 版起）或 nCipherKM 或 LunaProvider
keystoretype	使用的金鑰儲存庫名稱。	PKCS11IMPLKS（從 5.2.6.2 版起）或 nCipher.sworld 或 Luna **註：**'keystoretype' 值應該與 'provider' 值同步。
certificate.request.Name	要更新的 CSR 名稱。	指派給 CSR 的名稱
add.trusted	識別憑證資訊是否已新增至授信憑證表。	True | false
ca.cert.file	寫入 CA 發行的憑證相關資訊之檔案的路徑和檔名。	CA 發行的憑證檔案之有效路徑和檔名

2. 更新 HSM 金鑰儲存庫。

   指令語法為：`./GenCSR.sh -a update -p ../properties/csr_update.properties`

列出憑證簽章要求

搭配使用 GenCSR 公用程式和 list 引數，以顯示 HSM 資料庫中的 CSR。list 引數不需要內容檔配置。

關於這項作業

指令語法如下：`./GenCSR.sh -a list`

刪除憑證簽署要求

使用 GenCSR 公用程式與 delete 引數來刪除 CSR。此公用程式只會刪除 CSR。它不會刪除以 CA 發出憑證更新的系統憑證。

程序

1. 確定已適當配置 cacert.properties 檔。 在使用 delete 引數之前，您必須先配置內容檔。下列表格說明 cacert.properties 檔中 delete 引數的必要參數。

參數	說明	有效值
certificate.request.Name	要刪除的 CSR 名稱。	CSR 的名稱
keystoretype	使用的金鑰儲存庫名稱。	PKCS11IMPLKS（從 5.2.6.2 版起）或 nCipher.sworld 或 Luna
provider	金鑰儲存庫提供者的名稱。	IBMPKCS11IMPL（從 5.2.6.2 版起）或 nCipherKM 或 LunaProvider **註：**'keystoretype' 值應該與 'provider' 值同步。

2. 刪除 CSR。 指令語法為 `./GenCSR.sh -a delete -p ../properties/cacert.properties`

將 CSR 資訊寫入 pkcs10 格式

關於這項作業

使用 GenCSR 公用程式搭配 getpkcs10 引數，以 pkcs10 格式將 CSR 寫入指定的檔案。

程序

1. 請確定 csr_getpkcs10.properties 檔已正確配置。

   下表針對 getpkcs10 引數說明 csr_getpkcs10.properties 檔所需的參數。您必須先配置內容檔，才可使用 getpkcs10 引數。

參數	說明	有效值
certificate.request.Name	CSR 的名稱。	指派給 CSR 的名稱
keystoretype	使用的金鑰儲存庫名稱。	PKCS11IMPLKS（從 5.2.6.2 版起）或 nCipher.sworld 或 Luna
csr.file	寫入 CSR 資訊之檔案的完整路徑。	寫入 CSR 資訊之檔案的路徑和檔名

2. 將 CSR 寫入檔案。

   指令語法為 `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

將系統憑證移至 HSM

您可以將自簽憑證或 CA 發出的憑證從資料庫移至 HSM。

關於這項作業

更安全的作法是利用 CreateSystemCert.sh 或 GenCSR.sh 來重新產生金鑰和憑證。

如果要將自簽憑證或 CA 發出的憑證從資料庫移至 HSM，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 停止 Sterling B2B Integrator。
3. 啟動資料庫。
4. 將系統憑證匯出至 PKCS12 檔：

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

5. 尋找要移除之系統憑證的物件 ID。輸入：

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

6. 從資料庫中移除系統憑證。輸入：

   `RemoveSystemCert.sh -r`*xxxx*，其中 *xxxx* 是所要移除憑證的物件 ID。

7. 如果要匯入您匯出至 HSM 的系統憑證並建立對應的資料庫項目，請執行下列指令：

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

   註：如果您將 OpsDrv、OpsKey 及 UIKey 移至 HSM，請使用確切名稱。否則，Sterling B2B Integrator 將無法適當地運作。如果是其他所有系統憑證，則名稱並不重要。當移動 OpsDrv、OpsKey 及 UIKey 以外的系統憑證時，會變更服務和配接器所用的物件 ID。請重新配置使用已移動之系統憑證的任何服務。

將 CA 發行的憑證寫入檔案

關於這項作業

使用 GenCSR 公用程式搭配 getcacert 引數，將 CA 發行的憑證寫入檔案。

程序

1. 請確定 getcacert.properties 檔已正確配置。

   下表針對 getcacert 動作說明 getcacert.properties 檔所需的參數。您必須先配置 getcacert.properties 檔，才可使用 getcacert 引數。

參數	說明	有效值
certificate.request.Name	CSR 的名稱。	憑證名稱
keystoretype	使用的金鑰儲存庫名稱。	PKCS11IMPLKS（從 5.2.6.2 版起）或 nCipher.sworld 或 Luna

參數	說明	有效值
ca.cert.file	寫入 CA 憑證資訊之檔案的完整路徑。	CA 憑證檔案的名稱和路徑

2. 將憑證寫入檔案。

   指令語法為 `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

在 HSM 上產生內部系統憑證（OpsDrv、OpsKey、UIKey）

三個系統憑證會隨 Sterling B2B Integrator 一起安裝來保護內部作業的安全。將它們移至 HSM 可以有益於增加少許的安全性。您的安全原則可能會要求將含有私密金鑰的所有憑證儲存在 HSM 中。

關於這項作業

當在 HSM 上產生稱為 OpsDrv、OpsKey 及 UIKey 的 Sterling B2B Integrator 內部系統憑證時，請使用確切名稱。否則，Sterling B2B Integrator 將無法適當地運作。

如果要產生內部系統憑證，請執行下列動作：

程序

1. 導覽至 */install_dir*/install/bin。
2. 輸入 `./RemoveSystemCert.sh -l`，以檢視資料庫中的憑證。記下每一個系統憑證的物件 ID。
3. 針對每一個憑證執行下列指令，以從資料庫中刪除系統憑證：`./RemoveSystemCert.sh -r xxxx`，其中 *xxxx* 是所要移除憑證的物件 ID。
4. 針對每一個憑證輸入下列指令，以在 HSM 上產生系統憑證：

   ```
   ./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 裝置

金鑰儲存庫提供者對映

Sterling B2B Integrator 具有加密服務提供者中唯一的金鑰儲存庫類型；它能夠定義金鑰儲存庫類型與提供者之間的對映，實作金鑰儲存庫物件本身、簽章演算法及金鑰傳輸演算法時需要此對映。

金鑰和金鑰資訊摘要物件包含此資訊，以及 com.sterlingcommerce.security.PrivateKeyInfo 的參照。

這可讓 Sterling B2B Integrator 同時在 HSM 上及在資料庫的軟體儲存庫中使用金鑰組合，除了金鑰或金鑰資訊初次載入到資料庫之外，並不需要其他配置。對於 Sterling B2B Integrator 而言，不論金鑰儲存在何處，所有金鑰看起來全都一樣。

對映會實作為 security.properties 中稱為 KeyStoreProviderMap 的內容。它由一組以分號 (;) 區隔的項目所組成。每一個項目有六個元素（以逗點區隔）並且遵循下列格式：

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

下表說明這些元素：

元素	說明	其他資訊
KeyStoreType	金鑰儲存庫的字串類型	
KeyStoreProvider	實作金鑰儲存庫的加密服務提供者名稱	
DoesAliasMatter	此金鑰儲存庫類型的金鑰別名是否必須是唯一的	這可以是 true 或 false。在每個裝置只有一個金鑰儲存庫的情況下，金鑰必須具有唯一別名。
SignatureProvider	要用來利用金鑰儲存庫中的金鑰建立簽章的加密服務提供者名稱	
EncryptionProvider	使用金鑰儲存庫中的金鑰來解密資訊時，所要使用的加密服務提供者名稱	這主要用於 RSA 金鑰傳輸作業
KeyOnHSM	金鑰儲存庫是否位於 HSM	

字串空值為可接受的值，且將視為形同尚未指定提供者。項目至少必須有兩個值。不論在儲存金鑰、簽章提供者、加密提供者時別名是否重要，以及金鑰是否在適用於 KeyStore 類型的 HSM 上，如果項目包含的值不足六個，這些值將從左到右指派給金鑰儲存庫提供者。其他值將被視為空值，在執行該類型的金鑰作業時，將不會要求特定的提供者。

目前的預設 KeyStoreProviderMap 如下：

```
nCipher = nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true
SafeNet Luna = Luna,LunaProvider,true,LunaProvider,LunaProvider,true
Use "PKCS11IMPLKS,IBMPKCS11Impl,true,IBMPKCS11Impl,IBMPKCS11Impl,true"
for both nCipher and SafeNet Luna from V5.2.6.2 onwards.
```

適用於 nCipher HSM 支援的 JDK 變更

為了使 Sterling B2B Integrator 能夠使用 nCipher HSM，您必須安裝 nCipher Java 加密服務提供者。如果要執行安裝，請複製 JDK 內 jre/lib/ext 子目錄中的下列 jar 檔案。修改 java.security，以載入 nCipher 提供者。

註：

1. 從 5.2.6.2 版起，如果您使用 "PKCS11IMPLKS" 實作建立新的金鑰或憑證，則不需要下列設定。
2. 升級至 5.2.6.2 版之後，若要繼續使用現有的金鑰或憑證，請遵循下列步驟。

nCipher 安裝程式會將下列檔案放置於 /opt/nfast/java/classes 中：

- jcetools.jar
- jutils.jar
- keysafe.jar
- kmjava.jar
- nCipherKM.jar
- nfjava.jar

- rsaprivenc.jar

您應該在 IBM JCE 提供者的後面與 Certicom 提供者的前面新增 nCipher 提供者。

您也必須從清單中移除 IBMJCEFIPS。

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
```

從 5.2.6.2 版起，請使用下列範例來支援現有的金鑰或憑證。

```
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
```

適用於 SafeNet Luna HSM 支援的 JDK 變更

為了使 Sterling B2B Integrator 能夠使用 SafeNet Luna HSM，您必須安裝 SafeNet Luna Java 加密服務提供者。如果要執行安裝，請將適當的 .jar 檔案置於 JDK 的 jre/lib/ext 子目錄中，然後修改 java.security，以載入 Luna 提供者。

註：

1. 從 5.2.6.2 版起，如果您使用 "PKCS11IMPLKS" 實作建立新的金鑰或憑證，則不需要下列設定。
2. 升級至 5.2.6.2 版之後，若要繼續使用現有的金鑰或憑證，請遵循下列步驟。

nCipher 安裝程式會將下列檔案放置於 /opt/nfast/java/classes 中：

- libLunaAPI.so
- LunaProvider.jar

您應該在 IBM JCE 提供者的後面與 Certicom 提供者的前面新增 LunaProvider。

您也必須從清單中移除 IBMJCEFIPS。

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
```

從 5.2.6.2 版起，請使用下列範例來支援現有的金鑰或憑證。

```
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 配置 HSM（5.2.6.2 版或更新版本）

使用 IBM PKCS11 IMPLKS 實作來配置 HSM（5.2.6.2 版或更新版本）

關於這項作業

從 5.2.6.2 版起，系統支援 HSM 裝置的 IBM PKCS11 實作。HSM 實作 Java JCE API。此介面會存取裝置中的金鑰。

程序

1. 已新增內容檔 **hsm.properties.in** 以支援 PKCS11IMPLKS/IBMPKCS11Impl。

   下表列出專用於配置 HSM 的內容清單。

屬性	說明
HSM_KEYSTORE_TYPE	如果 HSM_ENABLED 設為 *true*，此屬性值必須為 *IBMPKCS11IMPLKS*。
HSM_KEYSTORE_PROVIDER	如果 HSM_ENABLED 設為 *true*，此屬性值必須為 *IBMPKCS11Impl*。
HSM_KEYSTORE_FILE	<應該空白>
HSM_ADAPTER_TYPE	ncipher 或 safeNetFor ncipher，請在建立或更新金鑰或憑證時執行下列指令 - UNIX： export CKNFAST_OVERRIDE_SECURITY_ASSURANCES= "longterm;tokenkeys" Windows： set CKNFAST_OVERRIDE_SECURITY_ASSURANCES ="longterm;tokenkeys"
HSM_ENABLED	此屬性必須設為 *true*，才能取得 HSM 支援。

屬性	說明
HSM_PRNG_ALGORITHM	如果 HSM_ENABLED 設為 *true*，此屬性值必須為 *PKCS11DeviceRNG*。
HSM_CONFIG_FILE_LOCATION	如果 HSM_ENABLED 設為 *true*，此屬性值必須設為 IBMPKCS11 配置檔的位置

2. 根據 HSM 類型更新或建立 HSM 設定所需的配置檔。

   關於 HSM 類型，您可以尋找裝置的配置檔，如下所示，或聯絡 IBM 支援中心以取得配置檔。您可以依需要更新任何預設值。如果您的位置不是預設值，則必須編輯 *library* 值。

   SafeNet Luna 裝置：

```
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}
```

nCipher 裝置：

```
======= 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}
```

註：SafeNet Luna 不容許您匯入外部建立的私密金鑰。您必須建立它們並儲存於 HSM 裝置上。

注意事項

本資訊係針對 IBM 在美國所提供之產品與服務所開發。 IBM 可能會以其他語言提供本資料。然而，您可能需要擁有該語言的產品或產品版本副本，才能存取。

在其他國家或地區中，IBM 不見得有提供本文件所提及之各項產品、服務或功能。請洽詢當地的 IBM 業務代表，以取得當地目前提供的產品和服務之相關資訊。本文件在提及 IBM 的產品、程式或服務時，不表示或暗示只能使用 IBM 的產品、程式或服務。只要未侵犯 IBM 之智慧財產權，任何功能相當之產品、程式或服務皆可取代 IBM 之產品、程式或服務。不過，任何非 IBM 之產品、程式或服務，使用者必須自行負責作業之評估和驗證責任。

本文件所說明之主題內容，IBM 可能擁有其專利或專利申請案。提供本文件不代表提供這些專利的授權。您可以書面提出授權查詢，來函請寄到：

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

如果是有關雙位元組字集 (DBCS) 資訊的授權查詢，請洽詢所在國的 IBM 智慧財產部門，或書面提出授權查詢，來函請寄到：

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 只依「現狀」提供本出版品，不提供任何明示或默示之保證，其中包括且不限於未涉侵權、可售性或符合特定效用的隱含保證。有些轄區不允許放棄在特定交易中的明示或默示保證，因此，這項聲明對您可能不適用。

本資訊中可能會有技術上或排版印刷上的訛誤。因此，IBM 會定期修訂；並將修訂後的內容納入新版中。IBM 隨時會改進及/或變更本出版品所提及的產品及/或程式，不另行通知。

本資訊中任何對非 IBM 網站之敘述僅供參考，IBM 對這些網站不提供保證。這些網站所提供的資料不是本 IBM 產品的資料內容，如果要使用這些網站的資料，您必須自行承擔風險。

IBM 得以各種 IBM 認為適當的方式使用或散布 貴客戶提供的任何資訊，而無需對 貴客戶負責。

如果本程式之獲授權人為了 (i) 在個別建立的程式和其他程式（包括本程式）之間交換資訊，以及 (ii) 相互使用所交換的資訊，因而需要相關的資訊，請洽詢：

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

上述資料之取得有其特殊要件，在某些情況下必須付費方得使用。

IBM 基於雙方之「IBM 客戶合約」、「IBM 國際程式授權合約」或任何同等合約之條款，提供本文件中所述之授權程式及其所有適用的授權資料。

本文件中引用的效能資料及用戶範例僅供敘述之目的。實際的效能結果可能會因為特定的配置與運作條件而有差異。

本文件所提及之非 IBM 產品資訊，取自產品的供應商，或其發佈的聲明或其他公開管道。 IBM 並未測試過這些產品，也無法確認這些非 IBM 產品的執行效能、相容性或任何對產品的其他主張是否完全無誤。如果您對非 IBM 產品的性能有任何的疑問，請逕向該產品的供應商查詢。

關於 IBM 未來方針或意向之聲明，僅代表 IBM 的目標與目的，隨時可能變動或撤消，不另行通知。

所顯示的所有 IBM 價格皆為 IBM 目前的建議零售價，此售價得隨時變更，不另行通知。經銷商價格可能各不相同。

本資訊僅供規劃之用。在所描述的產品上市之前，這裡的資訊將視情況變更。

本資訊含有日常商業運作所用之資料和報告範例。為了盡可能地加以完整說明，範例中含有個人、公司、品牌及產品的名稱。這些名稱全為虛構，如與實際個人或企業雷同，純屬巧合。

著作權：

本資訊含有原始語言之範例應用程式，用以說明各作業平台中之程式設計技術。 貴客戶可以為了研發、使用、銷售或散布符合範例應用程式所適用的作業平台之應用程式設計介面程式的應用程式，以任何形式複製、修改及散布這些範例程式，不必向 IBM 付費。該等範例並未在一切情況下完整測試。因此，IBM 不保證或暗示這些程式的可靠性、有用性或功能。程式範例以「現狀」提供，且無任何保證。IBM 不負擔任何因該等範例程式之使用而產生的任何損害。

這些範例程式或任何衍生成果的每份複本或任何部分，都必須包含下一段所顯示的著作權聲明。

© 2015.
本程式碼之若干部分係衍生自 IBM 公司的範例程式。© Copyright IBM Corp. 2015.

商標

IBM、IBM 標誌和 ibm.com 是 International Business Machines Corp. 在全球許多適用範圍內註冊的商標或註冊商標。其他產品及服務名稱，可能是 IBM 或其他公司的商標。IBM 商標的最新清單可於下列網站之「著作權與商標資訊」(Copyright and trademark information) 網頁上取得：www.ibm.com/legal/copytrade.shtml。

Adobe、Adobe 標誌、PostScript 和 PostScript 標誌是 Adobe Systems Incorporated 在美國及/或其他國家或地區的註冊商標或商標。

IT Infrastructure Library 是 Central Computer and Telecommunications Agency（目前隸屬於 Office of Government Commerce）的註冊商標。

Intel、Intel 標誌、Intel Inside、Intel Inside 標誌、Intel Centrino、Intel Centrino 標誌、Celeron、Intel Xeon、Intel SpeedStep、Itanium 和 Pentium 是 Intel Corporation 或其子公司在美國及/或其他國家或地區的商標或註冊商標。

Linux 是 Linus Torvalds 在美國及/或其他國家或地區的註冊商標。

Microsoft、Windows、Windows NT 及 Windows 標誌是 Microsoft Corporation 在美國及/或其他國家或地區的商標。

ITIL 是 Office of Government Commerce 的註冊商標和註冊社群商標，並已在 U.S. Patent and Trademark Office 註冊。

UNIX 係 The Open Group 在美國及/或其他國家或地區之註冊商標。

Java™ 及所有以 Java 為基礎的商標與標誌均為 Oracle 及/或其關係企業的商標或註冊商標。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美國及/或其他國家或地區的商標，並獲其授權使用。

Linear Tape-Open、LTO、LTO 標誌、Ultrium 和 Ultrium 標誌是 HP、IBM Corp. 和 Quantum 在美國及其他國家或地區的商標。

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 公司）的商標或註冊商標。

其他公司、產品及服務名稱，可能是第三者的商標或服務標誌。

產品說明文件條款

根據下述條款，將授與您對這些出版品的使用權限。

適用範圍

這些條款為 IBM 網站使用條款的增補條款。

個人用途

貴客戶可以為了非商務性的私人用途而重製這些出版品，但必須保留所有專利注意事項。未經 IBM 明文同意，貴客戶不得散布、展示或製作這些出版品或其任何部分的衍生著作。

商業用途

貴客戶可以在企業內重製、散布和展示這些出版品，但必須保留所有專利注意事項。未經 IBM 明文同意，貴客戶不得產生這些出版品的衍生著作，不得在所屬企業之外，重製、散布或展示這些出版品或其中任何部份。

權利

除了本項許可權所明確授予者之外，並未明示或暗示授予出版品或任何資訊、資料、軟體或其中的其他智慧財產的任何其他許可權、授權或權利。

如 IBM 認為出版品的使用損及 IBM 的利益，或經 IBM 判斷為未適當遵守上述指示時，IBM 保留撤銷本項授權的權利。

除非完全符合一切適用的法令規章，其中包括所有美國出口法令規章，否則，貴客戶不能下載、輸出或再輸出本項資訊。

IBM 對這些出版品的內容，不提供任何保證。這些出版品是依「現狀」提供，不含任何明示或默示之保證（包括但不限於可售性、未涉侵權及符合特定效用的保證）。

程式號碼：

Printed in Taiwan