Sterling B2B Integrator

Security (V5.2.3 oder höher)

Version 5.2.3

Sterling B2B Integrator

Security (V5.2.3 oder höher)

Version 5.2.3

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 149 gelesen werden.

Diese Ausgabe bezieht sich auf Version 5, Release 2, Modifikation 3 von Sterling B2B Integrator und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
Sterling B2B Integrator Security (V5.2.3 or later) Version 5.2.3
herausgegeben von International Business Machines Corporation, USA

Herausgegeben von:
TSC Germany
Kst. 2877
Juni 2016

Inhaltsverzeichnis

Security (V5.2.3 oder höher)

Sterling B2B Integrator verwendet eine Vielzahl von Sicherheitsmechanismen einschließlich Systemkennwörtern für Verwaltungsfunktionen, Kennwortrichtlinien auf der Basis der Sicherheitsrichtlinien Ihres Unternehmens und die rollenbasierte Sicherheit, um unterschiedliche Ebenen des Zugriffs für unterschiedliche Benutzer innerhalb Ihres Unternehmens bereitzustellen.

Von Sterling B2B Integrator werden die folgenden Sicherheitsfunktionen bereitgestellt:

- Die rollenbasierte Sicherheit ermöglicht Benutzern den Zugriff auf bestimmte Dateien, Geschäftsprozesse, Webvorlagen, Dienste und Produktfunktionen auf der Basis der Berechtigungen, die dem betreffenden Benutzerkonto zugeordnet sind.
- Bei Kennwortrichtlinien handelt es sich um Gruppen von Sicherheitsentscheidungen, die Sie treffen und auf unterschiedliche Benutzerkonten gemäß den Sicherheitsrichtlinien Ihres Unternehmens anwenden. Die Entscheidungen betreffen Bereiche wie z. B. die Anzahl der Tage, die ein Kennwort gültig ist, oder die maximale oder minimale Länge eines Kennworts.
- Sie können die LDAP-Authentifizierung verwenden, um die Authentifizierung eines externen Benutzerkontos an ein LDAP-Verzeichnis zu delegieren und die Authentifizierung anhand der gleichen Sicherheitsinformationen zu ermöglichen, die für andere Anwendungen in Ihrem Unternehmen verwendet werden. Wenn Ihr Unternehmen bereits LDAP verwendet, dann können Sie die bereits bestehenden LDAP-Verzeichnisse für die Anwendung benutzen.
- Kennphrase für Systeminstallation - Während der Installation erstellen Sie eine Systemkennphrase für Ihre Sterling B2B Integrator-Installation. Die Kennphrase ist eine sehr komplexe Zeichenfolge mit mehr als 16 Zeichen. Die Systemkennphrase ist erforderlich, um das System starten und auf geschützte Systeminformationen zugreifen zu können.
- Unterstützung für x.509-Zertifikate für die Verschlüsselung, das Signieren und die Sicherheit in der Transportschicht.
- Gemäß Federal Information Processing Standards (FIPS) 140-2 zertifiziertes Softwaremodul und Unterstützung für auf der Basis von FIPS 140-2 zertifizierter Hardware aus nCipher und SafeNet.
- Secure Socket Layering (SSL) und Transport Layer Security (TLS).

Zusätzlich können die folgenden Sicherheitsfunktionen konfiguriert werden:

- Die Sicherheitszeitlimitfunktion bietet Ihnen die Möglichkeit, Zeitlimits für Benutzersitzungen zu konfigurieren.
- Die Funktion für angepasste Kennwortrichtlinien ermöglicht Ihnen das Hinzufügen zusätzlicher Kennwortrichtlinienregeln. Diese zusätzlichen Kennwortregeln können Sie dabei unterstützen, die Verwendung schwacher, leicht zu hackender Kennwörter zu verhindern und nicht den Bildungsregeln entsprechende Kennwörter zurückzuweisen.
- Bei der SSO-Funktion (SSO = Single Sign-on) handelt es sich um einen Authentifizierungsprozess, mit dem Benutzer auf mehrere Anwendungen zugreifen und dazu nur einmal den Benutzernamen und das Kennwort eingeben müssen.

- Die Funktion für die Dokumentverschlüsselung ermöglicht die Konfiguration einer zusätzlichen Sicherheitsebene, die über die traditionellen Datei- und Datenbankberechtigungen hinausgeht.

Rollenbasierte Sicherheit

Überblick zur rollenbasierten Sicherheit

Die rollenbasierte Sicherheit ermöglicht Benutzern den Zugriff auf bestimmte Dateien, Geschäftsprozesse, Webvorlagen, Dienste und Produktfunktionen auf der Basis der Berechtigungen, die dem betreffenden Benutzerkonto zugeordnet sind.

Um zu verstehen, wie die rollenbasierte Sicherheit verwaltet wird, müssen Sie sich mit der Art und Weise vertraut machen, wie Gruppen, Berechtigungen und Benutzerkonten interagieren.

- Berechtigungen bieten Zugriff auf Benutzerschnittstellenseiten und die auf diesen Seiten bereitgestellte Funktionalität.
- Bei Gruppen handelt es sich um Sammlungen von Berechtigungen.
- Benutzerkonten werden bestimmten Berechtigungen und Kennwortrichtlinien zugeordnet.

Die Verwaltung der rollenbasierten Sicherheit umfasst die folgenden Tasks:

- Berechtigungen erstellen
- Gruppen erstellen
- Kennwortrichtlinien erstellen
- Benutzerkonten erstellen

Gruppen

Bei Gruppen handelt es sich um Sammlungen von Berechtigungen. Gruppen ermöglichen die zentrale Verwaltung von Zugriffsberechtigungen für mehrere Benutzer. Gruppen tragen außerdem zur Reduzierung des Arbeitsaufwands bei, der beim Verwalten von Benutzerkonten insbesondere dann entsteht, wenn Benutzer den gleichen Aufgabenbereich haben.

Sie können viele Berechtigungen unterschiedlichen Benutzern zuordnen, indem Sie Gruppen für jeden Aufgabenbereich anstatt für jeden Benutzer erstellen. Sie können eine Gruppe auch als Untergruppe einer anderen Gruppe zuordnen.

Beispiel: Eine Beschaffungsabteilung, der fünf Beschaffungsfachleute angehören, die alle denselben Job ausführen. Anstatt Berechtigungen für das Benutzerkonto der einzelnen Beschaffungsfachleute einzeln anzuwenden, können Sie eine Beschaffungsgruppe erstellen und die Zugriffsberechtigungen für alle diese Mitarbeiter in einer Gruppe verwalten. Innerhalb der Beschaffungsgruppe können Sie Untergruppen zuordnen, um Ihre Zugriffsberechtigungen auf der Basis des speziellen Beschaffungsbereichs, für den der jeweilige Mitarbeiter zuständig ist, weiter zu differenzieren. Sie können der Beschaffungsgruppe z. B. Untergruppen zuordnen, die die Bereiche 'Bürobedarf', 'Maschinen', 'Betriebseinrichtung' oder 'Fahrzeuge' abdecken, um die Zugriffsberechtigungen zu differenzieren.

Um Überschreibungen zu vermeiden, wenn Upgrades oder Patches angewendet werden, sollten die Gruppen, die vorkonfiguriert zum Lieferumfang des Systems gehören, nicht geändert werden.

Es gibt die folgenden Gruppentasks:

- Gruppe erstellen
- Gruppe suchen
- Gruppe bearbeiten
- Gruppe löschen

Vorkonfigurierte Gruppen

Um Benutzern Berechtigungen zuzuordnen, können Sie die vorkonfigurierten Gruppen zuordnen. Benutzer übernehmen alle Berechtigungen, die den Gruppen zugeordnet sind. Eine vordefinierte Gruppe kann einem Benutzer zugeordnet werden, wenn für das Benutzerkonto der Zugang und das Thema definiert werden.

Zum Erstellen von Gruppen müssen Sie über die Berechtigung für das Modul 'Konten' verfügen.

Namenskonventionen für Gruppen

Beim Zuweisen von Gruppennamen sind bestimmte Namenskonventionen zu beachten.

Verwenden Sie für Gruppen die folgenden Namenskonventionen:

- Gruppen-IDs müssen unterschiedlich sein.
- Bei den Namen ist die Groß-/Kleinschreibung zu beachten.
- Zwei Gruppennamen mit unterschiedlicher Groß-/Kleinschreibung werden als unterschiedliche Namen betrachtet.
- Wenn ein Gruppenname verwendet wurde, dann kann er nicht als Name einer neuen Gruppe verwendet werden. Es wird eine Fehlernachricht angezeigt.

Gruppen suchen

Ein Gruppe können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Gruppe zu suchen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Gruppen** aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Geben Sie unter 'Suchen' im Feld **Gruppenname** einen Teil des Namens oder die vollständige Zeichenfolge für **Gruppenname** ein, nach dem bzw. der Sie suchen möchten, und klicken Sie auf **Los!**. Auf der Seite 'Gruppen' werden alle Gruppen aufgelistet, die mit den Suchkriterien übereinstimmen.
   - Wählen Sie unter 'Auflisten' die Option ALLE oder (im Feld **Alphabetisch**) den Buchstaben aus, mit dem der Name der Gruppe beginnt, die Sie suchen möchten, und klicken Sie auf **Los!**. Auf der Seite 'Gruppen' werden alle Gruppen aufgelistet, die mit den Suchkriterien übereinstimmen.

Gruppen erstellen

Eine Gruppe können Sie über das **Verwaltungsmenü** erstellen.

Informationen zu diesem Vorgang

Bevor Sie mit der Erstellung von Gruppen beginnen können, benötigen Sie die folgenden Informationen:

- Gruppen-ID der zu erstellenden Gruppe.

- Gruppenname der zu erstellenden Gruppe.
- Name des Eigners der Gruppe.
- Identität des Handelspartners, der der Gruppe zugeordnet werden soll. Einer Gruppe kann nur ein Handelspartner zugeordnet werden. Ein Benutzerkonto kann jedoch mehreren Gruppen zugeordnet werden. Dadurch ist es für ein Benutzerkonto möglich, mehreren Handelspartnern zugeordnet zu sein. Das Identitätsfeld wird zum Weiterleiten von Nachrichten in die Mailbox verwendet.

Gehen Sie wie folgt vor, um eine Gruppe zu erstellen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Gruppen** aus.
2. Klicken Sie neben **Neue Gruppe erstellen** auf **Los!**.
3. Geben Sie auf der Seite 'Neue Gruppe' die **Gruppen-ID** ein.
4. Geben Sie einen Wert für **Gruppenname** ein.
5. Geben Sie den **Inhaber** (Eigner) ein.
6. Wählen Sie die **Identität** aus.
7. Klicken Sie auf **Weiter**.
8. Wenn Sie Gruppen nach dem Namen filtern möchten, dann geben Sie auf der Seite 'Untergruppen zuweisen' unter 'Daten filtern' im Feld **Nach Name** einen Teil des Namens oder den gesamten Namen der Gruppe ein, für die die Filterung durchgeführt werden soll, und klicken Sie dann auf die Filterungsschaltfläche.
9. Wählen Sie die Gruppen aus, die dieser Gruppe zugewiesen werden sollen. Verschieben Sie die Gruppen aus dem Teilfenster 'Verfügbar' in das Teilfenster 'Zugeordnet'.
10. Klicken Sie auf **Weiter**.
11. Auf der Seite 'Berechtigungen zuweisen' müssen Sie angeben, ob Berechtigungen gefiltert werden sollen.
    - Um eine Filterung nach Namen durchzuführen, müssen Sie unter 'Daten filtern' im Feld **Nach Name** einen Teil des Namens oder den gesamten Namen der Berechtigung eingeben, für die die Filterung durchgeführt werden soll, und dann auf die Filterungsschaltfläche rechts neben dem Feld **Nach Typ** klicken.
    - Um eine Filterung nach Typ durchzuführen, müssen Sie unter 'Daten filtern' in der Liste 'Nach Typ' den Typ der Berechtigung auswählen, für die die Filterung durchgeführt werden soll, und dann auf die Filterungsschaltfläche rechts neben dem Feld **Nach Typ** klicken.
12. Wählen Sie die Berechtigungen aus, die dieser Gruppe zugewiesen werden sollen. Verschieben Sie die Berechtigungen aus dem Teilfenster 'Verfügbar' in das Teilfenster 'Zugeordnet'. Standardmäßig sind die Berechtigungen der Untergruppen, die dieser Gruppe zugeordnet sind, bereits ausgewählt. Die zugeordneten Berechtigungen werden in der Spalte für die verfügbaren Elemente nicht angezeigt. Stattdessen werden sie auf der Bestätigungsseite angezeigt.
13. Klicken Sie auf **Weiter**.
14. Überprüfen Sie die Gruppeninformationen.
15. Klicken Sie auf **Fertig stellen**.

Gruppen bearbeiten

Sie können Gruppen bearbeiten, um Einstellungen, Untergruppen und Berechtigungen zu aktualisieren.

Informationen zu diesem Vorgang

Bei der Bearbeitung von Gruppen können die folgenden Elemente aktualisiert werden:

- Einstellungen
- Untergruppen
- Berechtigungen

Die Gruppen-ID kann nicht geändert werden. Wenn Sie die Gruppen-ID ändern müssen, dann müssen Sie eine neue Gruppe erstellen.

Gehen Sie wie folgt vor, um eine Gruppe zu bearbeiten:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Gruppen** aus.
2. Suchen Sie nach der zu bearbeitenden Gruppe und verwenden Sie hierzu entweder die Gruppensuche über Name oder die alphabetische Liste. Klicken Sie anschließend auf **Los!**.
3. Wählen Sie für die Gruppe, die aktualisiert werden soll, **Bearbeiten** aus.
4. Aktualisieren Sie die gewünschte Gruppeneinstellung und klicken Sie dann auf **Weiter**.
5. Aktualisieren Sie die zugeordneten Untergruppen und klicken Sie dann auf **Weiter**.
6. Aktualisieren Sie die zugeordneten Berechtigungen und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Weiter**.
8. Überprüfen Sie die Gruppeninformationen.
9. Klicken Sie auf **Fertig stellen**.

Gruppen löschen

Gruppen können Sie über das **Verwaltungsmenü** löschen.

Informationen zu diesem Vorgang

Sie können die Sterling B2B Integrator-Berechtigung 'Admin group' oder 'UI Accounts' eines Benutzers mit Administratorberechtigung nicht entfernen. Diese Berechtigungen ermöglichen dem Systemadministrator die Verwaltung des Systems.

Gehen Sie wie folgt vor, um eine Gruppe zu löschen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Gruppen** aus.
2. Suchen Sie auf der Seite 'Gruppen' die Gruppe, die gelöscht werden soll. Verwenden Sie hierzu die Option 'Suchen' oder 'Auflisten'.
3. Klicken Sie auf der Seite 'Gruppen' neben der Gruppe, die gelöscht werden soll, auf **Löschen**.

   Das System löscht die Gruppe und zeigt die folgende Nachricht an:

   ```
   Die Systemaktualisierung wurde erfolgreich ausgeführt.
   ```

Gruppenname und ID überprüfen

Einen Gruppennamen und die zugehörige ID können Sie über das **Verwaltungsmenü** überprüfen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um einen Gruppennamen und die zugehörige ID zu überprüfen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konto** > **Gruppe** aus.
2. Suchen Sie auf der Seite 'Gruppe' die Gruppe, die überprüft werden soll. Verwenden Sie hierzu die Option 'Suchen' oder 'Auflisten'.
3. Wählen Sie die Gruppe aus. Daraufhin werden der Gruppenname und die ID angezeigt.

Berechtigungen

Berechtigungen ermöglichen den Zugriff auf die verschiedenen Module innerhalb von Sterling B2B Integrator und bilden die Grundlage der rollenbasierten Sicherheit. Die Berechtigungen eines Benutzers bestehen aus Berechtigungen von Gruppen und allen weiteren Berechtigungen, die einzeln zugewiesen wurden.

Verwenden Sie Berechtigungen zur Ausführung der folgenden Arbeitsschritte:

- Zentrale Verwaltung des Zugriffs mehrerer Benutzer.
- Verwaltung von Benutzerkonten mit minimalem Aufwand, insbesondere für mehrere Benutzer, denen der gleiche Aufgabenbereich zugeordnet ist.

In Bezug auf Berechtigungen können die folgenden Tasks ausgeführt werden:

- Erstellen einer Berechtigung
- Suchen einer Berechtigung
- Bearbeiten eines Berechtigungsnamens
- Löschen einer Berechtigung

Bevor Sie eine Berechtigung erstellen, bearbeiten oder löschen können, müssen Sie entscheiden, welche Module die Benutzer in dieser Gruppe benötigen bzw. nicht benötigen, um die ihnen zugewiesenen Funktionen ausführen zu können. Zum Erstellen von Berechtigungen muss Ihnen die Berechtigung für das Modul 'Konten' zugewiesen worden sein.

Um Überschreibungen zu vermeiden, wenn Upgrades oder Patches angewendet werden, sollten die Berechtigungen, die vorkonfiguriert zum Lieferumfang des Systems gehören, nicht geändert werden. Wenn angepasste Gruppierungen von Berechtigungen erforderlich sind, dann erstellen Sie eine neue Gruppe.

Namenskonventionen für Berechtigungen

Bei den Namen von Berechtigungen muss die Groß-/Kleinschreibung beachtet werden und die Namen dürfen nicht doppelt vorhanden sein.

Für Berechtigungen gelten die folgenden Namenskonventionen:

- Bei Berechtigungsnamen muss die Groß-/Kleinschreibung beachtet werden. Zwei identische Namen mit unterschiedlicher Groß-/Kleinschreibung werden als eindeutige Namen behandelt. Beispielsweise sind 'Beliebiges Dokument' und 'beliebiges Dokument' zwei unterschiedliche Berechtigungsnamen.
- Wenn ein Name für eine vorhandene Berechtigung verwendet wurde, dann kann er nicht als Name einer neuen Berechtigung verwendet werden. Es wird eine Fehlernachricht angezeigt.

Es ist zwar möglich, zwei Berechtigungen denselben Namen mit unterschiedlicher Groß-/Kleinschreibung zuzuweisen; diese Vorgehensweise wird aber nicht empfohlen.

Von Gruppen übernommene Berechtigungen

Im Folgenden werden vorinstallierte Gruppen und die Berechtigungen aufgelistet, die übernommen werden, wenn eine Berechtigungsgruppe einem bestimmten Benutzerkonto zugeordnet wird. Dieselben Berechtigungen werden übernommen, wenn eine Gruppe als Untergruppe zugeordnet wird.

Jede Gruppe enthält Berechtigungen für Menüelemente und die entsprechende Berechtigung für die Benutzerschnittstelle (UI = User Interface), die verwendet wird, um den Zugriff auf die Seite zu gewähren. EBXML enthält z. B. die Berechtigung 'UI EBXML'.

Gruppenname	**Gruppen-ID**	**Von der Gruppe übernommene Berechtigungen**
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	Alle Berechtigungen aus der Untergruppe BPMONITOR plus die Berechtigungen 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.
Abnormal Event Notification	eventAbnormal	Keine
Accounts	acctadmin	Alle Berechtigungen aus der Untergruppe ACCOUNTS plus die Berechtigungen UI Groups, UI User Accounts.
Alert Notifications	notifications	Keine
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.
Business Process	bpadmin	Alle Berechtigungen aus den Untergruppen BPMONITOR und SERVICES plus die Berechtigungen UI BP Manager, UI Business Process, UI Delete BP.
CD Server Proxy Administrator	cdsp_admin	Alle Berechtigungen aus den Untergruppen ACCOUNTS, BPMONITOR, CD Server Proxy User, OPERATIONS und SERVICES plus die Berechtigungen UI Groups, UI Licenses, UI Password Policy, UI SQL Tool, UI User Accounts.
CD Server Proxy User	cdsp_user	Diese Gruppe ist standardmäßig zugeordnet, wenn ein Benutzerkonto mit CDSP-Zugriffsmöglichkeit erstellt wird. Alle Berechtigungen aus den Untergruppen ACCOUNTS, BPMONITOR, OPERATIONS und SERVICES plus die Berechtigungen 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.

Gruppenname	Gruppen-ID	Von der Gruppe übernommene Berechtigungen
Command-Line User	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.
Dashboard Users	dashboardUsers	Diese Gruppe ist standardmäßig zugeordnet, wenn ein Benutzerkonto mit Dashboard-UI-Zugriffsmöglichkeit und den folgenden Dashboardschemas erstellt wird: • AFT • Standard • Community Management Operator, Participant, Participant Sponsor, oder 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.
Deployment	deploymentadmin	Alle Berechtigungen aus den Untergruppen ADAPTER_UTILITIES, DEPLOYMENT, EBXML, MAILBOX, MAPS, SERVICES, WEB_EXTENSIONS und WEB_SERVICES plus die Berechtigungen 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 Administrators	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.
EBICS Operators	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.
Exceptional Event Notifications	eventExceptional	Keine

Gruppenname	Gruppen-ID	Von der Gruppe übernommene Berechtigungen
MAILBOX	MAILBOX	Configuration, Messages, Routing Rules, UI Mailbox, VirtualRoots.
MAPS	MAPS	ExtendedRuleLibraries, Maps, Standards, UI Maps.
Mailbox Administrators	mboxadmins	Alle Berechtigungen aus den Gruppen MAILBOX und Mailbox Browser Interface Users plus die Berechtigungen DeadLetter Mailbox, Mailbox Global Delete, Mailbox Global Query, EBICS_DEADLETTER Mailbox.
Mailbox Browser Interface Users	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.
Provisional Trading Partners	provisionalpartners	Keine
SERVICES	SERVICES	Configuration, Installation/Setup, UI Services.
SSH	SSH	AuthorizedUserKey, KnownHostKey, RemoteProfiles, UI SSH, UserIdentityKey.
Session Demo Web Suite Buyer	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.
Session Demo Web Suite Suppliers	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.

Gruppenname	Gruppen-ID	Von der Gruppe übernommene Berechtigungen
Sterling B2B Integrator Admin	super	Alle Berechtigungen aus den Untergruppen ACCOUNTS, ADAPTER_UTILITIES, ADVANCED_SETUP, BPMONITOR, DEPLOYMENT, EBXML, ENVELOPES, MAILBOX, MAPS, Mailbox Administrators, OPERATIONS, SERVICES, SSH, WEB_EXTENSIONS und WEB_SERVICES plus die Berechtigungen UI Archive, UI AS2 Trading Profile Setup, UI Basic Trading Profile Setup, UI BP Manager, UI Business Process, UI CA Certs, UI CodeLists, UI Connect:Direct, UI Contracts, UI Delete BP, UI Delete CPA and CPSS Schema/Extension, UI Delete Map, UI Delete PGP Profile, UI Delete SAP Routes, UI Delete Schema, UI Delete Service Instance, UI Delete SWIFTNet Routing Rule, UI Delete Trading Partner Data, UI Delete Web Resource, UI Delete Web Templates, UI Delete WSDL, UI Delete XSLT Template, UI Federated, UI Generate/Download WAR Files, UI Groups, UI Import/Export, UI Licenses, UI Lock Manager, UI Logs, UI Notify, UI Perimeter Servers, UI PGP Profile Manager, UI Reports, UI Scheduler, UI Schemas, UI SQL Tool, UI SSH Local Identity Key, UI Support Case Tool, UI SWIFTNet Routing Rule, UI System Certs, UI Trading Partners, UI Trusted Certs, UI User Accounts, UI XSLT.
System Operations	operator	Alle Berechtigungen aus der Untergruppe OPERATIONS plus die Berechtigungen 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.
Trading Profiles	tpadmin	Alle Berechtigungen aus den Untergruppen ADVANCED_SETUP, ENVELOPES und SSH plus die Berechtigungen 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 Suite Buyers	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.

Gruppenname	Gruppen-ID	Von der Gruppe übernommene Berechtigungen
Web Suite Employees	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 Suite Finance	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.
Web Suite Human Resources	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 Suite Managers	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 Suite Purchasers	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.

Gruppenname	Gruppen-ID	Von der Gruppe übernommene Berechtigungen
Web Suite Suppliers	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.

Für Zugriff auf Benutzerschnittstellenressourcen benötigte Berechtigungen

Im Folgenden wird die mindestens erforderliche Gruppe von Berechtigungen aufgeführt, die ein Benutzer für den Zugriff auf ein Menüelement und die zugehörige Seite und Funktionalität benötigt. Durch die Zuweisung der mindestens erforderlichen Gruppe von Berechtigungen werden möglicherweise weitere Funktionen für den Benutzer bereitgestellt. Wenn Sie nicht über die Berechtigung für ein Menüelement und die zugehörige Funktionalität verfügen, dann wird es nicht angezeigt.

Über 'Verwaltungsmenü > Geschäftsprozess, UI Resource'	Berechtigungsname / Berechtigungs-ID
Geschäftsprozess > Manager	UI BP Manager (BPMANAGE) plus UI Business Process (BUSINESS_PROCESS)
Geschäftsprozess > Überwachen > Erweiterte Suche > Geschäftsprozess	BusinessProcesses (PLTADM2) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > SWIFTNet-Korrelation	SWIFTNETCorrelation (GISADM9) plus UI BP Monitor (BPMONITOR) und UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
Geschäftsprozess > Überwachen > Erweiterte Suche > Datenflüsse	DataFlows (GISADM1) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > Dokumente	Documents (GISADM2) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > Kommunikationssitzungen	Communication Sessions (GISADM3) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > Korrelation	Correlation (GISADM4) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > BPSS-Korrelation	BPSSCorrelations (GISADM5) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > EBXML-Korrelation	EBXMLCorrelation (GISADM6) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Erweiterte Suche > EDI-Korrelation	EDICorrelation (GISADM7) plus UI BP Monitor (BPMONITOR)

Über 'Verwaltungsmenü > Geschäftsprozess, UI Resource'	**Berechtigungsname / Berechtigungs-ID**
Geschäftsprozess > Überwachen > Erweiterte Suche > EDIINT	EDIINT (STDSADM6) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Zentrale Suche	CentralSearch (GISADM10) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Aktuelle Prozesse	CurrentProcesses (PLTADM3) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Aktuelle Dokumente	CurrentDocuments (GISADM11) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Überwachen > Aktuelle Aktivitäten	CurrentActivities (PLTADM4) plus UI BP Monitor (BPMONITOR)
Geschäftsprozess > Workstation für Nachrichteneinträge	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

Über 'Verwaltungsmenü > Handelspartner, UI Resource'	**Berechtigungsname / Berechtigungs-ID**
Handelspartner > Setup > Standard	UI Basic Trading Profile Setup (BASIC_SETUP)
Handelspartner > Setup > Erweitert > Identitäten	Identities (GISADM12) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP) Für Löschoperationen ist außerdem die Berechtigung UI Delete Trading Partner (TP_DELETE) erforderlich.
Handelspartner > Setup > Erweitert > Transporte	Transports (GISADM13) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP) Für Löschoperationen ist außerdem die Berechtigung UI Delete Trading Partner (TP_DELETE) erforderlich.
Handelspartner > Setup > Erweitert > Dokumentaustausch	DocumentExchange (GISADM14) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP) Für Löschoperationen ist außerdem die Berechtigung UI Delete Trading Partner (TP_DELETE) erforderlich.
Handelspartner > Setup > Erweitert > Zustellungskanäle	DeliveryChannels (GISADM15) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP) Für Löschoperationen ist außerdem die Berechtigung UI Delete Trading Partner (TP_DELETE) erforderlich.
Handelspartner > Setup > Erweitert > Packaging	Packaging (GISADM16) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP) Für Löschoperationen ist außerdem die Berechtigung UI Delete Trading Partner (TP_DELETE) erforderlich.

Über 'Verwaltungsmenü > Handelspartner, UI Resource'	Berechtigungsname / Berechtigungs-ID
Handelspartner > Setup > Erweitert > Profile	Profiles (GISADM17) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP) Für Löschoperationen ist außerdem die Berechtigung UI Delete Trading Partner (TP_DELETE) erforderlich.
Handelspartner > Digitale Zertifikate > CA	UI CA Certs (CA_CERTS) plus UI System Certs (SYSTEM_CERTS) UI Mit System Certs wird die Option 'System' hinzufügt.
Handelspartner > Digitale Zertifikate > Vertrauenswürdig	UI Trusted Certs (TRUSTED_CERTS)
Handelspartner > Digitale Zertifikate > System	UI System Certs (SYSTEM_CERTS)
Handelspartner > Dokument-Envelopes > Envelopes	Envelopes (STDSADM1) plus UI Envelope (ENVELOPE)
Handelspartner > Dokument-Envelopes > Kontrollnummern	ControlNumbers (STDSADM2) plus UI Envelope (ENVELOPE)
Handelspartner > Dokument-Envelopes > Transaktionsregister	TransactionRegister (STDSADM3) plus UI Envelope (ENVELOPE)
Handelspartner > Dokument-Envelopes > Kontrollnummernprotokoll	ControlNumberHistory (STDSADM4) plus UI Envelope (ENVELOPE)
Handelspartner > Dokument-Envelopes > Warteschlange der EDI-Sequenzprüfung	EDISequenceCheckQueue (STDSADM5) plus UI Envelope (ENVELOPE)
Handelspartner > Verträge	UI Contracts (CONTRACTS) plus UI Advanced Trading Partner Setup (ADVANCED_SETUP)
Handelspartner > Codelisten	UI CodeLists (CODELISTS)
Handelspartner > AS2	UI AS2 Trading Profile Setup (AS2_SETUP)
Handelspartner > SSH > Ferne Profile	RemoteProfiles (ASSETADM1) plus UI SSH
Handelspartner > SSH > Bekannter Hostschlüssel	KnownHostKey (ASSETADM2) plus UI SSH
Handelspartner > SSH > Benutzeridentitätsschlüssel	UserIdentityKey (ASSETADM3) plus UI SSH
Handelspartner > SSH > Autorisierter Benutzerschlüssel	AuthorizedUserKey (ASSETADM4) plus UI SSH
Handelspartner > AS3	UI AS3 Trading Profile Setup (AS3_SETUP)
Handelspartner > Odette-FTP-Partnerprofil > Physischer Partner	OftpPhysicalPartner (ASSETOFTP1) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Handelspartner > Odette-FTP-Partnerprofil > Physischer Partnervertrag	OftpPhysicalPartnerContract (ASSETOFTP3) plus UI Adapter Utilities (ADAPTER_UTILITIES)

Über 'Verwaltungsmenü > Handelspartner, UI Resource'	Berechtigungsname / Berechtigungs-ID
Handelspartner > Odette-FTP-Partnerprofil > Logischer Partner	OftpLogicalPartner (ASSETOFTP2) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Handelspartner > Odette-FTP-Partnerprofil > Logischer Partnervertrag	OftpLogicalPartnerContract (ASSETOFTP4)
Handelspartner > PGP > PGP-Servermanager	PGP Server Manager (ASSETADM55) plus UI PGP Profile Manager (PGP)
Handelspartner > PGP > PGP-Sponsormanager	PGP Sponsor Manager (ASSETADM56) plus UI PGP Profile Manager (PGP)
Handelspartner > PGP > PGP-Partnermanager	PGP Partner Manager (ASSETADM57) plus UI PGP Profile Manager (PGP)

Über 'Verwaltungsmenü > Bereitstellung, UI Resource'	Berechtigungsname / Berechtigungs-ID
Bereitstellung > Dienste > Installation/Setup	Installation/Setup (PLTADM9) plus UI Services (SERVICES)
Bereitstellung > Dienste > Konfiguration	Configuration (PLTADM10) plus UI Services (SERVICES), UI BP Manager (BPMANAGE). Ab V5.2.4.3 und höher ist UI Adapters StartStop ebenfalls erforderlich.
Bereitstellung > Zeitpläne	UI Scheduler (SCHEDULER)
Bereitstellung > Maps	Maps (ASSETADM5) plus UI_Maps
Bereitstellung > Standards	Standards (STDSADM7) plus UI_Maps
Bereitstellung > Erweiterte Regelbibliotheken	ExtendedRuleLibraries (ASSETADM6) plus UI_Maps
Bereitstellung > XSLT	UI XSLT (XSLT)
Bereitstellung > Weberweiterungen > Webressourcen	WebResources (GISADM19) plus UI Web Extensions und UI Web Services (WEB_SERVICES) UI Web Services ermöglicht dem Benutzer das Einchecken einer Webressourcendatei.
Bereitstellung > Weberweiterungen > Dienstprogramme	Utilities (GISADM20) plus UI Web Extensions Nur sichtbar bei Upgrade von früherer Version.
Bereitstellung > Schemas	UI Schemas (SCHEMAS)
Bereitstellung > Mailboxen > Konfiguration	Configuration (MBXADM1) plus UI Mailbox (MAILBOX)
Bereitstellung > Mailboxen > Virtuelle Stammverzeichnisse	VirtualRoots (MBXADM2) plus UI Mailbox (MAILBOX)
Bereitstellung > Mailboxen > Weiterleitungsregeln	RoutingRules (MBXADM3) plus UI Mailbox (MAILBOX)
Bereitstellung > Mailboxen > Nachrichten	Messages (MBXADM4) plus UI Mailbox (MAILBOX)
Bereitstellung > EBXML > BPSS	BPSS (ASSETADM7) plus UI EBXML (EBXML)

Über 'Verwaltungsmenü > Bereitstellung, UI Resource'	Berechtigungsname / Berechtigungs-ID
Bereitstellung > EBXML > BPSS-Erweiterung	BPSSExtension (ASSETADM8) plus UI EBXML (EBXML)
Bereitstellung > EBXML > CPA	CPA (ASSETADM9) plus UI EBXM (EBXML)
Bereitstellung > Ressourcen-Manager > Ressourcen-Tags	Resource Tags (PLTADM1) plus UI Deployment (DEPLOYMENT)
Bereitstellung > Ressourcen-Manager > Import/Export	UI Import/Export (IMPORT_EXPORT)
Bereitstellung > Adapter-Dienstprogramme > SAP Suite Builder	SAPSuiteBuilder (ASSETADM10) plus UI Adapter Utilities
Bereitstellung > Adapter-Dienstprogramme > SAP-Routen > SAP-Routen	SAPRoutes (ASSETADM11) plus UI Adapter Utilities
Bereitstellung > Adapter-Dienstprogramme > SAP-Routen > SapRouteXRef	SAPRouteXREF (ASSETADM12) plus UI Adapter Utilities
Bereitstellung > Adapter-Dienstprogramme > BEATuxedo	BEATuxedo (ASSETADM13) plus UI Adapter Utilities Das Menüelement wird nur angezeigt, wenn die BEATuxedo-JAR-Datei installiert ist.
Bereitstellung > Adapter-Dienstprogramme > SWIFTNet-Weiterleitungsregeln	UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
Bereitstellung > Adapter-Dienstprogramme > SWIFTNet-Dienstprofil	UI SWIFTNet Service Profile (SWIFTNET_SVC_PROFILE)
Bereitstellung > Adapter-Dienstprogramme > SWIFTNet-Kopierdienstprofil	UI SWIFTNet Copy Profile (SWIFTNET_COPY_PROFILE)
Bereitstellung > Adapter-Dienstprogramme > Lockout-Richtlinien-Manager	LockoutPolicyManager (ASSETADM50)
Bereitstellung > Adapter-Dienstprogramme > C:D-Netmaps > C:D-Knoten	CDNetmaps (ASSETADM51) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Bereitstellung > Adapter-Dienstprogramme > C:D-Netmaps > C:D-Netmaps	CDNodes (ASSETADM52) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Bereitstellung > Adapter-Dienstprogramme > C:D-Netmaps > C:D-Netmap-Querverweis	CDNetmapXref (ASSETADM53) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Bereitstellung > Adapter-Dienstprogramme > Richtlinienkonfiguration	Adapter Policies (ASSETADM54)
Bereitstellung > Adapter-Dienstprogramme > Virtuelles Stammverzeichnis für Dateisystem	File System Virtual Root (ASSETADM58)
Bereitstellung > SSH-Hostidentitätsschlüssel	UI SSH Local Identity Key (SSH_LCL_ID_KEY) und UI SSH (SSH)
Bereitstellung > Webdienste > Manager	WebServicesManager (ASSETADM16) und UI Web Services (WEB_SERVICES)
Bereitstellung > Webdienste > Schemazuordnungen	SchemaMappings (ASSETADM17), UI Web Services (WEB_SERVICES) und UI EBXML (EBXML)
Bereitstellung > Webdienste > WSDL einchecken	WSDLCheckIn (ASSETADM18) plus UI Web Services (WEB_SERVICES)
Bereitstellung > Webdienste > Sicherheitstoken	SecurityToken (ASSETADM18) plus UI Web Services (WEB_SERVICES)

Über 'Verwaltungsmenü > e-Invoicing, UI Resource'	Berechtigungsname / Berechtigungs-ID
e-Invoicing > Vereinbarungen	eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT) Für Löschoperation ist außerdem die Berechtigung eInvoicing DELETE AGREEMENT (EINV_DELETE_AGREEMENT) erforderlich.
e-Invoicing > Integriertes Archiv	eInvoicing Archive (EINVOICING_ARCHIVE) plus eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE)
e-Invoicing > Konfiguration	eInvoicing Configuration (EINVOICING_CONFIGURATION)

Über 'Verwaltungsmenü > Operationen, UI Resource'	Berechtigungsname / Berechtigungs-ID
System > Fehlerbehebung	Troubleshooter (PLTADM17) plus UI Operations (OPERATIONS)
System > Leistung > Optimierung	Tuning (PLTADM18) plus UI Operations (OPERATIONS)
System > Leistung > Statistik	Statistics (PLTADM19) plus UI Operations (OPERATIONS)
System > Leistung > JVM-Überwachung	Perfdumps (GISADMIN27) plus UI Operations (OPERATIONS)
System > Support-Tools > SQL-Manager	UI SQL Tool (SQLMANAGER)
System > Support-Tools > Supportfall	UI Support Case Tool (SUPPORT_CASE)
System > Protokolle	UI Logs (SYSTEM_LOGS)
System > Lizenzen	UI Licenses (LICENSES)
Berichte	UI Reports (REPORTS)
Threadüberwachung	ThreadMonitor (PLTADM24) plus UI Operations (OPERATIONS)
JDBC-Überwachung	JDBCMonitor (PLTADM25) plus UI Operations (OPERATIONS) und UI SQL Tool (SQLMANAGER)
Archivmanager	UI Archive (ARCHIVE-UI) plus UI Operations (OPERATIONS), UI BP Manage (BPMANAGE) und UI Business Process (BUSINESS_PROCESS)
Sperr-Manager	UI Lock Manager (LOCK_MANAGER)
Nachrichtenüberwachung	MessageMonitor (GISADM24) plus UI Operations (OPERATIONS)
Perimeterdienste	UI Perimeter Servers (PSERVERS)
Proxy-Server	UI Proxy Servers (PROXYSERVERS) plus Sterling B2B Integrator Admin group

Über 'Verwaltungsmenü > Konten, UI Resource'	Berechtigungsname / Berechtigungs-ID
Gruppen	UI Groups (GROUPS) plus UI Accounts (ACCOUNTS)

Über 'Verwaltungsmenü > Konten, UI Resource'	Berechtigungsname / Berechtigungs-ID
Berechtigungen	Permissions (PLTADM27) plus UI Accounts (ACCOUNTS)
Benutzerkonten	UI User Accounts (USER_ACCOUNTS) plus UI Accounts (ACCOUNTS)
Kennwortrichtlinie	PasswordPolicy (PLTADM29) plus UI Accounts (ACCOUNTS)
Benutzernachrichten	UserNews (GISADM25) plus UI Accounts (ACCOUNTS)
Eigenes Konto	MyAccount (PLTADM30)

Vorkonfigurierte Berechtigungen

Im Lieferumfang des Systems sind vorkonfigurierte Berechtigungen enthalten. Wie angepasste Berechtigungen bieten sie Zugriff auf die unterschiedlichen Module innerhalb des Systems.

Berechtigungsnamen suchen

Eine Berechtigung können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um nach einer Berechtigung suchen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Berechtigungen** aus.
2. Führen Sie auf der Seite 'Berechtigungen' eine der folgenden Aktionen durch:
   - Geben Sie unter 'Suchen' im Feld **Berechtigungsname** entweder einen Teil des Berechtigungsnamens oder den vollständigen Berechtigungsnamen ein, nach dem Sie suchen möchten, und klicken Sie dann auf **Los!**. Auf der Seite 'Berechtigungen' werden alle Berechtigungen aufgelistet, die mit Ihren Suchkriterien übereinstimmen.
   - Wählen Sie unter 'Auflisten' im Feld **Alphabetisch** die Option **ALLE** oder den Buchstaben aus, mit dem der Name der Berechtigung beginnt, nach der Sie suchen, und klicken Sie dann auf **Los!**. Auf der Seite 'Berechtigungen' werden alle Berechtigungen aufgelistet, die mit Ihren Suchkriterien übereinstimmen.

Berechtigungen erstellen

Wenn Sie ein Upgrade von einer Vorgängerversion des Systems durchgeführt haben, dann werden die vorhandenen Berechtigungen standardmäßig auf 'Andere' festgelegt. Sie müssen möglicherweise alle Berechtigungen bearbeiten, um einen neuen Berechtigungstyp anzuwenden.

Informationen zu diesem Vorgang

Bevor Sie beginnen können, benötigen Sie die folgenden Informationen:

Feld	Beschreibung
Berechtigungs-ID	Die Berechtigungs-ID für die Berechtigung, die Sie erstellen. Die Berechtigungs-ID ist der Name des Geschäftsprozesses, des XSLT-Dokuments, der Webvorlage oder der Ressource, für den, das bzw. die die Berechtigung definiert wird. Geben Sie nach der ID die Erweiterung für die Ressource an. Erforderlich. Für Berechtigungs-IDs gilt Folgendes: • Sie müssen eindeutig sein. • Die Groß-/Kleinschreibung muss beachtet werden. • Die Berechtigungs-ID muss mit dem Namen des Geschäftsprozesses, des XSLT-Dokuments, der Webvorlage oder der Ressource übereinstimmen. Wenn die Berechtigungs-ID und der Name der Ressource nicht exakt übereinstimmen, dann kann die Ressource nicht gesperrt werden.
Berechtigungsname	Der Name der Berechtigung, die Sie erstellen. Erforderlich. Berechtigungsnamen müssen eindeutig sein. Außerdem muss bei Berechtigungsnamen die Groß-/Kleinschreibung beachtet werden. Beispielsweise sind 'Beliebiges Dokument' und 'beliebiges Dokument' zwei unterschiedliche Berechtigungsnamen.
Berechtigungstyp	Der Berechtigungstyp der Berechtigung, die Sie erstellen. Erforderlich. Folgende Berechtigungstypen stehen zur Verfügung: • UI – Ermöglicht den Zugriff auf bestimmte Menüelemente in der Schnittstelle. • Mailbox – Ermöglicht den Zugriff auf bestimmte Mailboxen im System. • Vorlage - Ermöglicht den Zugriff auf bestimmte Webvorlagen. • GP - Ermöglicht den Zugriff auf bestimmte Geschäftsprozesse. • Verfolgung - Ermöglicht den Zugriff auf bestimmte Dokumentverfolgungsoptionen. • Community – Ermöglicht den Zugriff auf bestimmte Community-Management-Optionen. • Webdienst. • Dienst. • Elektronische Rechnungsstellung. • Andere - Ermöglicht den Zugriff auf Ressourcen, die keinem der vorher aufgeführten Typen zugeordnet werden können.

Gehen Sie wie folgt vor, um eine Berechtigung zu erstellen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Berechtigungen** aus.
2. Klicken Sie neben **Neue Berechtigung erstellen** auf **Los!**.
3. Geben Sie auf der Seite 'Berechtigungen' eine **Berechtigungs-ID** ein.
4. Geben Sie einen Wert für **Berechtigungsname** ein.
5. Wählen Sie einen **Berechtigungstyp** aus.
6. Klicken Sie auf **Weiter**.

7. Überprüfen Sie die Berechtigungseinstellungen.
8. Klicken Sie auf **Fertig stellen**.

Berechtigungsnamen bearbeiten

Wenn Sie den Namen einer Berechtigung ändern müssen, um die Berechtigung aussagekräftiger zu benennen, dann müssen Sie den Berechtigungsnamen bearbeiten. Berechtigungsnamen müssen eindeutig sein und die Groß-/Kleinschreibung muss beachtet werden. Die Berechtigungs-ID kann nicht geändert werden. Wenn Sie die Berechtigungs-ID bearbeiten müssen, dann müssen Sie eine neue Berechtigung erstellen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um einen Berechtigungsnamen zu bearbeiten:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Berechtigungen** aus.
2. Suchen Sie nach der zu bearbeitenden Berechtigung und verwenden Sie hierzu entweder die Berechtigungssuche über Name oder die alphabetische Liste. Klicken Sie anschließend auf **Los!**.
3. Klicken Sie neben der Berechtigung, die bearbeitet werden soll, auf **Bearbeiten**.
4. Geben Sie einen neuen Wert für **Berechtigungsname** ein.
5. Aktualisieren Sie den Berechtigungstyp (sofern erforderlich) und klicken Sie dann auf **Weiter**.
6. Überprüfen Sie die Informationen zu den Berechtigungseinstellungen.
7. Klicken Sie auf **Fertig stellen**.

Berechtigungen löschen

Sie können eine Berechtigung, die einem Benutzerkonto zugeordnet ist, löschen. Wenn Sie eine Berechtigung löschen, dann kann sie von keinem Benutzerkonto mehr verwendet werden.

Informationen zu diesem Vorgang

Wenn die Berechtigung, die Sie entfernen, die einzige Berechtigung eines Benutzerkontos ist, dann müssen Sie das Benutzerkonto bearbeiten und ihm eine andere Berechtigung zuordnen. Wenn Sie dem Benutzerkonto nicht mindestens eine neue Berechtigung zuordnen, kann sich der zugehörige Benutzer zwar anmelden, jedoch auf keines der Menüs zugreifen.

Gehen Sie wie folgt vor, um eine Berechtigung zu löschen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Berechtigungen** aus.
2. Suchen Sie nach der zu löschenden Berechtigung und verwenden Sie hierzu entweder die Berechtigungssuche über Name oder die alphabetische Liste. Klicken Sie anschließend auf **Los!**.
3. Klicken Sie auf der Seite 'Berechtigungen' für die zu löschende Berechtigung auf **Löschen**.
4. Überprüfen Sie, ob die Berechtigungsinformationen mit den Informationen zu der Berechtigung übereinstimmen, die gelöscht werden soll, und klicken Sie dann auf **Löschen**.

   Das System löscht die Berechtigung und zeigt die folgende Nachricht an:

```
Die Systemaktualisierung wurde erfolgreich ausgeführt.
```

Berechtigungsname und ID überprüfen

Einen Berechtigungsnamen und die zugehörige ID können Sie über das **Verwaltungsmenü** überprüfen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um einen Berechtigungsnamen und die zugehörige ID zu überprüfen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Berechtigungen** aus.
2. Suchen Sie nach der zu überprüfenden Berechtigung und verwenden Sie hierzu entweder die Berechtigungssuche über Name oder die alphabetische Liste. Klicken Sie anschließend auf **Los!**.
3. Wählen Sie die Berechtigung aus. Daraufhin werden der Berechtigungsname und die ID angezeigt.

Benutzerkonten

Benutzerkonten werden anhand von Gruppen, Berechtigungen und Kennwortrichtlinien definiert, mit deren Hilfe Sie eine sichere Umgebung bereitstellen können. Dieser Typ der Benutzerkontendefinition wird als rollenbasiertes Sicherheitsmodell definiert.

Bevor Sie neue Benutzerkonten erstellen, müssen Sie feststellen, welche Gruppen, Berechtigungen und Kennwortrichtlinien für ihr Geschäftsumfeld erforderlich sind. Die Zuweisung von Gruppen, Berechtigungen und Kennwortrichtlinien ist optional.

Nur über ein Konto, dem Erstellungsberechtigungen zugewiesen sind, können neue Benutzerkonten erstellt werden. Es gibt die folgenden Tasks für Benutzerkonten:

- Erstellen eines Benutzerkontos
- Suchen eines Benutzerkontos
- Bearbeiten eines Benutzerkontos
- Löschen eines Benutzerkontos

Standardberechtigungen für Benutzerkonten

Die Berechtigungen 'MyAccount' und 'Admin Web App' werden den Benutzerkonten automatisch zugeordnet.

Benutzerkonten werden automatisch die folgenden Berechtigungen zugeordnet:

- MyAccount (Berechtigungs-ID PLTADM30) – Erlaubt den Zugriff auf die Seite 'Eigenes Konto' (Konten > Eigenes Konto).
- Admin Web App Permissions (Berechtigungs-ID WebAppAdminPermission) - Wird für den Zugriff auf andere Webanwendungen benutzt.

Diese Berechtigungen dürfen nicht aus Benutzerkonten entfernt werden. Wenn Sie versehentlich entfernt werden, dann bearbeiten Sie das Benutzerkonto und speichern Sie es. Die fehlenden Berechtigungen werden dann wiederhergestellt.

Authentifizierung von Benutzerkonten

Die Authentifizierung von Benutzerkonten kann entweder lokal oder extern erfolgen.

Die Authentifizierung von Benutzerkonten kann auf eine der folgenden Arten durchgeführt werden:

- Lokal - Die Authentifizierung wird anhand der Datenbank ausgeführt.
- Extern - Die Authentifizierung wird anhand eines LDAP-Servers ausgeführt. Für die externe Authentifizierung ist kein LDAP-Adapter erforderlich, der bei Geschäftsprozessen verwendet wird, und dem System die Kommunikation mit lokalen oder fernen LDAP-Servern über JNDI (Java Naming and Directory Interface) ermöglicht. Wenn Sie nicht über eine Lizenz für Single Sign-on oder LDAP verfügen, handelt es sich bei sämtlichen von Ihnen erstellten Benutzern um lokale Benutzer, die anhand der Datenbank der Anwendung authentifiziert werden. Um ein externes Benutzerkonto erstellen zu können, müssen Sie über eine Anwendungslizenz für Single Sign-on oder LDAP verfügen.

Prüfliste für Erstellung von Benutzerkonten

Sie können ein Benutzerkonto erstellen.

Verwenden Sie die folgende Prüfliste, um ein Benutzerkonto zu erstellen:

Task	Prüfliste zur rollenbasierten Sicherheit	Ihre Notizen
1	Erstellen neuer Berechtigungen oder Überprüfen der vorkonfigurierten Berechtigungen, die bereits auf dem System vorinstalliert sind.	
2	Erstellen neuer Gruppen oder Überprüfen der Gruppen, die bereits auf dem System vorinstalliert sind.	
3	Erstellen einer angepassten Kennwortrichtlinie, die dem Benutzer zugewiesen werden soll.	
4	Bei Verwendung der externen Authentifizierung Einrichten der Umgebung für die externe Authentifizierung.	
5	Erstellen des Benutzerkontos und Zuweisen der Berechtigungen, Gruppen und Kennwortrichtlinien.	

Umgebung zur Authentifizierung externer Benutzerkonten einrichten

Wenn Sie einen externen Benutzer erstellen, dann können Sie eine alternative Authentifizierungsmethode (normalerweise LDAP) angeben.

Informationen zu diesem Vorgang

Vor der Erstellung eines externen Benutzerkontos müssen Sie die folgenden Arbeitsschritte ausführen:

Vorgehensweise

1. Stoppen Sie Sterling B2B Integrator.
2. Geben Sie die alternative Authentifizierungsmethode an, indem Sie die Authentifizierungskonfiguration in der Datei 'authentication_policy.properties.in' hinzufügen oder ändern. Die Eigenschaften müssen im folgenden Format angegeben werden: authentication_4.*xxx*=*xxx*_value.
3. Geben Sie `setupfiles.sh` ein.
4. Starten Sie Sterling B2B Integrator.

Nach Benutzerkonten suchen

Ein Benutzerkonto können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um nach einem Benutzerkonto zu suchen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzerkonten** aus.
2. Führen Sie eine der folgenden Aktionen aus:
   - Geben Sie unter 'Suchen' im Feld **Kontoname** entweder einen Teil des Namens oder den vollständigen Namen des Benutzerkontos ein, nach dem Sie suchen möchten, und klicken Sie dann auf **Los!**. Auf der Seite 'Konten' werden alle Benutzerkonten aufgelistet, die mit den Suchkriterien übereinstimmen.
   - Wählen Sie unter 'Auflisten' im Feld **Alphabetisch** die Option **ALLE** oder den Buchstaben aus, mit dem der Name des Benutzerkontos beginnt, nach dem Sie suchen, und klicken Sie dann auf **Los!**. Auf der Seite 'Konten' werden alle Benutzerkonten aufgelistet, die mit den Suchkriterien übereinstimmen.

Benutzerkonten erstellen

Ein neues Benutzerkonto können Sie über das **Verwaltungsmenü** erstellen.

Informationen zu diesem Vorgang

Bevor Sie beginnen, müssen Sie feststellen, ob Sie mit der lokalen oder der externen Authentifizierung arbeiten:

- Lokal - Die Authentifizierung wird anhand der Datenbank der Anwendung ausgeführt. Dies ist die Standardeinstellung.
- Extern - Die Authentifizierung wird anhand eines LDAP-Servers ausgeführt. Für die externe Authentifizierung wird kein LDAP-Adapter benötigt, der bei Geschäftsprozessen verwendet wird und dem System die Kommunikation mit lokalen oder fernen LDAP-Servern über JNDI (Java Naming and Directory Interface) ermöglicht.

Wenn Sie diesem Konto einen oder auch mehrere berechtigte Benutzerschlüssel zuordnen, dann müssen die Schlüssel von Ihrem Handelspartner angefordert werden und vor der Erstellung des Benutzerkontos eingecheckt werden.

Anmerkung: Obwohl mehrere Fremdsprachen unterstützt werden, sollte ein Benutzerkonto jeweils nur mit einer bestimmten Sprache verwendet werden, um Probleme mit der Anzeige der Benutzerschnittstelle zu vermeiden.

Außerdem benötigen Sie die folgenden Informationen:

Feld	Beschreibung
Benutzer-ID	Die Benutzer-ID für das Benutzerkonto, das Sie erstellen. Die Benutzer-ID muss aus mindestens fünf alphanumerischen Zeichen bestehen. Sonderzeichen oder Interpunktionszeichen sind nicht zulässig. Erforderlich. Nur für die MySQL-Datenbank muss bei der Anmeldung die Groß-/Kleinschreibung nicht beachtet werden. Sie sollten immer eindeutig geschriebene IDs verwenden, sodass nicht ein Benutzer unbeabsichtigt die ID eines anderen Benutzers verwendet.
Kennwort (nur bei lokaler Authentifizierung)	Das Kennwort für das Benutzerkonto, das Sie erstellen. Das Kennwort muss aus mindestens sechs alphanumerischen Zeichen bestehen. Sonderzeichen sind zulässig. Erforderlich für lokale Benutzer. Dieses Feld wird für externe Benutzer nicht angezeigt.
Kennwort bestätigen (nur bei lokaler Authentifizierung)	Geben Sie das Kennwort ein zweites Mal ein. Erforderlich für lokale Benutzer. Dieses Feld wird für externe Benutzer nicht angezeigt.
Richtlinie (nur bei lokaler Authentifizierung)	Die Kennwortrichtlinie, die diesem Benutzerkonto zugeordnet werden soll. Wählen Sie in der Liste die Richtlinie aus, die Sie zuordnen möchten. Optional. Dieses Feld wird für externe Benutzer nicht angezeigt. Das System berechnet das Ablaufdatum ab dem Datum der ersten Anmeldung des Benutzers mit diesem Kennwort.
Authentifizierungshost (nur bei externer Authentifizierung)	Der LDAP-Server (LDAP = Lightweight Directory Access Protocol), auf dem der Benutzer authentifiziert wird. Die in diesem Feld aufgelisteten Server werden in der Datei 'authentication_policy.properties.in' angegeben.
Sitzungszeitlimit	Die Zeitdauer in Minuten, die ein Benutzer inaktiv sein kann, bevor er sich erneut anmelden muss. Die Zeitdauer wird in Minuten angegeben. Erforderlich.
Zugang	Der Teil der Benutzerschnittstelle des Dashboards, auf den das Benutzerkonto zugreifen kann. Optional. Die Zugangsoptionen lauten wie folgt: • Admin-UI - Greift nur auf die Admin-Konsole im Dashboard zu. • AS2-UI - Greift nur auf die Schnittstelle der AS2-Edition zu. • Dashboard-UI - Greift auf die Schnittstelle des Dashboards zu. Diese Einstellung können Sie differenzieren, indem Sie ein Dashboardschema auswählen.

Feld	Beschreibung
Dashboardschema	Vordefiniertes Dashboard, auf das der Benutzer zugreifen kann. Erforderlich, wenn der Zugang auf "Dashboard-UI" festgelegt wurde. Im Folgenden sind Optionen für das Dashboardschema aufgeführt: • Standard • Operator • Teilnehmer • Teilnehmer-Sponsor • Sponsor • AFT
Vorname	Der Vorname des Benutzers. Erforderlich.
Nachname	Der Nachname des Benutzers. Erforderlich.
E-Mail	Die E-Mail-Adresse des Benutzers.
Pager	Die Pagernummer des Benutzers.
Bevorzugte Sprache	Geben Sie **Clientanwendungseinstellungen verwenden** an. **Anmerkung:** Dieser Wert weist Sterling B2B Integrator an, die Sprache zu verwenden, die im Browser des Benutzers und/oder der Ländereinstellung des Betriebssystems des Clients angegeben ist. **Anmerkung:** Dies ist der Standardwert.
Manager-ID	Die Benutzer-ID des Managers des Benutzers.
Identität	Die Identität des Handelspartners, der dem Benutzerkonto zugeordnet werden soll. Einem Benutzerkonto kann nur ein Handelspartner zugeordnet werden. Ein Benutzerkonto kann jedoch mehreren Gruppen zugeordnet werden, wobei für jede eine eigene Zuordnung für die Identität des Handelspartners bestehen kann. Dadurch ist es für ein Benutzerkonto möglich, mehreren Handelspartnern zugeordnet zu sein. Das Feld 'Identität' wird zum Weiterleiten von Nachrichten in die Mailbox verwendet. Wählen Sie eine Handelspartneridentität in der Liste aus. Der Standardwert ist 'Huborganisation'.

Gehen Sie wie folgt vor, um ein Benutzerkonto zu erstellen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzerkonten** aus.
2. Klicken Sie neben **Neues Konto erstellen** auf **Los!**.
3. Wählen Sie auf der Seite 'Neues Konto' den **Authentifizierungstyp** aus.
4. Geben Sie die **Benutzer-ID** ein.
5. Geben Sie das **Kennwort** ein.
6. Bestätigen Sie das Kennwort.
7. Wählen Sie die **Richtlinie** aus.

8. Geben Sie das **Sitzungszeitlimit** ein.
9. Wählen Sie den **Zugang** aus.
10. Wählen Sie das **Dashboardschema** aus.
11. Klicken Sie auf **Weiter**.
12. Ordnen Sie auf der Seite 'Autorisierter SSH-Benutzerschlüssel' mindestens einen öffentlichen Schlüssel zu. Verschieben Sie die Schlüssel vom Teilfenster **Verfügbar** in das Teilfenster **Zugeordnet** und klicken Sie dann auf **Weiter**.
13. Ordnen Sie auf der Seite 'Gruppen' Gruppen von Berechtigungen zu. Verschieben Sie die Gruppennamen vom Teilfenster **Verfügbar** in das Teilfenster **Zugeordnet** und klicken Sie dann auf **Weiter**.
14. Ordnen Sie auf der Seite 'Berechtigungen' einzelne Berechtigungen zu. Verschieben Sie die Berechtigungen vom Teilfenster **Verfügbar** in das Teilfenster **Zugeordnet** und klicken Sie dann auf **Weiter**. Standardmäßig sind die Berechtigungen der Gruppen, denen dieser Benutzer zugeordnet ist, bereits ausgewählt. Die erforderlichen Berechtigungen sind 'Admin Web App Permission' und 'MyAccount'.
15. Geben Sie auf der Seite 'Benutzerinformationen' eine Wert für **Vorname** ein.
16. Geben Sie einen Wert für **Nachname** ein.
17. Geben Sie die **E-Mail-Adresse** ein.
18. Geben Sie die **Pagernummer** ein.
19. Wählen Sie eine Einstellung für **Bevorzugte Sprache** aus. Wählen Sie den Wert **Clientanwendungseinstellungen verwenden** aus.

    Anmerkung: Dieser Wert weist Sterling B2B Integrator an, die Sprache zu verwenden, die im Browser des Benutzers und/oder der Ländereinstellung des Betriebssystems des Clients angegeben ist.
20. Geben Sie die **Manager-ID** ein.
21. Wählen Sie die **Identität** aus.
22. Klicken Sie auf **Weiter**.
23. Überprüfen Sie die Benutzerkontoeinstellungen.
24. Klicken Sie auf **Fertig stellen**. Das Benutzerkonto wird erstellt und die folgende Nachricht wird angezeigt:

    ```
    Die Systemaktualisierung wurde erfolgreich ausgeführt.
    ```

    Wenn Sie einen externen Benutzer erstellt haben, dann melden Sie sich beim System ab und unter der externen Benutzer-ID bzw. dem externen Konto wieder an. Das System authentifiziert die externe Benutzer-ID auf dem externen LDAP-Server.

Benutzerkonten bearbeiten

Ein Benutzerkonto können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Anmerkung: Obwohl mehrere Fremdsprachen unterstützt werden, sollte ein Benutzerkonto jeweils nur mit einer bestimmten Sprache verwendet werden, um Probleme mit der Anzeige der Benutzerschnittstelle zu vermeiden.

Gehen Sie wie folgt vor, um ein Benutzerkonto zu bearbeiten:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzerkonten** aus.
2. Suchen Sie das Benutzerkonto, das bearbeitet werden soll. Verwenden Sie hierzu die Option 'Suchen' oder 'Auflisten'.
3. Klicken Sie für das zu bearbeitende Benutzerkonto auf **Bearbeiten**.
4. Nehmen Sie die gewünschten Änderungen am Authentifizierungstyp des zugehörigen Benutzers vor.

   Wenn Sie den Authentifizierungstyp von 'Extern' in 'Lokal' ändern, dann müssen Sie ein Kennwort für den Benutzer erstellen. Wenn Sie den Authentifizierungstyp von 'Lokal' in 'Extern' ändern, dann kann das Kennwort oder die Kennwortrichtlinie des Benutzers nicht geändert werden.
5. Nehmen Sie alle Änderungen für **Neues Kennwort** vor und bestätigen Sie das neue Kennwort.
6. Nehmen Sie alle Änderungen für **Richtlinie** vor.
7. Nehmen Sie alle Änderungen für **Sitzungszeitlimit** vor und klicken Sie dann auf **Weiter**.
8. Nehmen Sie alle Änderungen für **Autorisierter SSH-Benutzerschlüssel** vor und klicken Sie dann auf **Weiter**.
9. Nehmen Sie alle Gruppenänderungen vor und klicken Sie dann auf **Weiter**.
10. Nehmen Sie alle Berechtigungsänderungen vor und klicken Sie dann auf **Weiter**.

    Die Berechtigungen 'Admin Web App Permission' und 'MyAccount' können nicht entfernt werden.
11. Nehmen Sie alle Änderungen an den Benutzerinformationen vor und klicken Sie dann auf **Weiter**.

    Anmerkung: Bei Benutzerkonten, bei denen die Benutzerschnittstelle in einer unterstützten Fremdsprache angezeigt wird, müssen Sie prüfen, ob der Wert für 'Bevorzugte Sprache' auf **Clientanwendungseinstellungen verwenden** gesetzt ist. Dieser Wert weist Sterling B2B Integrator an, die Sprache zu verwenden, die im Browser des Benutzers und/oder der Ländereinstellung des Betriebssystems des Clients angegeben ist.
12. Überprüfen Sie die Benutzerkontoeinstellungen.
13. Klicken Sie auf **Fertig stellen**.

Benutzerkonten löschen

Ein Benutzerkonto können Sie über das **Verwaltungsmenü** löschen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Benutzerkonto zu löschen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzerkonten** aus.
2. Suchen Sie das Benutzerkonto, das gelöscht werden soll. Verwenden Sie hierzu die Option 'Suchen' oder 'Auflisten'.
3. Klicken Sie für das zu löschende Benutzerkonto auf **Löschen**.
4. Klicken Sie auf **OK**.
5. Überprüfen Sie die Benutzerkontoeinstellungen.

6. Klicken Sie auf **Löschen**. Das ausgewählte Benutzerkonto wird gelöscht und die folgende Nachricht wird angezeigt:

   ```
   Die Systemaktualisierung wurde erfolgreich ausgeführt.
   ```

Informationen zu 'Eigenes Konto' aktualisieren

Die Informationen zu 'Eigenes Konto' sind Ihrem Benutzernamen und Kennwort zugeordnet. Wenn Sie sich anmelden, dann werden deswegen Ihre persönlichen Informationen auf der Seite 'Eigenes Konto' angezeigt. Sie können Ihre eigenen Kontoinformationen bearbeiten und die erste Seite ändern, die angezeigt wird, wenn Sie sich beim System anmelden.

Informationen zu diesem Vorgang

Es gibt zahlreiche Situationen, in denen Änderungen an den Informationen Ihres persönlichen Kontos eine Bearbeitung Ihrer Konteninformationen erforderlich machen. Zusätzlich können Sie aus Sicherheitsgründen auch Ihr Kennwort ändern.

Anmerkung: Obwohl mehrere Fremdsprachen unterstützt werden, sollte ein Benutzerkonto jeweils nur mit einer bestimmten Sprache verwendet werden, um Probleme mit der Anzeige der Benutzerschnittstelle zu vermeiden.

Gehen Sie wie folgt vor, um Ihre Konteninformationen zu aktualisieren:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Eigenes Konto** aus.
2. Wenn Sie das Kennwort Ihres Kontos aktualisieren wollen, dann geben Sie im Feld **Altes Kennwort** Ihr aktuelles Kennwort und anschließend im Feld **Neues Kennwort** ein neues Kennwort ein. Geben Sie das neue Kennwort anschließend nochmals im Feld **Neues Kennwort bestätigen** ein.
3. Geben Sie alle Änderungen ein, die in den Feldern **Vorname**, **Nachname**, **E-Mail** oder **Pager** erforderlich sind.
4. Wenn Sie den Wert für **Autorisierte SSH-Benutzerschlüssel**, der dem aktuellen Konto zugeordnet ist, ändern möchten, dann verschieben Sie die Schlüssel vom Teilfenster 'Verfügbar' ins Teilfenster 'Zugeordnet'.
5. Wählen Sie zur Änderung der Einstellung für **Bevorzugte Sprache** eine Sprache aus.

   Anmerkung: Bei Benutzerkonten, bei denen die Benutzerschnittstelle in einer unterstützten Fremdsprache angezeigt wird, müssen Sie prüfen, ob der Wert auf **Clientanwendungseinstellungen verwenden** gesetzt ist. Dieser Wert weist Sterling B2B Integrator an, die Sprache zu verwenden, die im Browser des Benutzers und/oder der Ländereinstellung des Betriebssystems des Clients angegeben ist.
6. Wählen Sie zum Ändern der **Willkommensseite** (Startseite Admin-Konsole), die bei der Anmeldung angezeigt wird, den gewünschten Wert in der Liste aus.
7. Wählen Sie zum Ändern der Anzahl der Prozesse, die auf einmal auf der Seite 'Aktuelle Prozesse' angezeigt werden, einen neuen Wert für **Seitengröße für aktuelle Prozesse** aus.
8. Wählen Sie zum Ändern der Anzahl der Dokumente, die auf einmal auf der Seite 'Aktuelle Dokumente' angezeigt werden, einen neuen Wert für **Seitengröße für aktuelle Dokumente** aus.

9. Wenn Sie Browserfenster erneut verwenden wollen, um Verknüpfungen zu starten, dann wählen Sie **Fenster zum Starten von Verknüpfungen wiederverwenden** aus.
10. Wenn Sie vom System Suchvorgänge auf der Basis von Zeichenfolgen, die Sie zuvor eingegeben haben, automatisch durchführen lassen wollen, dann wählen Sie **Für Suchvorgänge automatisch fertig stellen** aus.
11. Wenn das System die Werte, nach denen gesucht wurde, speichern soll, dann wählen Sie **Werte für Suchen nach speichern** aus. Diese Option speichert den letzten Wert, den Sie in jedem der Suchfelder eingegeben haben.
12. Klicken Sie auf **Speichern**. Die neuen Kontoinformationen werden gespeichert und die folgende Nachricht wird angezeigt:

    ```
    Ihre Aktualisierung wurde erfolgreich ausgeführt.
    ```

Benutzerexits für Benutzerkonten bei der Anmeldung (V5.2.5 und höher)

Sterling B2B Integrator bietet synchrone Benutzerexits mit Active Directory. Diese können Sie verwendne, um Ihre Benutzerkonten mit Active Directory anstelle der Sterling B2B Integrator-Benutzerschnittstelle zu verwalten. Diese Benutzerexits können durch den IBM Kundendienst während eines Kundenprojekts konfiguriert werden. Für weitere Informationen sprechen Sie bitte Ihren IBM Vertriebsbeauftragten oder IBM Händler an.

Benutzerexit	Beschreibung
IUserLoginUserExit_preAuthenticate	Zum Einfügen von angepasstem Code vor der Authentifizierung.
IUserLoginUserExit_postAuthenticateFail	Zum Einfügen von angepasstem Code nach einer erfolgreichen Authentifizierung.
IUserLoginUserExit_postAuthenticateSuccess	Zum Einfügen von angepasstem Code nach einer fehlgeschlagenen Authentifizierung.

Benutzerexits für Benutzerkonten bei der Abmeldung (V5.2.6 und höher)

Sterling B2B Integrator bietet synchrone Benutzerexits mit Active Directory. Diese können Sie verwendne, um Ihre Benutzerkonten mit Active Directory anstelle der Sterling B2B Integrator-Benutzerschnittstelle zu verwalten. Diese Benutzerexits können durch den IBM Kundendienst während eines Kundenprojekts konfiguriert werden. Für weitere Informationen sprechen Sie bitte Ihren IBM Vertriebsbeauftragten oder IBM Händler an.

Benutzerexit	Beschreibung
ILogoutUserExit_OnSessionInvalidate	Zum Einfügen von angepasstem Code, bevor die Sitzung ungültig wird.

Single Sign-on

Single Sign-on

Bei Single Sign-on (SSO) handelt es sich um einen Authentifizierungsprozess, mit dem Benutzer auf mehrere Anwendungen zugreifen und dazu nur einmal den Be-

nutzernamen und das Kennwort eingeben müssen. Zuvor musste sich ein Benutzer bei jeder Anwendung einzeln anmelden und verschiedene Benutzernamen und Kennwörter verwalten.

Für die Benutzerauthentifizierung bei SSO wird kein LDAP-Adapter benötigt, der bei Geschäftsprozessen verwendet wird und die Kommunikation mit lokalen oder fernen LDAP-Servern über JNDI (Java Naming and Directory Interface) ermöglicht.

Sterling B2B Integrator ermöglicht SSO durch die Integration mit Netegrity SiteMinder oder über angepasste Implementierungsklassen für SSO-Plug-ins in anderen SSO-Anwendungen und -Servern.

Single Sign-on kann nur für die folgenden Komponenten verwendet werden:

- Verwaltungsschnittstelle
- Mailbox-Schnittstelle
- Dashboardschnittstelle
- AFT-Schnittstelle (AFT = Advanced File Transfer)
- MyAFT-Schnittstelle

Standardklasse für Single Sign-on-Provider

Die URL für die SSO-Anmeldung für alle Schnittstellen mit Ausnahme des Dashboards ähnelt der normalen Anmeldeschnittstelle. Die URL der Dashboardschnittstelle lautet http:Host:port/dashboard/sso.jsp. Der Anforderungsheader für die Dashboardschnittstelle muss den Wert 'SM_USER=SSO User Name' aufweisen. (Alternativ kann der Wert auch in der Datei 'security.properties' unter SSO_USER_HEADER konfiguriert werden.)

Die Schnittstelle SSOProviderDefault ermöglicht dem SSO-Plug-in (SSO = Single Sign On) die Steuerung der SSO-Funktion für Netegrity SiteMinder.

Sie können die SSO so konfigurieren, dass eine Umleitung an eine externe HTTP-Seite (anstatt an die Sterling B2B Integrator-Abmeldeseite) durchgeführt wird, nachdem der Benutzer sich von einer SSO-Sitzung abmeldet. Die externe Seite vom SSO-Server kann entweder eine Anmelde- oder eine Abmeldeseite sein.

Im folgenden Beispiel ist die Klasse SSOProviderDefault.java dargestellt:

```
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)
}
}
```

Plug-in-Komponenten für Single Sign-on

Sterling B2B Integrator ermöglicht Ihnen die Verwendung einer angepassten Implementierungsklasse für SSO-Plug-ins (SSO = Single Sign-on) in anderen SSO-Anwendungen und -Servern. Sie müssen eine Implementierungsklasse mit dem Namen SSO_AUTHENTICATION_CLASS.<n>=<New class entry> in der Datei 'security.properties' hinzufügen, um ein SSO-Plug-in zu implementieren.

Sie können die angepassten Implementierungsklassen für SSO-Plug-ins auf der Basis der folgenden ISSOProvider.java-Schnittstellenklasse schreiben.

SSOProvider.java-Schnittstellenklasse

```
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;
}
```

Klasse SSOException

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

Klasse SSOAuthenticationException

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

Benutzerauthentifizierungsmethode

Die Authentifizierungsmethode wird während der Anmeldung initialisiert. Die Authentifizierungsmethode gibt die Benutzer-ID zurück, nachdem die Authentifizierung erfolgreich ausgeführt wurde. Die Ausnahmebedingung SSOAuthenticationException wird ausgelöst, wenn die Authentifizierung fehlgeschlagen ist. Die Ausnahmebedingung enthält einen entsprechenden Ursachencode und eine Umleitungsseite zur Behandlung des Fehlers, wenn SSO-Header vorhanden sind. Wenn keine SSO-Header vorhanden sind, wird die Steuerung wieder an die Systemanmeldungsanzeige übergeben.

Seitenauthentifizierungsmethode

Die Methode authenticatePage wird auf jeder Seite initialisiert. Alle zusätzlichen Validierungsmaßnahmen, die während des Seitenwechsels vom SSO-Server ausgeführt werden, werden über diese Methode ausgeführt. Sie können z. B. ein Pingsignal an den SSO-Server senden, um zu überprüfen, ob bei der SSO-Sitzung eine Zeitlimitüberschreitung aufgetreten ist. Wenn die Authentifizierung fehlschlägt, dann wird eine Ausnahmebedingung ausgelöst, die normalerweise den entsprechenden Ursachencode und eine Umleitungsseite enthält.

Ungültige SSO-Anforderungen

Die Inaktivierungsmethode wird initialisiert, wenn der Benutzer sich abmeldet, wenn die Authentifizierung bei der Anmeldung oder auf der Seite fehlschlägt oder wenn die Sitzung abläuft. Die HTTP-Umleitungsmethode muss ausgeführt werden, um SSO-Anforderungen zu inaktivieren. Die folgenden Methoden werden initialisiert, wenn die Authentifizierung fehlschlägt:

- Wenn die SSO-Serverauthentifizierung erfolgreich ausgeführt werden konnte und die Sterling B2B Integrator-Authentifizierung fehlgeschlagen ist, dann wird die Methode REASON_GIS_AUTHENTICATION_FAILURE mit dem entsprechenden Ursachencode initialisiert.
- Wenn die SSO-Serverauthentifizierung fehlgeschlagen ist, dann wird die Methode REASON_SSO_AUTHENTICATION_FAILURE mit dem entsprechenden Ursachencode initialisiert.
- Wenn der Benutzer sich abmeldet, dann wird die Methode REASON_LOGOUT mit dem entsprechenden Ursachencode initialisiert.
- Wenn die HTTP-Sitzung abläuft, wird die Methode REASON_HTTP_SESSION_EXPIRED mit dem entsprechenden Ursachencode initialisiert.
- Wenn die SSO-Sitzung des Benutzers abläuft, wird die Methode REASON_SSO_SESSION_EXPIRED mit dem entsprechenden Ursachencode initialisiert.

Prüfliste für Single Sign-on mit Netegrity SiteMinder

Bevor Sie Single Sign-on (SSO) konfigurieren können, müssen Sie sich mit SSO und Netegrity SiteMinder vertraut machen.

Verwenden Sie diese Prüfliste, um SSO für Netegrity SiteMinder zu konfigurieren:

Task	Prüfliste für Single Sign-on mit Netegrity SiteMinder	Anmerkungen
1	Installieren von Netegrity SiteMinder und Konfigurieren des Produkts mit einem Reverse-Proxy-Server.	
2	Konfigurieren der Eigenschaftendateien zur Verwendung mit Netegrity SiteMinder.	
3	Konfigurieren des Netegrity Secure Proxy Server.	
4	Erstellen sicherer Realms für Netegrity-Server.	

Informationen zur angepassten Implementierung von SSO-Plug-ins für andere SSO-Anwendungen und -Server finden Sie in den Informationen zu den Single Sign-on-Komponenten.

Einmalige Anmeldung mit IBM Global High Availability Mailbox (V5.2.6 oder höher)

Sterling B2B Integrator-Benutzer mit den entsprechenden Berechtigungen können direkt auf das IBM® Global High Availability Mailbox-Verwaltungstool mit einer einmaligen Anmeldung (Single Sign-on) von Sterling B2B Integrator aus zugreifen, um Global Mailbox zu verwalten.

Vorbereitende Schritte

Sterling B2B Integrator-Benutzer müssen einer der folgenden Gruppen angehören, um direkt auf das Global Mailbox-Verwaltungstool von Sterling B2B Integrator aus zugreifen zu können:

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

Informationen zu diesem Vorgang

Wenn Sie auf das Global Mailbox-Verwaltungstool mit einer einmaligen Anmeldung zugreifen, wird Ihre neue Sitzung von Global Mailbox in einer neuen Web-Browser-Registerkarte geöffnet und Ihre Sterling B2B Integrator-Sitzung bleibt verfügbar.

Sie können auf Global Mailbox mit einer einmaligen Anmeldung von Sterling B2B Integrator aus zugreifen. Wenn Sie Sie sich aus dem Global Mailbox-Verwaltungstool abmelden, werden Sie nicht aus Ihrer Sterling B2B Integrator-Sitzung abgemeldet.

Wenn Sie Ihr Global Mailbox-Administratorkennwort ändern wollen, müssen Sie sich direkt beim Global Mailbox-Verwaltungstool anmelden.

Einschränkung: Wenn Sie sich beim Global Mailbox-Verwaltungstool mit einer einmaligen Anmeldung anmelden, können Sie Ihr Global Mailbox-Administratorkennwort nicht ändern und die Option **Kennwort ändern** im Menü **Administrator** ist nicht verfügbar.

Gehen Sie wie folgt vor, um auf das Global Mailbox-Verwaltungstool mit einer einmalige Anmeldung zuzugreifen:

Vorgehensweise

1. Erweitern sie auf der Seite **Administratorkonsole** die Option **Implementierung** im Menü **Administration**.
2. Erweitern Sie **Globale Mailbox**.
3. Wählen Sie **Mailbox-Verwaltung** aus.
4. Klicken Sie auf den Hyperlink **Verwaltungstool der globalen Mailbox starten**, um eine neue Sitzung im Global Mailbox-Verwaltungstool zu öffnen.

   Hinweis: Wenn Sie auf den Hyperlink **Verwaltungstool der globalen Mailbox starten**, wird eine neue Sitzung von Global Mailbox in einer neuen Web-Browser-Registerkarte geöffnet.

Eigenschaftendateien für Single-Sign-On (SSO) mit Netegrity SiteMinder konfigurieren

Sie können Eigenschaftendateien für Single-Sign-on mit Netegrity SiteMinder konfigurieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die Dateien 'neo-ui.properties' und 'security.properties' zu bearbeiten:

Vorgehensweise

1. Stoppen Sie Sterling B2B Integrator.
2. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/properties'.
3. Öffnen Sie die Datei 'neo-ui.properties'.
4. Fügen Sie den zugehörigen SSO-Eintrag für jede Schnittstelle hinzu. Das folgende Codebeispiel zeigt den zugehörigen Eintrag für dieselben HTTP-Sites:

```
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. Speichern und schließen Sie die Datei 'neo-ui.properties'.

6. Öffnen Sie die Datei '/*installationsverzeichnis*/install/properties/security.properties' in einem Texteditor.
7. Suchen Sie in der Datei 'security.properties' nach den im folgenden Codebeispiel dargestellten Parametern für '## SSO Authentication configuration':

```
## 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. Führen Sie unterhalb des Eintrags '##SSO Authentication configuration' die folgenden Änderungen an den SSO-Parametern durch:

Parameter	Beschreibung	Bereitgestellter Wert	Neuer Wert
SSO_AUTHENTICATION_ENABLED	Aktiviert oder inaktiviert die Verwendung von SSO.	False (Falsch)	True (Wahr)
SSO_USER_HEADER	Benutzerheadername aus Netegrity SiteMinder oder Ihrer SSO-Anwendungskonfiguration.	SM_USER Dies ist der Wert in Netegrity SiteMinder.	Muss mit dem Eintrag in Netegrity SiteMinder oder Ihrer SSO-Anwendung übereinstimmen.

Parameter	Beschreibung	Bereitgestellter Wert	Neuer Wert
SSO_PAGE_ AUTHENTICATION_ ENABLED	Aktiviert oder inaktiviert die SSO-Authentifizierung auf allen Seiten.	False (Falsch)	True (Wahr) – Zur Authentifizierung von SSO auf allen Seiten. Nur ändern, wenn eine angepasste SSO-Providerklasse angegeben ist.
SSO_AUTHENTICATION_ CLASS.n	Implementierungsklasse zur Bereitstellung der Authentifizierungsunterstützung.	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	Auswahl in der Liste der angegebenen SSOProvider-Klassen.
SSO_FORWARD_ URL URL	Zeigt die URL-Seite an, die angegeben wird, nachdem Sie sich bei der Mailbox abgemeldet haben. Andernfalls wird der Standardwert angezeigt.	Kommentiert Zeigt die Standardseite an.	Angabe der URL.

9. Speichern und schließen Sie die Datei 'security.properties'.
10. Starten Sie Sterling B2B Integrator.

Netegrity Secure Proxy Server konfigurieren

Sie können Netegrity Secure Proxy Server konfigurieren, indem Sie Weiterleitungsregeln zur Datei 'proxyrules.xml' hinzufügen.

Informationen zu diesem Vorgang

Bevor Sie den Netegrity Secure Proxy Server konfigurieren können, müssen Sie die folgenden Arbeitsschritte ausführen:

- Installieren Sie Sterling B2B Integrator auf einem Server wie z. B. 'acme.si.com'.
- Ermitteln Sie die Portnummer, unter der MBI (Mailbox Browser Interface) installiert ist. Sie müssen diese Informationen in den entsprechenden Weiterleitungsregeln verwenden.
- Ermitteln Sie die Portnummer, unter der die Benutzerschnittstelle für das Sterling B2B Integrator-Dashboard installiert ist. Sie müssen diese Informationen in den entsprechenden Weiterleitungsregeln verwenden.

Gehen Sie wie folgt vor, um den Netegrity Secure Proxy Server zu konfigurieren:

Vorgehensweise

1. Fügen Sie die erforderlichen Weiterleitungsregeln für Sterling B2B Integrator zur Datei '/opt/netegrity/proxy-engine/conf/proxyrules.xml' hinzu.

   Im folgenden Beispiel wird gezeigt, wie die fertiggestellte Datei 'proxyrules.xml' nach dem Hinzufügen der Weiterleitungsregeln für den Zugriff auf die Sterling B2B Integrator-Komponenten dargestellt wird:

```
<?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. Fügen Sie die folgenden Zeilen zur Datei 'proxyrules.xml' hinzu, um die CSS-Überprüfung (CSS = Cross Server Scripting) auf dem sicheren Proxy-Server zu inaktivieren, da Sterling B2B Integrator keine Unterstützung für die Richtliniendurchsetzung von Netegrity Cross Server Scripting bietet.

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

3. Speichern und schließen Sie die Datei 'proxyrules.xml'.

Sichere Realms für Netegrity-Richtlinienserver erstellen

Der zuständige Administrator für Netegrity Policy Server muss sichere Realms für alle URL-Muster erstellen, die vom Secure Proxy Server weitergeleitet werden. Diese Sicherheitsrealms müssen über die erforderlichen Regeln für die Authentifizierung und Berechtigung verfügen.

Informationen zu diesem Vorgang

Darüber hinaus muss der Webagent im Secure Proxy Server so konfiguriert sein, dass eine Kommunikation mit dem Richtlinienserver möglich ist.

Erstellen Sie für jedes URL-Muster, das im Folgenden aufgelistet ist, einen sicheren Realm:

URL-Muster	Aktiviert Zugriff auf:
/mbi/*	Schnittstelle der Anwendungsmailbox
/dashboard/*	Schnittstelle des Anwendungsdashboards anhand des Formats http://host:port/dashboard
/datastore/*	Datenspeicherkomponenten
/portlets/*	Anwendungsportletkomponenten in der Dashboardschnittstelle
/help/*	Komponenten für kontextbezogene Hilfe
/webxtools/*	Weberweiterungsdienstprogramme
/gbm/*	Komponenten für grafischen Prozessmodellierer

Kennwörter

Kennwortrichtlinien

Bei Kennwortrichtlinien handelt es sich um Gruppen von Sicherheitsentscheidungen, die Sie treffen und auf unterschiedliche Benutzerkonten gemäß den Sicherheitsrichtlinien Ihres Unternehmens anwenden. Die Entscheidungen betreffen Bereiche wie z. B. die Anzahl der Tage, die ein Kennwort gültig ist, oder die maximale oder minimale Länge eines Kennworts.

Sie können Kennwortrichtlinien verwenden, um Ihre Sicherheitsoperationen zu optimieren, wenn neue Benutzer hinzugefügt werden. Anstatt einzelne Richtlinien für jeden Benutzer hinzuzufügen, können Sie eine Kennwortrichtlinie erstellen und diese Richtlinie dann auf alle Benutzer anwenden, die denselben Zugriff benötigen.

Nach der Erstellung einer Kennwortrichtlinie können Sie sie nur auf interne Benutzerkonten anwenden. Dadurch erhalten Sie die größtmöglichste Flexibilität bei der Verwaltung Ihrer Sicherheitsrichtlinien. Wenn Sie mit LDAP (Lightweight Directory Access Protocol) arbeiten, können Sie Kennwortrichtlinien nicht auf Ihre externen Konten anwenden.

Die Standardwerte für die Kennwortrichtlinie lauten wie folgt:

Parameter	Standardwert
Richtlinien-ID	default_user
Richtlinienname	Standardbenutzerrichtlinie
Anzahl von gültigen Tagen	60
Minimale Länge	6
Maximale Länge	28
Anzahl von im Verlaufsprotokoll gespeicherten Kennwörtern	5
Kennwort muss Sonderzeichen enthalten	Ausgewählt
Kennwortänderung beim ersten Anmeldeversuch erforderlich	Ausgewählt

Es gibt die folgenden Kennwortrichtlinientasks:

- Erstellen einer Kennwortrichtlinie
- Suchen einer Kennwortrichtlinie

- Bearbeiten einer Kennwortrichtlinie
- Löschen einer Kennwortrichtlinie
- Bearbeiten des Lockout-Parameters
- Bearbeiten der Nachricht zum Ablauf des Kennworts

Angepasste Kennwortrichtlinie

Die angepasste Kennwortrichtlinie von Sterling B2B Integrator ist eine Sicherheitseinrichtung zum Hinzufügen zusätzlicher Kennwortrichtlinienregeln. Diese zusätzlichen Kennwortregeln können Sie dabei unterstützen, die Verwendung schwacher, leicht zu hackender Kennwörter zu verhindern und nicht den Bildungsregeln entsprechende Kennwörter zurückzuweisen.

Gehen Sie wie folgt vor, um diese Funktionalität zu aktivieren:

- Implementieren Sie über einen Verbindungspunkt angepassten Java-Code. Nach der Aktivierung wird der Verbindungspunkt für alle Benutzer auf dem System verwendet, denen die Kennwortrichtlinie zugeordnet wurde. (Dies ist eine globale Einstellung.)
- Fügen Sie die Eigenschaft passwordPolicyExtensionImpl zur Datei 'customer_overrides.properties' hinzu.
- Wenden Sie die angepasste Kennwortrichtlinie auf 'Benutzerkonten' an.

Die Erweiterung für die angepasste Kennwortrichtlinie wird vor der Standardkennwortrichtlinie angewendet. Wenn ein Kennwort gegen mehr als eine Richtlinienanforderung verstößt (wobei eine von der Erweiterungsklasse und die andere von der Standardimplementierung umgesetzt wird), wird nur die Fehlernachricht, die von der Erweiterungsklasse zurückgegeben wird, für den Benutzer angezeigt.

Beispiel: Kennwortrichtlinie

Im folgenden Beispiel ist eine mögliche Einstellung für eine Kennwortrichtlinie dargestellt.

Eine Kennwortrichtlinie mit dem Namen 'Test' kann z. B. für ein Kennwort die folgenden Einstellungen aufweisen:

- Das Kennwort ist 10 Tage gültig.
- Das Kennwort hat eine Mindestlänge von 10 Zeichen.
- Das Kennwort hat eine maximale Länge von 20 Zeichen.
- Das Kennwort enthält mindestens zwei Sonderzeichen.
- Der Benutzer muss das Standardkennwort während der ersten Anmeldung ändern.
- Die Anzahl der im Verlaufsprotokoll gespeicherten Kennwörter.

Anhand des vorherigen Beispiels wird dem Benutzer vom Systemadministrator ein Benutzername und ein Kennwort zugeordnet. Der Benutzer meldet sich mit dem Benutzernamen und dem Kennwort an und wird vom System aufgefordert, das Kennwort zu ändern. Wenn der Benutzer kein Kennwort mit einer Mindestlänge von 10 Zeichen und einer maximalen Länge von 20 Zeichen oder mindestens zwei Sonderzeichen angibt, dann wird er vom System aufgefordert, seine Eingabe zu korrigieren. Nachdem alle Bedingungen, die in der Kennwortrichtlinie definiert sind, von dem Benutzer, der das Kennwort ändert, erfüllt wurden, speichert das System das neue Kennwort und gewährt dem Benutzer Zugriff. Jedem Benutzerkonto kann nur eine Kennwortrichtlinie zugeordnet sein, Sie können jedoch eine Kennwortrichtlinie auf mehrere Benutzerkonten anwenden.

Zusätzlich zu den Änderungen der Kennwortrichtlinie in der Schnittstelle können Sie die Anzahl der fehlgeschlagenen Anmeldeversuche des Benutzers ändern, die ausgeführt werden dürfen, bevor das Benutzerkonto des Benutzers gesperrt wird.

Beispiel: Wenn die Anzahl der nacheinander ausgeführten Anmeldeversuche auf den Wert '3' gesetzt ist und der Benutzer dreimal ein falsches Kennwort eingibt, kann er sich an dem betreffenden Computer nicht mehr anmelden. Die Anmeldung kann über einen anderen Computer versucht werden, der über Zugriff auf das System verfügt.

Installationskennwort oder -kennphrase

Während der Installation erstellen Sie eine Systemkennphrase für Ihre Sterling B2B Integrator-Installation. Die Kennphrase ist eine sehr komplexe Zeichenfolge mit mehr als 16 Zeichen. Die Systemkennphrase ist erforderlich, um das System starten und auf geschützte Systeminformationen zugreifen zu können.

Die einzige Person, die die Kennphrase aktualisieren oder ändern kann, ist derjenige Benutzer, der die Software erstellt/installiert hat. Wenn Sie die Kennphrase verlieren oder vergessen, dann kann das System von Ihnen nicht mehr gestartet werden. Der einzige Benutzer, der die Systemkennphrase aktualisieren kann, ist der Benutzer, der die Installation durchgeführt hat.

Die Systemkennphrase wird vom System nicht gespeichert. Eine Ausnahme bilden hierbei Windows-Installationen, in denen die Kennphrase in verschlüsselter Form in der Datei 'security.properties' gespeichert wird, um die Ausführung des Systems als nicht interaktiver Dienst zu ermöglichen. Sie kann auf anderen Plattformen im Klartextformat in der Datei 'security.properties' gespeichert werden, sodass Sie sie beim Systemstart nicht in der Befehlszeile eingeben müssen. Allerdings wird die Systemkennphrase dann nur über die Dateizugriffssteuerung des Betriebssystems geschützt.

Prüfliste für Kennwörter für angepasste Richtlinie

Sie können eine angepasste Kennwortrichtlinie implementieren.

Verwenden Sie die folgende Prüfliste, um Kennwörter für angepasste Richtlinien zu implementieren:

Task	Prüfliste für Kennwörter für angepasste Richtlinien
1	Erstellen einer Verzeichnisstruktur im <SI_Installationsverzeichnis> für Tests, Richtlinien und Erweiterungen.
2	Erstellen der Java-Klasse im Erweiterungsverzeichnis.
3	Angabe der Java-Klasse an, die zur Implementierung der Kennwortrichtlinie (Eigenschaft passwordPolicyExtensionImpl) in der Datei 'customer_overrides.properties' verwendet wird.
4	Hinzufügen der JAR-Datei für die Implementierungsklasse zum Klassenpfad.
5	Definieren der Fehlernachricht.

Beispiel - Kennwort für angepasste Richtlinie

Im folgenden Beispiel wird eine Erweiterung für ein Kennwort für eine angepasste Richtlinie dargestellt.

Im Folgenden finden Sie ein Beispiel einer Erweiterung für ein Kennwort für eine angepasste Richtlinie.

Die Schnittstelle 'com.sterlingcommerce.woodstock.security.PasswordPolicyExtension' wurde wie folgt zum System hinzugefügt:

```
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);
}
```

Wenn die Methode den Wert null zurückgibt, dann wurde das Kennwort akzeptiert. Wenn ein anderer Wert zurückgegeben wird, dann bedeutet dies, dass das Kennwort nicht gültig war.

Beispielimplementierung

```
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";
      }

}
```

Kennwortrichtlinien suchen

Eine Kennwortrichtlinie können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um nach Kennwortrichtlinien zu suchen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Kennwortrichtlinie** aus.

2. Führen Sie auf der Seite 'Kennwortrichtlinie' eine der folgenden Aktionen durch:
   - Geben Sie unter 'Suchen' im Feld **Name der Kennwortrichtlinie** entweder einen Teil des Namens oder den vollständigen Namen der Kennwortrichtlinie ein, nach der Sie suchen möchten, und klicken Sie dann auf **Los!**. Auf der Seite 'Kennwortrichtlinie' werden alle Elemente aufgelistet, die mit Ihren Suchkriterien übereinstimmen.
   - Wählen Sie unter 'Auflisten' im Feld **Alphabetisch** die Option **ALLE** oder den Buchstaben aus, mit dem der Name der Kennwortrichtlinie beginnt, nach der Sie suchen, und klicken Sie dann auf **Los!**. Auf der Seite 'Kennwortrichtlinie' werden alle Elemente aufgelistet, die mit Ihren Suchkriterien übereinstimmen.

Kennwortrichtlinien erstellen

Sie können eine Kennwortrichtlinie erstellen, um die Richtlinie bestimmten Benutzerkonten zuzuordnen. Sie müssen einem Benutzerkonto keine Kennwortrichtlinie zuordnen, diese Zuordnung erleichtert jedoch die Sicherheitsverwaltung.

Informationen zu diesem Vorgang

Bevor Sie beginnen können, benötigen Sie die folgenden Informationen:

Feld	Beschreibung
Richtlinien-ID	Die ID zur Identifikation der Kennwortrichtlinie in der Datenbank.
Richtlinienname	Der Richtlinienname zur Anzeige in der Benutzerschnittstelle, wenn Verweise auf die Kennwortrichtlinie angegeben werden.
Anzahl von gültigen Tagen	Die Anzahl von Tagen, die ein Benutzerkennwort gültig ist. Der Standardwert lautet 0, was bedeutet, dass das Kennwort niemals abläuft. Wenn Sie einen Wert zwischen 1 und 999 angeben, wird der Benutzer zur Änderung des Kennworts aufgefordert, sobald dieser Zeitraum abgelaufen ist. Der Ablaufcountdown startet bei der ersten Anmeldung des Benutzers nach der Zuordnung eines Kennworts zu seinem Benutzerkonto.
Minimale Länge	Die minimale Länge, die ein Kennwort aufweisen muss. Erforderlich. Die gültigen Werte sind alle Numerale. Diese Nummer muss mindestens auf den Wert '6' gesetzt sein. Der Standardwert ist '6'. Wenn keine Richtlinie angewendet wird, dann erzwingt das System eine Mindestlänge von 6 Zeichen.
Maximale Länge	Die maximale Länge, die das Kennwort haben kann. Erforderlich. Die gültigen Werte sind alle Numerale. Diese Zahl muss mindestens die gleiche Zahl wie die minimale Länge angeben. Der Standardwert lautet '28'.
Anzahl von im Verlaufsprotokoll gespeicherten Kennwörtern	Die Anzahl der Kennwörter, die in der Tabelle PWD_HISTORY in der Datenbank für einen Benutzer gespeichert wird. Wenn diese Anzahl von Kennwörtern überschritten wird, dann wird das älteste Kennwort aus der Tabelle entfernt und kann vom Benutzer erneut verwendet werden. Der Standardwert lautet '0'.

Feld	Beschreibung
Kennwort muss Sonderzeichen enthalten	Gibt an, dass das Kennwort mindestens ein Sonderzeichen enthalten muss. Gültige Werte sind Ziffern, Großbuchstaben oder eines der Zeichen !, @, #, $, %, ^, & oder *.
Kennwortänderung beim ersten Anmeldeversuch erforderlich	Gibt an, dass der Benutzer das Standardkennwort nach der ersten Anmeldung ändern muss. Das System fordert den Benutzer nach der ersten Anmeldung zur Änderung des Kennworts auf.

Gehen Sie wie folgt vor, um eine Kennwortrichtlinie zu erstellen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Kennwortrichtlinie** aus.
2. Klicken Sie neben **Neue Kennwortrichtlinie erstellen** auf **Los!**.
3. Geben Sie auf der Seite 'Kennwortrichtlinie' die **Richtlinien-ID** ein.
4. Geben Sie einen Wert für **Richtlinienname** ein.
5. Geben Sie einen Wert für **Anzahl von gültigen Tagen** ein.
6. Geben Sie einen Wert für **Minimale Länge** ein.
7. Geben Sie einen Wert für **Maximale Länge** ein.
8. Geben Sie einen Wert für **Anzahl von im Verlaufsprotokoll gespeicherten Kennwörtern** ein.
9. Wenn das Kennwort Sonderzeichen enthalten muss, dann wählen Sie das entsprechende Kontrollkästchen aus.
10. Wenn der Benutzer das Kennwort bei der ersten Anmeldung ändern muss, dann wählen Sie das entsprechende Kontrollkästchen aus.
11. Klicken Sie auf **Weiter**.
12. Überprüfen Sie die Kennwortrichtlinieneinstellungen.
13. Klicken Sie auf **Fertig stellen**.

Kennwortrichtlinien bearbeiten

Eine Kennwortrichtlinie können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Kennwortrichtlinie zu bearbeiten:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Kennwortrichtlinie** aus.
2. Suchen Sie die Kennwortrichtlinie, die bearbeitet werden soll. Verwenden Sie hierzu die Option 'Suchen' oder 'Auflisten'.
3. Klicken Sie für die zu bearbeitende Kennwortrichtlinie auf **Bearbeiten**.
4. Nehmen Sie auf der Seite 'Einstellungen für Kennwortrichtlinie' die gewünschten Änderungen vor und klicken Sie dann auf **Weiter**.
5. Überprüfen Sie die Kennwortrichtlinieneinstellungen.
6. Klicken Sie auf **Fertig stellen**.

   Daraufhin wird die folgende Nachricht angezeigt:

   ```
   Die Systemaktualisierung wurde erfolgreich ausgeführt.
   ```

Kennwortrichtlinien löschen

Wenn Sie eine Kennwortrichtlinie löschen, dann können sich Benutzerkonten, die dieser bestimmten Kennwortrichtlinie zugeordnet sind, weiterhin anmelden, aber der zugehörige Benutzer wird nicht mehr zwingend zur Änderung des Kennworts aufgefordert. Wenn der Benutzer das Kennwort ändert, dann wird das neue Kennwort nicht überprüft.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Kennwortrichtlinie zu löschen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Kennwortrichtlinie** aus.
2. Suchen Sie die Kennwortrichtlinie, die gelöscht werden soll. Verwenden Sie hierzu die Option 'Suchen' oder 'Auflisten'.
3. Klicken Sie für die zu löschende Kennwortrichtlinie auf **Löschen**.
4. Klicken Sie auf der Seite 'Bestätigen' auf **Löschen**.

   Daraufhin wird die folgende Nachricht angezeigt:

   ```
   Die Systemaktualisierung wurde erfolgreich ausgeführt.
   ```

Anzahl der Tage für Ablauf des Benutzerkennworts ändern

Das System benachrichtigt Sie, wenn sich das Ablaufdatum des Kennworts ändert. Dazu wird im Bereich für Systemalerts auf der Startseite der Admin-Konsole eine Nachricht ausgegeben. Systemadministratoren können angeben, in welchem Zeitraum (Anzahl der Tage vor dem Ablauf des Kennworts) die Benutzer benachrichtigt werden sollen.

Informationen zu diesem Vorgang

In der Nachricht ist angegeben, dass das Kennwort in einer bestimmten Anzahl von Tagen abläuft. Jeden Tag wird diese Anzahl um den Wert '1' reduziert, bis der Tag erreicht wird, an dem das Kennwort abläuft und Sie zur Änderung des Kennworts aufgefordert werden.

Systemadministratoren können die Anzahl der Tage vor dem Ablauf in der Datei 'ui.properties.in' ändern. Sie sollten alle Änderungen in der Datei 'ui.properties.in' und nicht in der Datei 'ui.properties' durchführen. Wenn Sie die Änderungen in der Datei 'ui.properties' durchführen und das System neu starten, dann werden die in der Datei 'ui.properties' vorgenommenen Änderungen von den Daten in der Datei 'ui.properties.in' überschrieben.

Gehen Sie wie folgt vor, um die Anzahl der Tage für den Ablauf des Kennworts zu ändern:

Vorgehensweise

1. Stoppen Sie Sterling B2B Integrator.
2. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/properties'.
3. Öffnen Sie die Datei 'ui.properties.in'.
4. Suchen Sie den Eintrag 'MsgPwdExpires= 15'.
5. Ändern Sie den Wert und geben Sie anstatt '15' die neue Anzahl von Tagen für den Ablauf des Benutzerkennworts an.

6. Speichern Sie die Datei.
7. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
8. Geben Sie **setupfiles.sh** ein.
9. Starten Sie Sterling B2B Integrator erneut. Die Änderungen an der Datei 'ui.properties.in' werden auf die Datei 'ui.properties' angewendet und sind dann für alle Benutzerkonten wirksam.

Eigenes Kennwort nach Lockout zurücksetzen

Wenn die Sperre aktiviert ist (Lockout), können Sie sich über einen anderen Computer anmelden oder 30 Minuten warten, bis die Sperre abgelaufen ist, oder den Systemadministrator bitten, die Sperre aufzuheben.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, wenn Sie von Ihrem System ausgesperrt wurden:

- Melden Sie sich bei einem anderen als dem sonst verwendeten Computer, der über Zugriff auf das gewünschte System verfügt, an.
- Warten Sie 30 Minuten, bis die Sperre aufgehoben wird, sodass Sie erneut versuchen können, sich auf dem gesperrten Computer anzumelden.
- Wenden Sie sich an den Systemadministrator und bitten Sie diesen, die Sperre über die Seite 'Sperr-Manager' aufzuheben. Daraufhin können Sie erneut versuchen, sich an dem gesperrten Computer anzumelden.

Fehlernachricht für angepasste Kennwortrichtlinie definieren

Sie können Fehlernachrichten für die Erweiterung einer angepassten Kennwortrichtlinie definieren.

Informationen zu diesem Vorgang

Fehlernachrichten informieren den Benutzer über Kennwortregeln und listen die Ursachen auf, die zur Ablehnung einer Kennwortänderung geführt haben. Die angepassten Kennwortfehlernachrichten werden in Dateien mit dem Namen 'Login_*sprachverzeichnis*.properties_*eindeutigeID*_ext' definiert. Wenn kein angepasster Text angegeben wurde, dann erhält der Benutzer die Standardfehlernachricht. Die Datei 'Login_*sprachverzeichnis*.properties_*eindeutigeID*_ext' ist nicht Bestandteil des Standardsystemcodes. Sie muss nach der Erstinstallation des System erstellt und mit den für Ihre Umgebungen verfügbaren Daten gefüllt werden.

Gehen Sie wie folgt vor, um eine Fehlernachricht für die Erweiterung einer angepassten Kennwortrichtlinie zu definieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '*/installationsverzeichnis*/install/properties/lang/*sprachverzeichnis*'. Hierbei steht *sprachverzeichnis* für die Sprache, die für die Ländereinstellung des Kunden angegeben wurde (z. B. 'en', 'ja' oder 'fr').
2. Bearbeiten Sie die Datei 'Login_*sprachverzeichnis*.properties_*eindeutigeID*_ext'. Hierbei steht *sprachverzeichnis* für die Sprache, die für die Ländereinstellung des Kunden angegeben wurde, und *eindeutigeID* für die eindeutige Kennung, die der neuen angepassten Kennworterweiterung zugeordnet ist. Beispiel: Login_en.properties_custompasswd_ext.
3. Fügen Sie für die Fehlerbedingung, die in der angepassten Erweiterungsdatei definiert wurde, einen Eintrag zu der Datei hinzu und definieren Sie eine beschreibende Zeichenfolge, die an den Benutzer zurückgegeben werden soll. Bei-

spiel: nogood = Das Kennwort muss mindestens ein Zeichen in Kleinschreibung, eines in Großschreibung und eine Zahl oder ein Sonderzeichen enthalten.

4. Speichern und schließen Sie die Datei.

Erweiterung für angepasste Kennwortrichtlinie in Datei 'customer_overrides.property' angeben

Sie können die Java-Klasse zum Implementieren der Kennwortrichtlinienerweiterung angeben.

Informationen zu diesem Vorgang

Um die angepasste Implementierung zu integrieren, muss der Name der Java-Klasse in der Eigenschaft passwordPolicyExtensionImpl in der Datei 'customer_overrides.properties' angegeben werden.

Gehen Sie wie folgt vor, um die Java-Klasse anzugeben, die die Erweiterung für die Kennwortrichtlinie implementiert:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'properties'.
3. Bearbeiten Sie die Datei 'customer_overrides.properties'.
4. Fügen Sie die Eigenschaft passwordPolicyExtensionImpl am Ende der Datei hinzu und geben Sie den Namen der Java-Klasse ein, die die erweiterte Validierungsfunktion für Kennwörter implementiert. Beispiel: security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl.
5. Speichern und schließen Sie die Datei.

JAR-Datei für Implementierungsklasse für angepasste Kennwortrichtlinie zum Klassenpfad hinzufügen

Für eine angepasste Kennwortrichtlinie müssen Sie die JAR-Datei für die Implementierungsklasse zum Klassenpfad hinzufügen.

Informationen zu diesem Vorgang

Die Implementierungsklasse für die Erweiterung muss kompiliert und wie folgt in einer JAR-Datei komprimiert werden:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis *SI_Installationsverzeichnis*.
2. Geben Sie den folgenden Befehl ein, um die angepasste Klassendatei zu kompilieren:

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

3. Erstellen Sie die JAR-Datei, indem Sie den folgenden Befehl im *SI_Installationsverzeichnis* ausführen:

   `jar cf beliebiger_dateiname.jar absoluter_pfad_zur_angepassten_klassendatei.class` Hierbei steht `beliebiger_dateiname.jar` für den Namen der neuen JAR-Datei, die erstellt werden soll, und `absoluter_pfad_zur_angepassten_klassendatei.class` für den Namen der angepassten Java-Klassendatei für die Implementierung. Beispiel: `jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class`

4. Navigieren Sie zum Verzeichnis *SI_Installationsverzeichnis*.
5. Geben Sie den folgenden Befehl ein, um die neu erstellte JAR-Datei dem Klassenpfad hinzuzufügen:

   ```
   ./install3rdParty.sh userExit 1_0 -j
   pfad_zu_der_in_schritt3_erstellten_klassendatei
   ```

   Beispiel: `./install3rdParty.sh userExit 1_0 -j SI_Installationsverzeichnis/userExit.jar`

LDAP-Authentifizierung

LDAP als Authentifizierungstool für Sterling B2B Integrator

Lightweight Directory Access Protocol (LDAP) ist eine Gruppe von Protokollen, die zum Zugriff auf Informationen verwendet werden, die in einem Informationsverzeichnis gespeichert sind, bei dem es sich um ein LDAP-Verzeichnis handelt.

Ein LDAP-Verzeichnis ist eine Datenbank, die jedoch nicht nach dem relationalen Prinzip aufgebaut ist. Sie wird zum Verwalten von Informationen verwendet, die über mehrere Server in einem Netz verteilt sind, und sie ist in Bezug auf die Leseleistung optimiert.

Sie können LDAP verwenden, um die Authentifizierung eines externen Benutzerkontos an ein LDAP-Verzeichnis zu delegieren und die Authentifizierung anhand der gleichen Sicherheitsinformationen zu ermöglichen, die für andere Anwendungen in Ihrem Unternehmen verwendet werden. Wenn Ihr Unternehmen bereits LDAP verwendet, dann können Sie die bereits bestehenden LDAP-Verzeichnisse verwenden.

Für die Authentifizierung von Benutzerkonten wird kein LDAP-Adapter benötigt, der bei Geschäftsprozessen verwendet wird und die Kommunikation mit lokalen oder fernen LDAP-Servern über JNDI (Java Naming and Directory Interface) ermöglicht.

Wenn der LDAP-Server nicht arbeitet, dann behalten Benutzer, die über interne Konten verfügen, weiterhin Zugriff. Die Benutzer, die jedoch über externe Konten verfügen, haben erst dann wieder Zugriff, wenn der LDAP-Server wieder arbeitet.

Bevor Sie LDAP für Sterling B2B Integrator konfigurieren können, müssen Sie über Folgendes verfügen:

- Kenntnisse zu LDAP
- Zugriff auf einen installierten und konfigurierten LDAP-Server mit Benutzerinformationen
- Position des LDAP-Servers
- (Für SSL) Installierte Sicherheitszertifikate im Keystore und Truststore
- Bereits erstellte externe Benutzerkonten für jeden Benutzer, der die Authentifizierung über Ihren LDAP-Server durchführt
- (Für SSL) Position des Keystores und Truststores

Beispiel: Konfigurationsparameter für LDAP-Authentifizierung

Im folgenden Beispiel werden die Konfigurationsparameter für die LDAP-Authentifizierung dargestellt.

Das folgende Beispiel zeigt die Konfigurationsparameter für die LDAP-Authentifizierung:

```
## 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
```

Konfigurationsprüfliste für LDAP-Authentifizierung

Sie können LDAP mit Sterling B2B Integrator konfigurieren.

Verwenden Sie diese Prüfliste, um LDAP mit Sterling B2B Integrator zu konfigurieren:

Tasks	LDAP-Konfigurationsprüfliste
1	Konfigurieren Sie LDAP in einem der folgenden Modi: • Kennwortvergleichsmodus • Kennwortbinärmodus
2	Konfigurieren Sie LDAP mit Sterling B2B Integrator.
3	Überprüfen Sie die LDAP-Konfiguration.
4	Optional. Verschlüsseln Sie die LDAP-Kennwörter.

LDAP im Kennwortbindungsmodus konfigurieren

Sie können LDAP in einem Kennwortbindungsmodus konfigurieren, indem Sie Ihre **Benutzer-ID** und Ihr **Kennwort** über Ihr externes Benutzerkonto eingeben.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um LDAP in einem Kennwortbindungsmodus zu konfigurieren:

Vorgehensweise

Geben Sie Ihre **Benutzer-ID** und das **Kennwort** über Ihr externes Benutzerkonto ein. Das System führt folgende Schritte aus:

- Herstellen einer Bindung zum LDAP-Repository mit den Berechtigungsnachweisen, die die Ausführung der erforderlichen Abfragen ermöglichen.
- Suchen nach dem Benutzer mit der entsprechenden Benutzer-ID im LDAP-Verzeichnis.
- Abrufen des DN (definierter Name) des Benutzers aus dem LDAP-Verzeichnis.
- Herstellen einer Bindung zum LDAP-Repository mithilfe des definierten Namens und des Kennworts des Benutzers.
- Erfolg – Das System stellt unter einem bestimmten Benutzer eine Bindung zum LDAP-Repository her.
- Fehler - Das System kann unter dem angegebenen Benutzer keine Bindung zum LDAP-Repository herstellen.

LDAP im Kennwortvergleichsmodus konfigurieren

Sie können LDAP in einem Kennwortvergleichsmodus konfigurieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um LDAP in einem Kennwortvergleichsmodus zu konfigurieren:

Vorgehensweise

1. Geben Sie Ihre **Benutzer-ID** und das **Kennwort** über Ihr externes Benutzerkonto ein.

2. Das System versucht, eine Bindung zum LDAP-Repository mit den Berechtigungsnachweisen herzustellen, die die Ausführung der erforderlichen Abfragen ermöglichen.
3. Das System sucht nach dem Benutzer mit der entsprechenden Benutzer-ID im LDAP-Verzeichnis.
4. Das System ruft das Benutzerkennwort aus dem LDAP-Verzeichnis ab.
5. Das System vergleicht das vom Benutzer angegebene Kennwort mit dem Kennwort, das aus dem LDAP-Verzeichnis abgerufen wird. Wenn die Kennwörter übereinstimmen, dann werden Sie authentifiziert und erhalten Zugriff auf das System. Wenn die Kennwörter nicht übereinstimmen, dann werden Sie nicht authentifiziert und der Zugriff auf das System wird Ihnen verweigert.

LDAP mit Sterling B2B Integrator konfigurieren

Um Sterling B2B Integrator für die Verwendung von LDAP zu konfigurieren, müssen Sie die Datei 'authentication_policy.properties.in' bearbeiten. Sie können auch die Datei 'customer_overrides.properties' verwenden, um die Eigenschaftswerte zu definieren, die von der Installation einer Programmkorrektur nicht überschrieben werden sollen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die LDAP-Authentifizierung zu konfigurieren:

Vorgehensweise

1. Stoppen Sie Sterling B2B Integrator.
2. Navigieren Sie zum Installationsverzeichnis.
3. Navigieren Sie zum Verzeichnis 'properties'.
4. Öffnen Sie die Datei 'authentication_policy.properties.in'.
5. Suchen Sie in der Datei 'authentication_policy.properties.in' nach dem Eintrag '## GIS/LDAP Authentication configuration'.
6. Führen Sie unterhalb des Eintrags '##GIS/LDAP Authentication configuration' die folgenden Änderungen an den LDAP-Parametern durch:

Parameter	Beschreibung	Bereitgestellter Wert	Änderung in
#LDAP_SECURITY_ TRUSTSTORE	Pfad zum lokalen Truststore. Im Truststore müssen die erforderlichen LDAP-Zertifikate gespeichert sein. Zertifikate von Handelspartnern können nicht verwendet werden. Optional. Verwenden Sie diesen Parameter nur, wenn Sie mit SSL arbeiten.	Inaktiver Pfad	Vollständiger Pfad zum lokalen Truststore.
#LDAP_SECURITY_ TRUSTSTORE_ PASSWORD	Kennwort für den Zugriff auf den Truststore. Optional. Verwenden Sie diesen Parameter nur, wenn Sie mit SSL arbeiten.	changeit	Kennwort für den Zugriff auf den lokalen Truststore.

Parameter	Beschreibung	Bereitgestellter Wert	Änderung in
#LDAP_SECURITY_ KEYSTORE	Pfad zum lokalen Keystore. Im Keystore müssen die erforderlichen LDAP-Zertifikate gespeichert sein. Zertifikate von Handelspartnern können nicht verwendet werden. Optional. Verwenden Sie diesen Parameter nur, wenn Sie mit SSL arbeiten.	Inaktiver Pfad	Vollständiger Pfad zum lokalen Keystore.
#LDAP_SECURITY_ KEYSTORE_ PASSWORD	Kennwort für den Zugriff auf den Keystore. Optional. Verwenden Sie diesen Parameter nur, wenn Sie mit SSL arbeiten.	password	Kennwort für den Zugriff auf den lokalen Keystore.
#authentication_ <number>. enabled	Aktiviert oder inaktiviert die Verwendung von LDAP. False – Alle Benutzer, die anhand dieses Authentifizierungshosts erstellt wurden, werden inaktiviert (können sich nicht anmelden). True – Auf alle Benutzer kann intern oder extern, jedoch nicht auf beide Arten zugegriffen werden, da jede Benutzer-ID eindeutig ist. Dieser Wert wird nicht überprüft, wenn er für die interne Authentifizierung verwendet wird.	False (Falsch)	True (Wahr)
#authentication_<number> .jndi_factory	Klassenname der Factory-Klasse, die den Ausgangskontext für den LDAP-Service-Provider erstellt. Dies ist die Standardkontextfactory, die zusammen mit JDK ausgeliefert wird.	com.sun. jndi.ldap. LdapCtx Factory	Keine Änderung.
#authentication_ <number>.server	URL zur Angabe des Hostnamens des LDAP-Servers.	Inaktiver Pfad	URL des lokalen LDAP-Hosts.
#authentication_ <number>.port	Portnummer des LDAP-Servers.		
#authentication_ <number>. security_type	Authentifizierungsmethode, die vom Provider verwendet werden soll. Das System unterstützt nur die einfache Authentifizierung.	Einfach	Keine Änderung.

Parameter	Beschreibung	Bereitgestellter Wert	Änderung in
#authentication_ <number>. principle	Identität des zu authentifizierenden Principals, der dem System die Ausführung von Abfragen ermöglicht. Dieser Parameter stellt die Namenskomponente in einer LDAP ASN.1-Bindeanforderung dar.	cn=Manager, dc=amr, dc=stercomm, dc=com	Lokale Benennungsinformationen.
#authentication_ <number>. credentials	Im LDAP-Repository definiertes Kennwort für den LDAP-Principal, der dem System die Ausführung von Abfragen ermöglicht.	SecretPassword	Lokales Kennwort, das dem lokalen Principal zugeordnet ist.
#authentication_ <number>. security_protocol	Objekt zur Angabe des durch den Provider zu verwendenden Sicherheitsprotokolls.	SSL	Keine Änderung. Dieser Parameter wird nicht angezeigt, wenn Sie nicht mit SSL arbeiten.
#authentication_ <number>. password_attribute	Name des LDAP-Attributs, das das Benutzerkennwort enthält. Dieser Parameter wird nur verwendet, wenn für #LDAP_ AUTHENTICATE_ WITH_USER_BIND der Wert 'false' angegeben ist.	userPassword	Lokales Attribut, das das Kennwort enthält.
#authentication_ <number>. search_root	Objekt zur Angabe des Stammelements, auf dem die Benutzerabfrage basiert.	dc=amr, dc=stercomm, dc=com	Lokaler Suchpfad.
#authentication_ <number>.search_filter	Objekt zur Angabe der Vorlage, die in der Suche verwendet werden soll. Der Wert für <userid> wird dynamisch während der Anforderung durch die Benutzer-ID des Benutzers ersetzt, der die Authentifizierung anfordert.	(uid=<userid>)	Ein Windows Active Directory-Server kann einen Eintrag wie z. B. den folgenden verwenden: (sAMAccount Name=<userid>)

Parameter	Beschreibung	Bereitgestellter Wert	Änderung in
#authentication_ <number>. with_user_bind	Gibt an, ob ein Benutzer anhand einer erfolgreichen Bindung authentifiziert werden soll. False – Das System extrahiert den Wert für das Benutzerkennwort aus dem LDAP-Server und führt einen Vergleich mit den angegebenen Benutzerberechtigungen durch. True – Das System stellt eine Bindung zum LDAP-Server her und verwendet dazu den definierten Namen und die angegebenen Berechtigungsnachweise des Benutzers. Eine erfolgreiche Bindung bedeutet, dass der Benutzer erfolgreich authentifiziert wurde.	false	Dieser Wert muss in 'true' geändert werden, wenn die Authentifizierung anhand der Benutzerbindung durchgeführt werden soll.

7. Speichern Sie die Datei 'authentication_policy.properties.in'.
8. Geben Sie '/*installationsverzeichnis*/install/bin/setupfiles.sh' (UNIX) oder '*installationsverzeichnis*\install\bin\setupfiles.cmd' (Windows) ein, um die LDAP-Einträge in der Datei 'authentication_policy.properties' anhand der Daten in der Datei 'authentication_policy.properties.in' zu aktualisieren.
9. Starten Sie Sterling B2B Integrator.

   Die Änderungen an der Datei 'authentication_policy.properties' werden angewendet und Sie können dann mit der Verwendung des LDAP-Servers zur Authentifizierung von Benutzern beginnen.

   Nach dem Systemstart identifiziert das System LDAP-Server anhand der Angaben in der Datei 'authentication_policy.properties'. Das System authentifiziert externe Benutzer, wenn sich die entsprechenden Benutzer anmelden.

LDAP-Konfiguration überprüfen

Um zu überprüfen, ob LDAP (Lightweight Directory Access Protocol) mit Sterling B2B Integrator korrekt konfiguriert wurde, müssen Sie die Datei 'Authentication.log' unter 'Benutzerauthentifizierung' überprüfen, um sicherzustellen, dass das System die LDAP-Konfiguration übernommen hat.

Informationen zu diesem Vorgang

Wenn Probleme in Bezug auf die Herstellung der Verbindung zum LDAP-Verzeichnis bestehen oder wenn die LDAP-Authentifizierung fehlschlägt, dann müssen Sie die DEBUG-Protokollanweisungen in der Datei 'Authentication.log' überprüfen, um den aufgetretenen Fehler zu beheben. In der Datei 'Authentication.log' werden alle Anmeldeversuche (erfolgreiche und fehlgeschlagene) aufgezeichnet.

LDAP-Kennwörter verschlüsseln

Sie können LDAP-Kennwörter in Eigenschaftendateien ausblenden, indem Sie sie in der Datei 'customer_overrides.property' verschlüsseln.

Informationen zu diesem Vorgang

Die folgenden Parameter (Eigenschaften) können zum Verschlüsseln der LDAP-Kennwörter in der Datei 'customer_overrides.properties' verwendet werden:

Parameter/Eigenschaft	Beschreibung
authentication_policy.authentication _1.credentials	Dieser Parameter bzw. diese Eigenschaft steuert das Kennwort des Principals, das für den Zugriff auf eine LDAP-Instanz erforderlich ist. Dieses Kennwort sollte gesichert werden, da kein Kennwort, das die Sicherheit und den Zugriff steuert, im Klartextformat vorliegen sollte.
authentication_policy. LDAP_SECURITY_ TRUSTSTORE_PASSWORD	Dieser Parameter bzw. diese Eigenschaft steuert das Kennwort für den Truststore (JKS-Format), das zum Sichern von LDAP-Verbindungen benutzt wird. Die Kennphrase für diesen JKS (Java Keystore) muss angegeben werden, sodass auf den Truststore zugegriffen werden kann, da es sich bei ihm um eine verschlüsselte Datei handelt.
authentication_policy. LDAP_SECURITY_KEYSTORE_PASSWORD	Dieser Parameter bzw. diese Eigenschaft steuert das Kennwort, wenn zur Sicherung der Verbindungen zu einer angegebenen LDAP-Instanz die clientbasierte SSL-Authentifizierung verwendet wird.

Gehen Sie wie folgt vor, um LDAP-Kennwörter zu verschlüsseln:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis 'bin'.
2. Verwenden Sie 'encrypt_string.[sh/cmd]', um den tatsächlichen Wert der Eigenschaft bzw. des Parameters zu ermitteln, die bzw. den Sie verschlüsseln wollen.
3. Aktualisieren Sie die Parameter/Eigenschaften in der Datei 'customer_overrides.properties', sodass sie die folgenden Einträge aufweisen. Ersetzen Sie alle Vorkommen von <ENCVAL> durch den verschlüsselten Wert der nicht verschlüsselten Zeichenfolge, die für diese Eigenschaft auskommentiert wurde. Verwenden Sie dazu 'bin/encrypt_string.sh' (oder .cmd). Beispiel:

```
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
```

Benutzernachrichten

Benutzernachrichten

Die Funktion für Benutzernachrichten ermöglicht Ihnen das Bereitstellen von Nachrichten auf den Startseiten der Admin-Konsole. Über die Benutzernachrichten können Benutzer über Änderungen informiert oder an wichtige Ereignisse und Tasks erinnert werden.

Nachrichten können für die folgenden Benutzer bereitgestellt werden:

- Für alle Benutzer
- Für einen bestimmten Benutzer
- Für mehrere Benutzer

Das Nachrichtenelement wird auf der Basis eines Gültigkeitsdatums und eines Ablaufdatums angezeigt. Sie können die Nachricht auch wie folgt einrichten:

Nachrichtentyp	Symbol	Beschreibung
Benachrichtigung		Stellt Ankündigungsinformationen mit allgemeiner oder niedriger Priorität bereit.
Warnung		Stellt Ankündigungsinformationen mit hoher Priorität bereit.

Sie müssen über Schreibberechtigungen für 'Konten' verfügen, um Newsnachrichten für Benutzer zu erstellen. Durch das Löschen alter Nachrichten können Sie den Speicherbedarf und auch den Aufwand reduzieren, der zum Abrufen bestimmter Nachrichten aufgewendet werden muss.

Für Benutzernachrichten können die folgenden Tasks ausgeführt werden:

- Newsnachricht für Benutzer für bestimmte Benutzer erstellen
- Newsnachricht für Benutzer für alle Benutzer erstellen
- Newsnachricht für Benutzer suchen
- Newsnachricht für Benutzer bearbeiten
- Newsnachricht für Benutzer löschen

Newsnachrichten für Benutzer für alle Benutzer erstellen

Newsnachrichten für Benutzer können Sie für alle Benutzer über das **Verwaltungsmenü** erstellen.

Informationen zu diesem Vorgang

Bevor Sie beginnen können, benötigen Sie die folgenden Informationen:

Feld	Beschreibung
Typ	Der Typ der zu erstellenden Nachricht. Gültige Werte sind 'Notice' und 'Alert'.
Betreff	Der Betreff der Nachricht, die Sie erstellen.
Nachricht	Der Nachrichtentext der Nachricht, die Sie erstellen.

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzernachrichten** aus.
2. Klicken Sie neben **Neue Nachricht** auf **Los!**.
3. Geben Sie einen Wert für **Typ** ein.
4. Geben Sie den **Betreff** ein.
5. Geben Sie einen Wert für **Nachricht** ein.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie **Alle Benutzer** aus und klicken Sie auf **Weiter**.
8. Geben Sie das **Gültigkeitsdatum** der Nachricht (im Format jjjj-mm-tt) ein.
9. Geben Sie das **Ablaufdatum** der Nachricht (im Format jjjj-mm-tt) ein.
10. Klicken Sie auf **Weiter**.
11. Überprüfen Sie die Einstellungen für Newsnachrichten.
12. Klicken Sie auf **Fertig stellen**.

Newsnachrichten für Benutzer für bestimmte Benutzer erstellen

Newsnachrichten für bestimmte Benutzer können Sie über das **Verwaltungsmenü** erstellen.

Informationen zu diesem Vorgang

Bevor Sie beginnen können, benötigen Sie die folgenden Informationen:

Feld	Beschreibung
Typ	Der Typ der zu erstellenden Nachricht. Gültige Werte sind 'Notice' und 'Alert'.
Betreff	Der Betreff der Nachricht, die Sie erstellen.
Nachricht	Der Nachrichtentext der Nachricht, die Sie erstellen.

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzernachrichten** aus.
2. Klicken Sie neben **Neue Nachricht** auf **Los!**.
3. Geben Sie einen Wert für **Typ** ein.
4. Geben Sie einen Wert für **Betreff** ein.
5. Geben Sie einen Wert für **Nachricht** ein.

6. Klicken Sie auf **Weiter**.
7. Wählen Sie **Ausgewählte Benutzer** aus.
8. Wählen Sie den Namen der Benutzer aus, die diese Nachricht erhalten sollen.
9. Klicken Sie auf **Weiter**.
10. Geben Sie das **Gültigkeitsdatum** der Nachricht (im Format jjjj-mm-tt) ein.
11. Geben Sie das **Ablaufdatum** der Nachricht (im Format jjjj-mm-tt) ein.
12. Klicken Sie auf **Weiter**.
13. Überprüfen Sie die Einstellungen für Newsnachrichten.
14. Klicken Sie auf **Fertig stellen**.

Newsnachrichten für Benutzer suchen

Eine Newsnachricht für Benutzer können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Newsnachricht für Benutzer zu suchen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzernachrichten** aus.
2. Verwenden Sie eine der folgenden Suchoptionen:

Suchoptionen für Benutzernachrichten	**Aktion**
Nach Benutzer-ID	Wählen Sie entweder ALLE oder einen bestimmten Benutzer in der Liste aus.
Nach Betreff	Geben Sie einen Teil des Nachrichtentextes ein.
Nach gültigem Datumsbereich	Geben Sie den Datumsbereich (mm/tt/jjjj) ein.

3. Klicken Sie auf **Los!**. Auf der Seite 'Benutzernachrichten' werden alle Nachrichten aufgelistet, die mit Ihren Suchkriterien übereinstimmen.

Newsnachrichten für Benutzer bearbeiten

Eine Newsnachricht für Benutzer können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Newsnachricht zu bearbeiten:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzernachrichten** aus.
2. Suchen Sie nach der Newsnachricht für Benutzer, die bearbeitet werden soll.
3. Klicken Sie für die zu bearbeitende Newsnachricht für Benutzer auf 'Bearbeiten'.
4. Aktualisieren Sie den Typ der Nachricht, den Betreff oder die Nachricht selbst, sofern dies erforderlich ist.
5. Klicken Sie auf **Weiter**.

6. Aktualisieren Sie die Benutzer, die diese Nachricht erhalten sollen, sofern dies erforderlich ist, und klicken Sie dann auf **Weiter**.
7. Aktualisieren Sie den Wert für **Gültigkeitsdatum** der Nachricht (jjjj-mm-tt), sofern dies erforderlich ist.
8. Aktualisieren Sie den Wert für **Ablaufdatum** der Nachricht (jjjj-mm-tt), sofern dies erforderlich ist.
9. Klicken Sie auf **Weiter**.
10. Überprüfen Sie die Einstellungen für Newsnachrichten.
11. Klicken Sie auf **Fertig stellen**.

Newsnachrichten für Benutzer löschen

Eine Newsnachricht für Benutzer können Sie über das **Verwaltungsmenü** löschen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Newsnachricht zu löschen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Konten** > **Benutzernachrichten** aus.
2. Suchen Sie nach der Newsnachricht für Benutzer, die gelöscht werden soll.
3. Klicken Sie für die zu entfernende Newsnachricht auf **Löschen**.
4. Überprüfen Sie die Einstellungen für Newsnachrichten.
5. Klicken Sie auf **Löschen**. Daraufhin wird die folgende Nachricht angezeigt:
   ```
   Die Systemaktualisierung wurde erfolgreich ausgeführt.
   ```

Dokumentverschlüsselung

Übersicht zur Dokumentverschlüsselungsfunktion

Die Dokumentverschlüsselung wird mit Sterling B2B Integrator bereitgestellt, das eine zusätzliche Sicherheitsebene konfiguriert, die über die traditionellen Datei- und Datenbankberechtigungen hinausgeht. Wenn Sie Sterling File Gateway mit Sterling B2B Integrator integrieren, dann verwendet das Produkt dieselbe Dokumentverschlüsselungsfunktion zum Schutz momentan nicht verwendeter Daten.

Sterling File Gateway ist eine Anwendung zur sicheren Übertragung von Dateien zwischen Partnern mithilfe von verschiedenen Protokollen, Dateinamenskonventionen und Dateiformaten.

Die Dokumentverschlüsselungsfunktion wurde zum Schutz momentan nicht verwendeter Daten vor unbefugter Verwendung konzipiert. Die Funktion ermöglicht Ihnen die Verschlüsselung der Nutzdaten, die in der Datenbank und/oder im Dateisystem gespeichert sind. Darüber hinaus kann die Funktion verwendet werden, um zu verhindern, dass systemexterne Benutzer die Nutzdaten über einen direkten Zugriff auf die Datenbank oder das Dateisystem anzeigen können.

Wichtige Faktoren der Dokumentverschlüsselung:

- Standardmäßig ist bei der Installation keine Verschlüsselung konfiguriert. Wenn Sie Ihre Dokumente verschlüsseln wollen, dann müssen Sie diese Funktion aktivieren.

- Sie können diese Funktion jederzeit aktivieren, es werden jedoch nur die Dokumente verschlüsselt, die nach der Aktivierung der Verschlüsselungsfunktion empfangen wurden.
- Nachdem Sie diese Funktion aktiviert haben, wird die Verschlüsselung für alle Nutzdaten auf dem gesamten System durchgeführt.
- Nur die Dokumentnutzdaten werden verschlüsselt, die Metadaten jedoch **nicht**.
- Zur Ver- und Entschlüsselung wird derselbe Chiffrierschlüssel verwendet.
- Das System verwendet ein vordefiniertes Zertifikat (doccrypto) zum Verschlüsseln von Dokumenten. Sie können ein anderes Systemzertifikat erstellen. In diesem Fall müssen Sie den Wert von CERT_NAME in der Datei 'customer_overrides.properties' aktualisieren.

Obwohl die Aktivierung der Verschlüsselungsfunktion immer Auswirkungen auf die Leistung des Systems hat, variiert das Ausmaß dieser Auswirkungen beim einzelnen Kunden abhängig von der verwendeten Hardware, der Anzahl und der Größe der verarbeiteten Dokumente und abhängig vom relativen Verarbeitungsaufwand, der von einem bestimmten Server im Vergleich zu anderen Aktivitäten für die Dokumentpersistenz und den Dokumentabruf aufgewendet werden muss.

Chiffrierschlüssel für Dokumentverschlüsselung

Zur Ver- und Entschlüsselung von Datenbank- oder Dateisystemdokumenten wird derselbe Chiffrierschlüssel verwendet. Das digitale Zertifikat wird verwendet, um die Schlüssel zu generieren und zu verschlüsseln. Die Systemkennphrase wird verwendet, um die digitalen Zertifikate zu verschlüsseln.

Bei der Dokumentverschlüsselung wird ein Schlüssel pro Dokument erstellt und dieser Schlüssel wird zusammen mit dem Dokument als Teil der Metadaten gespeichert. Digitale Zertifikate werden wie andere Systemzertifikate auch gespeichert.

Das System verwendet ein vordefiniertes Zertifikat (doccrypto) zum Generieren und Verschlüsseln der Schlüssel, die zum Verschlüsseln der Dokumente verwendet werden. Sie können ein anderes Systemzertifikat erstellen. In diesem Fall müssen Sie den Wert von CERT_NAME in der Datei 'customer_overrides.properties' aktualisieren.

Anderes Zertifikat für Dokumentverschlüsselung zuordnen

Das System verwendet ein vordefiniertes Zertifikat (doccrypto) zum Verschlüsseln von Dokumenten. Sie können ein anderes Systemzertifikat zum Verschlüsseln von Dokumenten erstellen, zum Beispiel, wenn das vorherige Zertifikat demnächst abläuft. In diesem Fall müssen Sie den Wert von CERT_NAME in der Datei 'customer_overrides.properties' aktualisieren.

Informationen zu diesem Vorgang

Vorsicht: Löschen Sie das vorherige Systemzertifikat nicht und benennen Sie es nicht um. Das vorherige Zertifikat ist weiterhin erforderlich, um Dokumente zu entschlüsseln, die zuvor mit diesem Zertifikat verschlüsselt wurden. Das neue Systemzertifikat kann diese Dokumente nicht entschlüsseln, da es nicht zum Verschlüsseln der Dokumente verwendet wurde.

Bevor Sie mit dieser Prozedur beginnen, müssen Sie die folgenden Arbeitsschritte ausführen:

- Generieren Sie ein neues Zertifikat.

- Legen Sie den Namen des Zertifikats fest.

Gehen Sie wie folgt vor, um den Wert von CERT_NAME zu aktualisieren:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'properties'.
3. Öffnen Sie die Datei 'customer_overrides.properties'.
4. Fügen Sie der Datei folgende Zeile hinzu:
   ```
   security.CERT_NAME=name_of_new_system_certificate
   ```
5. Speichern und schließen Sie die Datei 'customer_overrides.properties'.
6. Stoppen Sie Sterling B2B Integrator und starten Sie das Produkt anschließend erneut.

Dokumentverschlüsselung für Dateisystem- und Datenbankdokumente aktivieren

Sie können Dateisystem- und Datenbankdokumente im Verzeichnis 'properties' verschlüsseln.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Dateisystem- und Datenbankdokumente zu verschlüsseln:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'properties'.
3. Öffnen Sie die Datei 'customer_overrides.properties'.
4. Fügen Sie die folgende Zeile zur Datei hinzu.
   ```
   security.ENC_DECR_DOCS=ENC_ALL
   ```
5. Speichern und schließen Sie die Datei 'customer_overrides.properties'.
6. Stoppen Sie Sterling B2B Integrator und starten Sie das Produkt anschließend erneut.

Dokumentverschlüsselung für Datenbankdokumente aktivieren

Sie können Datenbankdokumente im Installationsverzeichnis verschlüsseln.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Datenbankdokumente zu verschlüsseln:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'properties'.
3. Öffnen Sie die Datei 'customer_overrides.properties'.
4. Fügen Sie die folgende Zeile zur Datei hinzu.
   ```
   security.ENC_DECR_DOCS=ENC_DB
   ```
5. Speichern und schließen Sie die Datei 'customer_overrides.properties'.

6. Stoppen Sie Sterling B2B Integrator und starten Sie das Produkt anschließend erneut.

Dokumentverschlüsselung für Dateisystemdokumente aktivieren

Sie können Dateisystemdokumente im Installationsverzeichnis verschlüsseln.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Dateisystemdokumente zu verschlüsseln:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'properties'.
3. Öffnen Sie die Datei 'customer_overrides.properties'.
4. Fügen Sie die folgende Zeile zur Datei hinzu.
   ```
   security.ENC_DECR_DOCS=ENC_FS
   ```
5. Speichern und schließen Sie die Datei 'customer_overrides.properties'.
6. Stoppen Sie Sterling B2B Integrator und starten Sie das Produkt anschließend erneut.

Dokumentverschlüsselung für Dokumente inaktivieren

Sie können die Dokumentverschlüsselung im Verzeichnis 'properties' inaktivieren.

Informationen zu diesem Vorgang

Standardmäßig ist bei der Installation keine Verschlüsselung konfiguriert.

Gehen Sie wie folgt vor, um die Dokumentverschlüsselung zu inaktivieren:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'properties'.
3. Öffnen Sie die Datei 'customer_overrides.properties'.
4. Aktualisieren Sie den Wert von ENC_DECR_DOCS und geben Sie dabei NONE an. Beispiel:
   ```
   security.ENC_DECR_DOCS=NONE
   ```
5. Speichern und schließen Sie die Datei 'customer_overrides.properties'.
6. Stoppen Sie Sterling B2B Integrator und starten Sie das Produkt anschließend erneut.

Zertifikate

Digitale Zertifikate

Verwenden Sie IBM Key Management Utility (iKeyman), um die Verwaltung digitaler Zertifikate zu vereinfachen.

Das System verwendet die folgenden Typen digitaler Zertifikate.

- CA-Zertifikate und vertrauenswürdige Zertifikate - Digitale Zertifikate, für die das System nicht über die privaten Schlüssel verfügt. Diese Zertifikate werden im DER-Standardformat gespeichert.
- Systemzertifikate - Ein digitales Zertifikat, dessen privater Schlüssel im System verwaltet wird. Diese Zertifikate werden zusammen mit dem privaten Schlüssel in einem sicheren Format gespeichert.

Im Folgenden sind Basisinformationen zur Verwendung digitaler Zertifikate aufgeführt:

- Jede Organisation, die sichere Dokumente mit anderen Organisationen austauscht, muss über ein Zertifikat verfügen. Verwenden Sie iKeyman, um das Zertifikat zu generieren. Alternativ kann das Zertifikat auch extern generiert werden. Informationen zu iKeyman finden Sie in „IBM Key Management Utility (iKeyman)" auf Seite 66.
- Jedes Handelsprofil für einen Handelspartner, mit dem Sie signierte und verschlüsselte Dokumente austauschen, muss über ein Zertifikat verfügen.
- Eine Organisation oder ein Handelsprofil darf zu einem bestimmten Zeitpunkt immer nur über ein aktives Zertifikat verfügen. Wenn zwei Zertifikate vorhanden sind, dann kann die Organisation mit einem aktiven Paar von Zertifikaten arbeiten. Dabei wird eines der Zertifikate für die Signatur und das andere für die Verschlüsselung verwendet.
- Eine Organisation oder ein Handelsprofil muss über ein aktives Zertifikat verfügen, um erfolgreich signierte und verschlüsselte Dokumente austauschen zu können.
- Eine Organisation oder ein Handelsprofil kann über mehrere gültige Zertifikate verfügen.
- Zertifikate können zum Signieren von Dokumenten verwendet werden, die von Ihnen mit den verfügbaren Transportmethoden übertragen werden.
- Die Schlüssellänge für ein Zertifikat muss nicht mit der Schlüssellänge des Zertifikats des Handelspartners übereinstimmen.
- Es ist ratsam, die Empfehlungen zu den bewährten Verfahren (Best Practices) zur Public Key-Infrastruktur in der Schnelleinführung von Microsoft (Microsoft PKI Quick Guide) zu lesen und anzuwenden, bevor Sie einen Gültigkeitszeitraum für das Zertifikat angeben. Informationen zu Empfehlungen für bewährte Verfahren bei der Verwendung von Zertifikaten enthält http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

Unterstützte digitale Zertifikate

Sterling B2B Integrator unterstützt Version 3 X.509 der digitalen Zertifikate. Digitale Zertifikate können entweder selbst signiert oder von einer Zertifizierungsstelle (Certificate Authority, CA) signiert sein.

- Ein selbst signiertes Zertifikat ist ein digitales Zertifikat, das mit dem privaten Schlüssel signiert wird, der dem öffentlichen Schlüssel im Zertifikat zugeordnet ist. Hierdurch wird belegt, dass der Aussteller über den privaten Schlüssel verfügt, der dem öffentlichen Schlüssel des Zertifikats zugeordnet ist.
- Ein von einer Zertifizierungsstelle signiertes Zertifikat ist ein digitales Zertifikat, das mithilfe von Schlüsseln signiert wurde, die von den Zertifizierungsstellen verwaltet werden. Bevor ein Zertifikat ausgestellt wird, überprüft die Zertifizierungsstelle den Anforderer des Zertifikats, um festzustellen, ob er tatsächlich der Zertifikatseigner ist, auf den im Zertifikat verwiesen wird.

CA-Zertifikate

Ein CA-Zertifikat ist ein digitales Zertifikat, das von einer Zertifizierungsstelle (CA = Certificate Authority) ausgestellt wird. Die Zertifizierungsstelle überprüft vertrauenswürdige Zertifikate für vertrauenswürdige Stammzertifikate. Vertrauenswürdige Stammzertifikate bilden die Basis, auf der Zertifikatsketten in Zertifikaten erstellt werden.

Wenn Sie ein CA-Stammzertifikat als vertrauenswürdig anerkennen, dann bedeutet das, dass Sie auch alle Zertifikate als vertrauenswürdig einstufen, die von der zugehörigen Zertifizierungsstelle ausgestellt wurden. Wenn Sie das CA-Stammzertifikat als nicht vertrauenswürdig einstufen, dann erkennt Sterling B2B Integrator keines der von dieser Zertifizierungsstelle ausgegebenen Zertifikate als vertrauenswürdig an.

CA-Zertifikate enthalten einen öffentlichen Schlüssel, der einem privaten Schlüssel zugeordnet ist. Die Zertifizierungsstelle ist Eigner des privaten Schlüssels und verwendet ihn, um die von ihr ausgestellten Zertifikate zu signieren. Um ein vertrauenswürdiges Zertifikat zu überprüfen, müssen Sie zuerst ein CA-Zertifikat einchecken.

Stammzertifikate allgemeiner Zertifizierungsstellen sind in einem Java-Keystore (JKS) in der JVM (Java Virtual Machine) enthalten, die zum Lieferumfang von Sterling B2B Integrator gehört. Auf diese Weise können Benutzer bestimmte, auf Berechtigungen basierende Vertrauensbeziehungen einfacher einrichten, als dies möglich wäre, wenn sie über die Website einer Zertifizierungsstelle nach Zertifikaten suchen und diese dort anfordern müssten.

CA-Zertifikate werden innerhalb des Produkts separat von den vertrauenswürdigen Zertifikaten gespeichert.

Über die Benutzerschnittstelle können Sie CA-Stammzertifikate einchecken, die aus jeder der folgenden Quellen stammen können:

- Allgemeine CA-Stammzertifikate, die zum Lieferumfang von Sterling B2B Integrator gehören und im JKS (Java Keystore) bereitgestellt werden.
- Nur Zertifikate und vertrauenswürdige Zertifikate werden erkannt. Zertifikate und private Schlüssel werden in der Benutzerschnittstelle nicht angezeigt.
- SSL-Zertifikate, die von Handelspartnern importiert werden.
- Weitere, extern angeforderte Zertifikate.

Auf der Basis der Sicherheitsrichtlinien Ihrer Site können die im JKS enthaltenen CA-Zertifikate auch über die Konsole eingecheckt werden. Obwohl es sich bei CA-Zertifikaten um öffentliche Dokumente handelt, müssen Sie die Benutzer, denen Sie die Berechtigung zum Hinzufügen dieser Zertifikate erteilen, sorgfältig auswählen. Andernfalls besteht das Risiko, dass falsche CA-Zertifikate absichtlich hinzugefügt werden, um ebenfalls falsche Endbenutzerzertifikate als gültig zu bestätigen.

Namen für CA-Zertifikate

Der Name des CA-Zertifikats ist nicht Bestandteil des Inhalts des Zertifikats. Der Name wird im Allgemeinen anhand des RDN (Relative Distinguished Name; relativ definierter Name) des Ausstellers und anhand der Seriennummer des Zertifikats erstellt. Allerdings werden Zertifikate aus dem JKS (Java Keystore) mit einer beliebigen Zeichenfolge benannt.

Da der Zertifikatsname in der Systemdatenbank gespeichert und als Alias verwendet wird, um in der grafischen Benutzerschnittstelle auf das Zertifikat zu verwei-

sen, ist es möglicherweise sinnvoll, die CA-Zertifikate gemäß Ihrer Dateinamenskonventionen umzubenennen und einen kürzeren oder aussagekräftigeren Namen anzugeben. Zertifikate können umbenannt werden, wenn sie eingecheckt oder bearbeitet werden.

Vorteile selbst signierter und von einer Zertifizierungsstelle signierter digitaler Zertifikate

Je nach Ihren speziellen Anforderungen, sprechen bestimmte Argumente für bzw. gegen selbst signierte oder von einer Zertifizierungsstelle signierte Zertifikate.

Wenn Sie und Ihre Handelspartner darüber entscheiden, ob ein selbst signiertes Zertifikat generiert oder ein signiertes Zertifikat einer Zertifizierungsstelle erworben werden soll, dann sollten Sie die folgenden Faktoren berücksichtigen:

- Sie können selbst signierte Zertifikate mit Sterling B2B Integrator auf einfache Weise erstellen. Allerdings werden diese selbst signierten Zertifikate nicht von einer vertrauenswürdigen dritten Partei überprüft.
- Der Hauptvorteil der Verwendung von Zertifikaten einer Zertifizierungsstelle besteht darin, dass die Identität des Zertifikatseigners von einer vertrauenswürdigen dritten Partei überprüft wird. Nachteilig ist hingegen, dass diese Vorgehensweise mit zusätzlichen Kosten und einem höheren Verwaltungsaufwand verbunden ist. Wenn Sie sich für ein Zertifikat einer dritten Partei entscheiden, dann sollten Sie es von einer Zertifizierungsstelle anfordern.
- Eine Zertifizierungsstelle stellt eine zentrale Quelle für die Veröffentlichung und Anforderung von Informationen zu Zertifikaten (einschließlich Informationen zu widerrufenen Zertifikaten) bereit.

Standardmäßig stuft das System alle CA-Zertifikate und selbst signierten Zertifikate, die von der Anwendung generiert werden, als vertrauenswürdig ein. Sie können allerdings angeben, ob alle oder nur bestimmte der von einer bestimmten Zertifizierungsstelle ausgestellten Zertifikate als vertrauenswürdig eingestuft werden sollen. Außerdem können Sie explizit angeben, dass ein selbst signiertes Zertifikat eines Handelspartners als nicht vertrauenswürdig eingestuft werden soll.

Ablaufdatum von Zertifikaten

Wenn ein Adapter und ein Servlet für die eingehende Kommunikation verwendet wird, dann müssen Sie das Ablaufdatum der Systemzertifikate überwachen, um sicherzustellen, dass die Zertifikate gültig sind. Vor Ablauf der Zertifikate müssen Sie durch neue, gültige Zertifikate ersetzt werden.

Parameterdefinitionen für Systemzertifikate

Wenn ein Adapter und ein Servlet für die eingehende Kommunikation verwendet wird, dann müssen Sie das Ablaufdatum der Systemzertifikate überwachen, um sicherzustellen, dass die Zertifikate gültig sind. Vor Ablauf der Zertifikate müssen Sie durch neue, gültige Zertifikate ersetzt werden.

Parameter	Beschreibung
alias	Der Name des Schlüssels, der im HSM (Hardware Security Module; Hardwaresicherheitsmodul) gespeichert ist. Verwenden Sie nur solche Aliasnamen, die die Zeichen a - z, A - Z, 0 - 9 oder Bindestriche (-) enthalten und deren Gesamtlänge die Länge der GUID (global eindeutige ID) für das System nicht überschreitet.
certname	Der Name, der dem Systemzertifikat in der Datenbank zugewiesen wird.

Parameter	Beschreibung
Certtype	Der Typ des zu importierenden Zertifikats. Das System unterstützt die folgenden vier Zertifikatsdateitypen: pkcs12, pkcs8, pem und keystore. Sterling B2B Integrator unterstützt nur PEM-Schlüssel, die mit DES oder 3DES verschlüsselt wurden. Verwenden Sie keystore, um den Keystore aufzulisten oder zu importieren.
file	Der Name der zu importierenden Datei.
keypass	Die PIN (persönliche Identifikationsnummer) für den Slot (Bereich) auf der Eracom-Einheit.
keystoretype	Der Typ des zu importierenden Keystores. Der zulässige Wert ist CRYPTOKI.
keystoreprovider	Der Typ des Providers. Eracom ist der einzige Providertyp, der vom HSM unterstützt wird. Folgende Werte sind gültig: • ERACOM • ERACOM.n (wenn Sie Zertifikate in einen anderen als den an der ersten Position befindlichen Slot importieren)
password	Die Speicherkennphrase für die Zertifikatsdatei.
pkcs12file	Der Name der zu importierenden PKCS12-Datei.
pkcs12storepass	Die Speicherkennphrase, die zum Generieren der PKCS12-Datei verwendet wird.
pkcs12keypass	Die gültige Kennphrase für die PKCS12-Datei.
storepass	Die PIN (persönliche Identifikationsnummer) für den Slot auf der Eracom-Einheit, auf der sich der Keystore befindet.
systempass	Die Kennphrase für das System.

IBM Key Management Utility (iKeyman)

IBM Key Management Utility (iKeyman) ist eine Komponente des IBM SDK, die Schlüssel, Zertifizierungsanforderungen und selbst signierte Zertifikate generiert.

Sie können iKeyman verwendne, um Zertifikate für eine sichere Kommunikation zu erstellen und um Daten zu verschlüsseln bzw. zu entschlüsseln. Bei einer sicheren Übertragung mit SSL bieten Zertifikate einen weiteren Sicherheitsschutz.

In Sterling B2B Integrator können Sie iKeyman für die Erstellung von Folgendem verwenden:

- Zertifikatssignieranforderungen (CSRs = Certificate Signing Requests) - Eine Datei, die via E-Mail an eine Zertifizierungsstelle gesendet wird, um ein X.509-Zertifikat anzufordern.
- Schlüsselzertifikate - Eine Kombination eines in ASCII codierten Zertifikats und eines in ASCII codierten verschlüsselten privaten PKCS12-Schlüssels. Wenn Sie Schlüsselzertifikate mithilfe des Standardformats (default) mit bestimmten Codes generieren, dann tritt beim Ausgabezertifikat ein Fehler auf, wenn der Import in Sterling B2B Integrator durchgeführt wird. PKCS12 ist das empfohlene Format für Schlüsselzertifikate.

Weitere Informationen zum Konfigurieren und Verwenden von iKeyman siehe iKeyman Überblick für IBM SDK, Java Technology Edition 7.0.0

Zertifikattasks

Selbst signiertes Zertifikat erstellen

Ein selbst signiertes Zertifikat können Sie über das **Verwaltungsmenü** erstellen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein selbst signiertes Zertifikat zu erstellen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie neben **Selbst signiertes Zertifikat erstellen** auf **Los!**.
3. Geben Sie im Feld **Name** einen Namen für das selbst signierte Zertifikat ein.
4. Geben Sie den Namen für die **Organisation** ein, die als Quelle verwendet wird.
5. Wählen Sie das **Land** oder den Ursprung des selbst signierten Zertifikats aus.
6. Geben Sie als Kontaktadresse die **E-Mail** der Person ein, die in der Organisation für Zertifikate zuständig ist, und klicken Sie dann auf **Weiter**.
7. Geben Sie die **Seriennummer** des Zertifikats ein. Die Seriennummer ist die Nummer, die dem selbst signierten Zertifikat zugeordnet werden soll.
8. Geben Sie die Anzahl der Tage (**Dauer**) ein, die das selbst signierte Zertifikat gültig ist.

   Anmerkung: In V5.2.6.2 oder höher ist das maximale Ablaufdatum der *1. Januar 2080*. Für jede eingegebene Dauer, die zu einem Ablaufdatum nach dem 1. Januar 2080 führen würde, wird standardmäßig der *1. Januar 2080* angegeben. In früheren Versionen wurde keine Obergrenze gesetzt.
9. Geben Sie im Feld 'SubjectAltName' die **IP-Adressen** der Netzschnittstellen ein, die dem Zertifikat zugeordnet werden sollen.
10. Geben Sie im Feld 'SubjectAltName' die **DNS-Namen** der Netzschnittstellen ein, die dem Zertifikat zugeordnet werden sollen.
11. Wählen Sie **Schlüssellänge** aus. Wählen Sie dann eine der folgenden Schlüssellängenangaben aus:
    - 512
    - 1024
    - 2048

    Anmerkung: Die Schlüssellänge 1024 bietet ein gutes Mittelmaß in Bezug auf Sicherheit, Interoperabilität und Effizienz. Die Schlüssellänge 2048 ist zwar die sicherste, jedoch auch die langsamste Variante. Außerdem sind Probleme mit bestimmten Anwendungen zu erwarten.

    Anmerkung: Wenn Sie die Schlüssellänge 512 auswählen, müssen Sie auch JDK 7 SR5 verwenden. JDK 7 SR7 FP1 unterstützt keine Schlüssellängen unter 1024.
12. Wählen Sie einen **Signaturalgorithmus** aus.

13. Wählen Sie die Option **Bei Verwendung validieren** aus. Die folgenden Validierungsoptionen stehen zur Verfügung:
    - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
    - Aut.-Kette - Diese Option erstellt eine Zertifikatskette für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.
14. Setzen Sie das **Zertifikatsignatur-Bit**, indem Sie das entsprechende Kontrollkästchen auswählen.
15. Klicken Sie auf **Weiter**.
16. Überprüfen Sie die Informationen zum selbst signierten Zertifikat.
17. Klicken Sie auf **Fertig stellen**.

Vertrauenswürdiges Zertifikat automatisch von Handelspartnern anfordern

Das Dienstprogramm zur Erfassung von Zertifikaten automatisiert den Prozess zur Anforderung eines SSL-Zertifikats von einem Handelspartner. Diese Methode zum Anfordern von Zertifikatsinformationen ermöglicht einem Partner die einfache Verbindung und Speicherung eines Zertifikats.

Informationen zu diesem Vorgang

Falls dies gewünscht wird, kann anschließend eine externe Sicherheitsprüfung durchgeführt werden, bevor das Zertifikat als CA-Zertifikat oder vertrauenswürdiges Zertifikat in das System eingecheckt wird.

Vorbemerkungen:

- Überprüfen Sie, ob das Hostsystem Ihres Partners SSL-fähig ist.
- Fordern Sie Host- und Portinformationen für den Server Ihres Handelspartners an.
- Wenn der FTPS-Modus verwendet werden soll, dann stellen Sie fest, ob der Modus explizit oder implizit angegeben werden soll.
- Konfigurieren Sie die Standarddienstinstanz für SSLCertGrabberAdapter, um den entsprechenden Perimeterserver und (nur bei HTTPS) den Proxy-Server zu verwenden. Detaillierte Informationen hierzu finden Sie in der Dokumentation des Adapters.

Gehen Sie wie folgt vor, um das SSL-Zertifikat automatisch von einem Handelspartner anzufordern:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > Dienstprogramm zur Erfassung von Zertifikaten** aus.
2. Klicken Sie neben **Zertifikat für Erfassung von Partnern** auf **Los!**.
3. Wählen Sie den Verbindungstyp für den Server aus und klicken Sie auf **Weiter**.
    - FTPS
    - HTTPS
4. Geben Sie einen Wert für **Hostname** oder **IP-Adresse** ein.

5. Geben Sie die Nummer für den **Port** ein.
6. Wählen Sie den Verbindungsmodus für FTPS aus (oder überspringen Sie diesen Schritt, wenn Sie HTTPS verwenden):
   - Explizit – Die SSL-Vereinbarung findet nach der Herstellung der FTP-Verbindung statt. Dies ist die Standardeinstellung.
   - Implizit – Die SSL-Vereinbarung findet vor der Herstellung der FTP-Verbindung statt.
7. Klicken Sie auf **Weiter**. Das System versucht, eine Verbindung herzustellen und Zertifikate abzurufen.
8. Nach Abschluss der Erfassung müssen Sie die Übersichtsdaten überprüfen und festlegen, welche Zertifikate Sie speichern möchten.
9. Wählen Sie eine Verschlüsselungsmethode für jedes Zertifikat aus und klicken Sie dann auf **Speichern**. Folgende Verschlüsselungsformate sind möglich:
   - BASE64 – Verwendet die BASE64-Verschlüsselung im DER-Standardzertifikat. Dies ist die Standardeinstellung.
   - DER – Standardformat für digitale Zertifikate, das von den meisten Anwendungen akzeptiert wird.
10. Klicken Sie auf **Speichern** und rufen Sie die Position auf, unter der die Datei gespeichert werden soll.
11. Übernehmen Sie den Standarddateinamen oder bearbeiten Sie den Namen auf der Basis Ihrer Dateinamenkonventionen. Klicken Sie anschließend auf **Speichern**.
12. Nach der Speicherung können die Zertifikate in das System eingecheckt werden. Gehen Sie wie folgt vor, wenn Sie sich für das Einchecken eines Zertifikats in das System entschieden haben:
    a. Überprüfen Sie, ob jedes der Zertifikate gültig und vertrauenswürdig ist.
    b. Checken Sie das Zertifikat abhängig von der jeweiligen Funktion als CA-Zertifikat oder als vertrauenswürdiges Zertifikat ein. Für eine Vertrauensstellung, die sich auf die Zertifizierungsstelle gründet, müssen Sie möglicherweise die Zertifikatskette einchecken und dabei das Endbenutzerzertifikat ausschließen. Für eine direkte Vertrauensstellung checken Sie das Endbenutzerzertifikat ein.

Statusinformationen in Zertifikatzusammenfassungen konfigurieren

Standardmäßig werden die Informationen zum Zertifikatstatus am Ende Popup-Fensters mit der Zusammenfassung bereitgestellt, wenn ein mit einem Hyperlink versehener Zertifikatsname ausgewählt wird. Sie haben die Möglichkeit, die Statusinformationen ein- oder auszuschließen. Da die Statusinformationen in Echtzeit kompiliert werden, möchten Sie sie möglicherweise nicht einschließen.

Informationen zu diesem Vorgang

Die Eigenschaft VerificationOnPopupInfo steuert, ob die Statusinformationen in der Zertifikatzusammenfassung angezeigt werden. Diese Eigenschaft wird in der Datei 'ui.properties' gespeichert. Die Werte für die Eigenschaft VerificationOnPopupInfo lauten wie folgt:

- true - Die Validierungsinformationen werden eingeschlossen (Standardwert).
- false - Die Validierungsinformationen werden im Popup-Fenster nicht kompiliert oder angezeigt.
- (andere Werte) - Die Validierungsinformationen werden eingeschlossen.

Gehen Sie wie folgt vor, um zu verhindern, dass die Statusinformationen kompiliert und angezeigt werden:

Vorgehensweise

1. Öffnen Sie die Datei 'ui.properties'.
2. Aktualisieren Sie den Wert für VerificationOnPopupInfo und geben Sie 'false' an. Beispiel:

   ```
   VerificationOnPopupInfo=false
   ```

3. Speichern und schließen Sie die Datei.
4. Führen Sie für Sterling B2B Integrator einen Neustart durch.

Anzeige des Fingerabdrucks konfigurieren

Zusätzlich zu dem vorab berechneten SHA1-Hashwert können weitere Fingerabdrücke für das Zertifikat in der Zertifiaktanzeige, in Bestätigungs- und in Zusammenfassungsanzeigen aufgeführt werden. Die Berechnung von Hashwerten wird bedarfsgesteuert ausgeführt, wenn eine Anzeige generiert wird.

Informationen zu diesem Vorgang

Zusätzliche Fingerabdruckanzeigen werden in den Anzeigen der grafischen Benutzerschnittstelle angezeigt, haben jedoch keine Auswirkungen auf die Nachrichtenbehandlung oder die Systemkommunikation.

Gehen Sie wie folgt vor, um das System für die Berechnung und Anzeige zusätzlicher Zertifikatfingerabdrücke zu konfigurieren:

Vorgehensweise

1. Ändern Sie in der Datei 'ui.properties' die folgende Zeile:

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   Wenn Sie mehr als einen zusätzlichen Hashwert anzeigen wollen, dann trennen Sie die einzelnen Werte durch Kommas. Beispiel:

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

Parameter	Beschreibung
hash_algorithm	Der Name eines Hashalgorithmus, der auf den Zertifikatfingerabdruck angewendet werden soll. Folgende Werte sind gültig: • SHA-256 • SHA-384 • SHA-512

2. Speichern und schließen Sie die Datei 'ui.properties'.
3. Führen Sie für Sterling B2B Integrator einen Neustart durch.

CA-Zertifikate suchen

Ein CA-Zertifikat können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein CA-Zertifikat zu suchen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:

- Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > CA** aus.
- Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.

2. Führen Sie einen der folgenden Arbeitsschritte aus und klicken Sie dann auf **Los!**.
   - Geben Sie unter 'Suchen' im Feld **Nach Zertifikatsname** entweder einen Teil des Namens oder den vollständigen Namen des CA-Zertifikats ein, das Sie suchen möchten. Auf der Seite 'Digitale CA-Zertifikate' werden alle CA-Zertifikate aufgelistet, die mit Ihren Suchkriterien übereinstimmen.
   - Wählen Sie unter 'Auflisten' im Feld **Alphabetisch** die Option **ALLE** oder den Buchstaben aus, mit dem der Name des CA-Zertifikats beginnt, nach dem Sie suchen. Wenn Sie ALLE auswählen, werden alle CA-Zertifikate aufgelistet. Auf der Seite 'Digitale CA-Zertifikate' werden alle CA-Zertifikate aufgelistet, die mit Ihren Suchkriterien übereinstimmen.

Übersichtsdaten zum CA-Zertifikat anzeigen

Wenn eine Liste mit Zertifikaten angezeigt wird, können Sie auf den Zertifikatsnamen klicken, um die Übersichtsdaten zu diesem Zertifikat anzuzeigen. Sie können den Systemnamen, den Fingerabdruck und den Status konfigurieren.

Informationen zu diesem Vorgang

Auf dem System können die folgenden Felder konfiguriert werden.

Zertifikatzusammenfassungsfeld	**Beschreibung**
Systemname	Der Zertifikatsname ist die Datenbankbezeichnung. Er wird verwendet, um in der grafischen Benutzerschnittstelle auf dieses Zertifikat zu verweisen und dient zum Speichern dieses Namens in der zugehörigen Datenbank. Der Standardname für ein Zertifikat aus dem JKS (Java Keystore) ist eine beliebige Zeichenfolge. Namen für andere Zertifikate werden anhand des RDN (relativ definierter Name) des Ausstellers und der Seriennummer des Zertifikats erstellt. Sie können einen Zertifikatsnamen in einen kürzeren oder einfacher zu erkennenden Namen ändern, wenn Sie das Zertifikat einchecken oder bearbeiten.
Fingerabdruck	Informationen zum SHA1-Hashwert sind standardmäßig enthalten. Um die Berechnung und Anzeige von Fingerabdruckinformationen für andere Hashwerte zu konfigurieren, müssen Sie die Datei 'ui.properties' bearbeiten.
Status	Eine Echtzeitüberprüfung des aktuellen Status, in der angegeben ist, ob die Zertifikatsdatumsangaben gültig sind, und ob das Zertifikat überprüft wurde. Um zu konfigurieren, ob diese Informationen während der Anzeige berechnet werden, müssen Sie die Datei 'ui.properties' bearbeiten.

Obwohl diese Informationen für die Übersichtsdaten eines CA-Zertifikats gelten, werden ähnliche Felder auch in den Übersichts- und Bestätigungsanzeigen für andere Zertifikatstypen aufgeführt.

CA-Zertifikate aus der Benutzerschnittstelle einchecken

Ein CA-Zertifikat können Sie in der Benutzerschnittstelle über das **Verwaltungsmenü** einchecken.

Informationen zu diesem Vorgang

Auf der Basis der Sicherheitsrichtlinien Ihrer Site können die im JKS enthaltenen CA-Zertifikate auch über die Konsole eingecheckt werden.

Bevor Sie beginnen, speichern Sie alle CA-Zertifikate, die Sie extern angefordert haben, in einer lokalen Datei.

Gehen Sie wie folgt vor, um ein CA-Zertifikat einzuchecken:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > CA** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie neben **Neues Zertifikat einchecken** auf **Los!**.
3. Wählen Sie eine Methode für den Import von Zertifikaten aus:

Importmethode	Nächste Schritte
Aus JVM importieren – Importiert aus dem JKS (Java Keystore)	1. Klicken Sie auf **Aus JVM importieren**. 2. Übernehmen Sie das Standardkennwort, das im Kennwortfeld angezeigt wird, und klicken Sie auf **Weiter**. Das Standardkennwort für den Keystore wird von Sun Microsystems bereitgestellt. Wenn das Kennwortfeld leer ist, dann verwendet das System trotzdem das Standardkennwort.
Aus Datei importieren - Importiert Zertifikate, die als Datei auf dem lokalen Laufwerk gespeichert wurden.	1. Klicken Sie auf **Aus Datei importieren**. 2. Geben Sie den Dateinamen ein oder klicken Sie auf **Durchsuchen**, um eine CA-Zertifikatsdatei auszuwählen. Klicken Sie auf 'Weiter'. Sie können das im Kennwortfeld angezeigte Kennwort ignorieren. Der Eintrag muss nicht gelöscht werden.

   Verfügbare Zertifikate werden mit einer Zusammenfassung von Identifikationsinformationen aufgelistet. Standardmäßig sind alle Zertifikate ausgewählt.
4. Klicken Sie auf die Kontrollkästchen links neben den einzelnen Einträgen, um Zertifikate für den Import aus- oder abzuwählen.
5. Für jedes ausgewählte Zertifikat müssen Sie den vorgeschlagenen Zertifikatsnamen übernehmen oder ihn gemäß den Dateinamenskonventionen Ihres Systems bearbeiten.
6. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:
   - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.

- Aut.-Kette - Diese Option erstellt eine Zertifikatskette bis zum Stammelement für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.

7. Wenn Sie eine Nachricht erhalten, in der Sie darüber informiert werden, dass das Zertifikat mit einem bereits in der Datenbank vorhandenen Zertifikat identisch ist, dann geben Sie J oder N ein, um anzugeben, ob das doppelte Zertifikat importiert werden soll.

   Diese Überprüfung wird nur für einzelne Zertifikate durchgeführt. Sie wird nicht durchgeführt, wenn eines oder auch mehrere Zertifikate aus einer Datei eingecheckt werden.

   Zertifikate werden anhand eines SHA1-Hashwerts identifiziert und auf Duplikate überprüft. In der Datenbank können mehrere Kopien eines Zertifikats vorhanden sein, da jedes sich in einer anderen Zeile befindet und jedem eine andere Objekt-ID zugewiesen ist. Das vorhandene Zertifikat wird nicht überschrieben.
8. Überprüfen Sie die CA-Zertifikatsinformationen.
9. Klicken Sie auf **Fertig stellen**.

CA-Zertifikate über die Konsole einchecken

Nachdem Sie beliebige CA-Zertifikate in einer lokalen Datei gespeichert haben, können Sie die CA-Zertifikate über die Konsole aus dem Installationsverzeichnis einchecken.

Informationen zu diesem Vorgang

Allgemeine CA-Zertifikate sind in einem JKS (Java Keystore) enthalten, der zur JVM (Java Virtual Machine) gehört, die im Lieferumfang von Sterling B2B Integrator enthalten ist. Der JKS befindet sich im Verzeichnis '/install_dir/jdk/jre/lib/security/cacerts'. Sie können Zertifikate allerdings auch extern anfordern.

Um Zertifikate in das Repository für vertrauenswürdige Zertifikate von Sterling B2B Integrator zu importieren, müssen Sie den Befehl unter '/installationsverzeichnis/install/bin/ImportCACerts.sh' (UNIX) oder '\installationsverzeichnis\install\bin\ImportCACerts.cmd' (Windows) ändern.

Bevor Sie beginnen, speichern Sie alle CA-Zertifikate, die Sie extern angefordert haben, in einer lokalen Datei.

Gehen Sie wie folgt vor, um ein CA-Zertifikat über die Konsole einzuchecken:

Vorgehensweise

1. Navigieren Sie zum Installationsverzeichnis.
2. Navigieren Sie zum Verzeichnis 'bin'.
3. Geben Sie den folgenden Befehl ein:

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   Alle Zertifikate in der Datei werden einzeln aufgelistet. Dabei gelten allerdings die folgenden Ausnahmen:

   - Einträge, die symmetrische oder private Schlüssel enthalten, werden nicht verarbeitet oder aufgelistet.

- Nur das erste Zertifikat in einer Datei im DER-Format wird verarbeitet und aufgelistet.

4. Geben Sie auf die entsprechende Eingabeaufforderung hin für jedes zu importierende Zertifikat 'J' (Groß-/Kleinschreibung muss nicht beachtet werden) ein.
5. Für jedes akzeptierte Zertifikat müssen Sie den vorgeschlagenen Zertifikatsnamen übernehmen oder ihn gemäß den Dateinamenskonventionen Ihres Systems bearbeiten.
6. Wenn die Zertifikatsbezeichnung mit einer Zertifikatsbezeichnung übereinstimmt, die in der Datenbank bereits vorhanden ist, dann geben Sie `J` oder `N` (Groß-/Kleinschreibung muss nicht beachtet werden) ein, um festzulegen, ob die Bezeichnung geändert werden soll. Obwohl Zertifikate nicht generell anhand der Bezeichnung identifiziert werden und die Datenbank doppelte Bezeichnungen zulässt, werden Zertifikate in bestimmten Diensten anhand der Bezeichnung gesucht. Vermeiden Sie deshalb doppelte Bezeichnungen, um ein unerwartetes Verhalten des Systems auszuschließen.
7. Wenn das Zertifikat (gemäß dem SHA1-Hashwert des Zertifikats) ein Duplikat eines bereits in der Datenbank vorhandenen Zertifikats darstellt, dann geben Sie durch Auswahl von 'J' oder 'N' an, ob das Duplikat importiert werden soll.

   Zertifikate werden anhand eines SHA1-Hashwerts identifiziert und auf Duplikate überprüft. In der Datenbank können mehrere Kopien eines Zertifikats vorhanden sein, da jedes sich in einer anderen Zeile befindet und jedem eine andere Objekt-ID zugewiesen ist. Das vorhandene Zertifikat wird nicht überschrieben.

CA-Zertifikate bearbeiten

Ein CA-Zertifikat können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein CA-Zertifikat zu bearbeiten:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > CA** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Suchen Sie anhand von 'Suchen' oder 'Auflisten' das CA-Zertifikat, das Sie bearbeiten wollen, und klicken Sie dann auf **Los!**.
3. Klicken Sie neben dem **CA-Zertifikat**, das bearbeitet werden soll, auf **Bearbeiten**.
4. Geben Sie den Zertifikatsnamen ein.
5. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:
   - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
   - Aut.-Kette - Diese Option erstellt eine Zertifikatskette für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.

6. Überprüfen Sie die CA-Zertifikatsinformationen.
7. Klicken Sie auf **Fertig stellen**.

CA-Zertifikate löschen

Ein CA-Zertifikat können Sie über das **Verwaltungsmenü** löschen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein CA-Zertifikat zu löschen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > CA** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie neben **Alphabetisch** auf **Los!**.
3. Klicken Sie neben dem CA-Zertifikat, das gelöscht werden soll, auf **Löschen**.

Systemzertifikate suchen

Ein Systemzertifikat können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Systemzertifikat zu suchen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Führen Sie in den Systemzertifikaten eine der folgenden Aktionen aus und klicken Sie dann auf **Los!**.
   - Geben Sie unter 'Suchen' im Feld **Nach Zertifikatsname** entweder einen Teil des Namens oder den vollständigen Namen des Systemzertifikats ein, das Sie suchen möchten. Auf der Seite 'Systemzertifikate' werden alle Systemzertifikate aufgelistet, die den vollständigen Namen oder den Teil des Namens enthalten, den Sie eingegeben haben.
   - Wählen Sie unter **Auflisten** im Feld **Alphabetisch** die Option **ALLE** oder den Buchstaben aus, mit dem der Name des CA-Zertifikats beginnt, nach dem Sie suchen. Wenn Sie ALLE auswählen, werden alle Systemzertifikate aufgelistet. Auf der Seite 'Systemzertifikate' werden alle Systemzertifikate aufgelistet, die mit Ihren Suchkriterien übereinstimmen.

Systemzertifikate bearbeiten

Ein Systemzertifikat können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Systemzertifikat zu bearbeiten:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Suchen Sie anhand von 'Suchen' oder 'Auflisten' das **Systemzertifikat**, das Sie bearbeiten wollen, und klicken Sie dann auf **Los!**.
3. Klicken Sie neben dem Systemzertifikat, das bearbeitet werden soll, auf **Bearbeiten**.
4. Geben Sie einen Wert für **Zertifikatsname** ein.
5. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:
   - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
   - Aut.-Kette - Diese Option erstellt eine Zertifikatskette für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.
6. Überprüfen Sie die Informationen zum Systemzertifikat.
7. Klicken Sie auf **Fertig stellen**.

Systemzertifikate in Sterling B2B Integrator angeben

Ein Systemzertifikat können Sie über das **Verwaltungsmenü** angeben.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Systemzertifikat anzugeben:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Bereitstellung > Dienste > Konfiguration** aus.
2. Wählen Sie im Abschnitt 'Liste' den anzuwendenden Dienst- oder Adaptertyp in der Liste **nach Diensttyp** aus und klicken Sie dann auf **Los!**.
3. Wählen Sie in der Liste der Konfigurationen die gewünschte Konfiguration aus.
4. Klicken Sie auf **Dienstname**, um die Konfigurationsinformationen anzuzeigen.
5. Überprüfen Sie die Zertifikatszusammenfassungsinformationen.

Ablaufdatum eines Systemzertifikats überprüfen

Wenn ein Adapter und ein Servlet für die eingehende Kommunikation verwendet wird, dann müssen Sie das Ablaufdatum der Systemzertifikate überwachen, um sicherzustellen, dass die Zertifikate gültig sind.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um das Ablaufdatum eines Systemzertifikats zu überprüfen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Um alle Systemzertifikate anzuzeigen, wählen Sie in der Dropdown-Liste 'Alphabetisch' den Eintrag **Alle** aus und klicken dann auf **Los!**.
3. Wählen Sie den Namen des Systemzertifikats aus, das angezeigt werden soll. Daraufhin wird die Zertifikatzusammenfassung angezeigt.
4. Überprüfen Sie im Abschnitt **Beschreibung** der Zertifikatzusammenfassung die im Feld **Gültige Datumsangaben** aufgeführten Informationen.
5. Überprüfen Sie die im Abschnitt **Status** angegebenen Informationen, um festzustellen, ob die Datumsangaben zulässig sind und das Zertifikat überprüft wurde.

Systemzertifikate in Sterling B2B Integrator exportieren

Dieser Exportbefehl gilt nur für Sterling B2B Integrator-Systemzertifikate. Sie können den Befehl nicht zum Exportieren von Systemzertifikaten in ein Hardwaresicherheitsmodul (HSM) verwenden.

Informationen zu diesem Vorgang

Geben Sie zum Exportieren eines Systemzertifikats den folgenden Befehl mit den entsprechenden Parametern ein:

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

Parameter	Beschreibung
keyname	Der Schlüsselname des Systemschlüssels, der exportiert werden soll.
pkcs12filename	Der Name der Datei, die die exportierten Informationen enthält.
pkcs12storepass	Das Speicherkennwort, das den Speicher schützt.
pkcs12keypass	Das Schlüsselkennwort, das den Schlüssel schützt.

Systemzertifikate in Sterling B2B Integrator löschen

Sie können eine Kopie des Systemzertifikats auf Ihre lokale Platte exportieren, bevor Sie es löschen. Bei 'OpsDrv', 'OpsKey' und 'UIKeys' handelt es sich um Systemzertifikate, die nicht gelöscht werden können.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Systemzertifikat zu löschen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.

2. Klicken Sie neben **Alphabetisch** auf **Los!**.
3. Klicken Sie neben dem Systemzertifikat, das gelöscht werden soll, auf **Löschen**.
4. Klicken Sie auf der Seite 'Bestätigen' auf **Löschen**.

Systemzertifikate auschecken

Um ein Systemzertifikat zu exportieren, müssen Sie es zuerst auschecken. Mit der folgenden Prozedur wird lediglich das öffentliche Zertifikat exportiert, nicht jedoch der private Schlüssel. Dadurch erhalten Sie ein öffentliches Zertifikat, das an einen Handelspartner gesendet werden kann.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Systemzertifikat auszuchecken:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Suchen Sie anhand von 'Suchen' oder 'Auflisten' das Systemzertifikat, das ausgecheckt werden soll.
3. Klicken Sie neben dem Systemzertifikat, das Sie auschecken wollen, auf **Auschecken**.
4. Wählen Sie im Dialogfeld **Systemzertifikat auschecken** das Zertifikatsformat aus und klicken Sie dann auf **Los!**:
   - PKCS12 – Diese Option dient zum Formatieren des digitalen Zertifikats als PKCS12-Datei. Sie haben auch die Möglichkeit, ein Kennwort für den privaten Schlüssel und ein Kennwort für den Schlüsselspeicher (Keystore) einzugeben.
   - BASE64 – Diese Option verwendet die BASE64-Verschlüsselung für das DER-Standardzertifikat.
   - DER – Dieses Standardformat für digitale Zertifikate wird von den meisten Anwendungen akzeptiert.
5. Klicken Sie im Dialogfeld **Dateidownload** auf **Speichern**.
6. Wählen Sie im Dialogfeld **Speichern unter** die Position aus, unter der das Zertifikat gespeichert werden soll, und klicken Sie dann auf **Speichern**. Die Option zum Öffnen des Zertifikats wird nicht unterstützt. Sie müssen das Zertifikat innerhalb des Betriebssystems öffnen. Wenn Sie eine Fehlernachricht erhalten, in der Sie darüber informiert werden, dass die Datei für das Sicherheitszertifikat ungültig ist, dann öffnen Sie die Datei in einem Texteditor und löschen Sie alle Leerzeilen, die sich vor der Zeichenfolge -----BEGIN CERTIFICATE----- befinden. Speichern Sie die bearbeitete Datei und versuchen Sie anschließend, sie zu öffnen.
7. Klicken Sie im Dialogfeld 'Systemzertifikat auschecken' auf **Schließen**. Daraufhin wird die Seite 'Systemzertifikat' angezeigt.

Vertrauenswürdige Zertifikate suchen

Ein vertrauenswürdiges Zertifikat können Sie über das **Verwaltungsmenü** suchen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Zertifikat zu suchen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > Vertrauenswürdig** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Führen Sie auf der Seite 'Vertrauenswürdige digitale Zertifikate' eine der folgenden Aktionen aus und klicken Sie dann auf **Los!**.
   - Geben Sie unter 'Suchen' im Feld **Nach Zertifikatsname** entweder einen Teil des Namens oder den vollständigen Namen des vertrauenswürdigen Zertifikats ein, das Sie suchen möchten. Auf der Seite 'Vertrauenswürdige digitale Zertifikate' werden alle vertrauenswürdigen Zertifikate aufgelistet, die mit Ihren Suchkriterien übereinstimmen.
   - Wählen Sie im Feld **Alphabetisch auflisten** die Option **ALLE** oder den Buchstaben aus, mit dem der Name des vertrauenswürdigen Zertifikats beginnt, nach dem Sie suchen. Auf der Seite 'Vertrauenswürdige digitale Zertifikate' werden alle vertrauenswürdigen Zertifikate aufgelistet, die mit Ihren Suchkriterien übereinstimmen.

Vertrauenswürdige Systemzertifikate einchecken

Sie können vertrauenswürdige Zertifikate einchecken (z. B. von Handelspartnern importierte SSL-Zertifikate oder andere externe Zertifikate).

Informationen zu diesem Vorgang

Vertrauenswürdige Zertifikate können aus den folgenden Quellen stammen:

- Von Handelspartnern importierte SSL-Zertifikate
- Andere, extern angeforderte Zertifikate

Bevor Sie beginnen, müssen Sie das vertrauenswürdige Systemzertifikat in einer Datei auf Ihrem lokalen Computer speichern.

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Systemzertifikat einzuchecken:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > Vertrauenswürdig** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie neben **Neues Zertifikat einchecken** auf **Los!**.
3. Geben Sie einen Wert für **Dateiname** ein oder klicken Sie auf **Durchsuchen**, um den Dateinamen des vertrauenswürdigen Zertifikats auszuwählen. Klicken Sie dann auf **Weiter**.
4. Geben Sie einen Wert für **Zertifikatsname** ein.

5. Überprüfen Sie den Namen des vertrauenswürdigen Zertifikats, das eingecheckt werden soll. Für jedes ausgewählte Zertifikat wird im Feld 'Zertifikatsname' ein Name vorgeschlagen. Anschließend wird eine Zusammenfassung der Identifikationsinformationen aufgeführt, die im Zertifikat enthalten sind. Sie können den Namen unter Berücksichtigung Ihrer Dateinamenskonventionen ändern.
6. Wenn die ausgewählte Datei mehrere vertrauenswürdige Zertifikate enthält, dann wählen Sie das Kontrollkästchen links neben den einzelnen Zertifikaten aus, um das jeweils zugehörige Zertifikat einzuchecken.
7. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:
   - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
   - Aut.-Kette - Diese Option erstellt eine Zertifikatskette bis zum Stammelement für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.
   - CRL-Cache - Steuert, ob der CRL-Cache bei jeder Verwendung des Systemzertifikats abgefragt wird.
8. Überprüfen Sie die Informationen zum vertrauenswürdigen Zertifikat.
9. Klicken Sie auf **Fertig stellen**.

Vertrauenswürdige Zertifikate bearbeiten

Ein vertrauenswürdiges Zertifikat können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Zertifikat zu bearbeiten:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > Vertrauenswürdig** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Suchen Sie anhand von 'Suchen' oder 'Auflisten' das vertrauenswürdige Zertifikat, das Sie bearbeiten wollen, und klicken Sie dann auf **Los!**.
3. Klicken Sie neben dem vertrauenswürdigen Zertifikat, das Sie bearbeiten möchten, auf **Bearbeiten**.
4. Geben Sie einen Wert für **Zertifikatsname** ein.
5. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:
   - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
   - Aut.-Kette - Diese Option erstellt eine Zertifikatskette bis zum Stammelement für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit

gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.
    - CRL-Cache - Steuert, ob der CRL-Cache bei jeder Verwendung des Systemzertifikats abgefragt wird.
6. Überprüfen Sie die Zertifikatsinformationen.
7. Klicken Sie auf **Fertig stellen**.

Vertrauenswürdige Systemzertifikate löschen

Ein vertrauenswürdiges Systemzertifikat können Sie über das **Verwaltungsmenü** löschen.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein vertrauenswürdiges Systemzertifikat zu löschen:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
    - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > Vertrauenswürdig** aus.
    - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie neben **Alphabetisch** auf **Los!**.
3. Klicken Sie neben dem vertrauenswürdigen Zertifikat, das gelöscht werden soll, auf **Löschen**.

PKCS12-Systemzertifikate importieren

Sie können ein PKCS12-Systemzertifikat importieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein PKCS12-Systemzertifikat zu importieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein:

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

PKCS12-Systemzertifikate einchecken

Nachdem Sie das PKCS12-Systemzertifikat in einer Datei auf Ihrem lokalen Computer gespeichert haben, können Sie das PKCS12-Systemzertifikat über das **Verwaltungsmenü** einchecken.

Informationen zu diesem Vorgang

Bevor Sie beginnen, müssen Sie das PKCS12-Systemzertifikat in einer Datei auf Ihrem lokalen Computer speichern.

Gehen Sie wie folgt vor, um ein PKCS12-Systemzertifikat einzuchecken:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie auf der Seite 'Systemzertifikate' unter 'Einchecken' neben **PKCS12-Zertifikat** auf **Los!**.
3. Geben Sie im Feld **Zertifikatsname** den Namen des PKCS12-Zertifikats ein.
4. Geben Sie einen Wert für **Kennwort für privaten Schlüssel** ein. Dies ist das Kennwort, das zur Verschlüsselung des PKCS12-Zertifikats verwendet wird.
5. Geben Sie einen Wert für **Kennwort für Schlüsselspeicher** ein. Dies ist das Kennwort für das PKCS12-Objekt. Es kann mit dem Kennwort für den privaten Schlüssel übereinstimmen.
6. Geben Sie einen Wert für **Dateiname** ein oder klicken Sie auf **Durchsuchen**, um den Dateinamen des PKCS12-Zertifikats auszuwählen. Klicken Sie dann auf **Weiter**.
7. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:
   - Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
   - Aut.-Kette - Diese Option erstellt eine Zertifikatskette für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.
8. Überprüfen Sie die Informationen zum PKCS12-Systemzertifikat.
9. Klicken Sie auf **Fertig stellen**.

PEM-Systemzertifikate importieren

Sie können ein mit DES oder 3DES verschlüsseltes PEM-Systemzertifikat importieren.

Informationen zu diesem Vorgang

Es werden nur PEM-Schlüssel, die mit DES oder 3DES verschlüsselt wurden, unterstützt.

Gehen Sie wie folgt vor, um ein PEM-Systemzertifikat zu importieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein:

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

Schlüsselsystemzertifikate importieren

Sie können ein Schlüsselsystemzertifikat importieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Schlüsselsystemzertifikat zu importieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein:

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

Keystore-Systemzertifikate importieren

Sie können ein Keystore-Systemzertifikat in einem Hardwaresicherheitsmodul generieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein Keystore-Systemzertifikat in einem Hardwaresicherheitsmodul zu generieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein:

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

Schlüsselsystemzertifikate einchecken

Nachdem Sie das Schlüsselsystemzertifikat in einer Datei auf Ihrem lokalen Computer gespeichert haben, können Sie das Schlüsselsystemzertifikat über das **Verwaltungsmenü** einchecken.

Informationen zu diesem Vorgang

Bevor Sie beginnen, müssen Sie das Schlüsselsystemzertifikat in einer Datei auf Ihrem lokalen Computer speichern.

Gehen Sie wie folgt vor, um ein Schlüsselsystemzertifikat einzuchecken:

Vorgehensweise

1. Wählen Sie eine der folgenden Methoden aus:
   - Wenn Sie Sterling B2B Integrator verwenden, dann wählen Sie im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale Zertifikate > System** aus.
   - Wenn Sie mit der AS2 Edition arbeiten, dann wählen Sie im **AS2-Verwaltungsmenü** die Option **Zertifikate** aus.
2. Klicken Sie neben **Schlüsselzertifikat** auf **Los!**.
3. Geben Sie einen Wert für **Zertifikatsname** ein.
4. Geben Sie einen Wert für **Kennwort für privaten Schlüssel** ein. Dies ist das Kennwort, das zur Verschlüsselung des privaten Schlüssels verwendet wird.
5. Geben Sie einen Wert für **Dateiname** ein oder klicken Sie auf **Durchsuchen**, um den Dateinamen des Schlüsselzertifikats auszuwählen. Klicken Sie dann auf **Weiter**.
6. Wählen Sie die Option **Bei Verwendung validieren** aus und klicken Sie auf **Weiter**. Die folgenden Validierungsoptionen stehen zur Verfügung:

- Gültigkeit - Diese Option überprüft, ob die im Gültigkeitszeitraum des Zertifikats angegebenen Datumsangaben noch gültig sind. Wenn die Datumsangaben nicht wirksam sind, wird das Zertifikat nicht verwendet.
- Aut.-Kette - Diese Option erstellt eine Zertifikatskette für Zertifikate, die nicht selbst signiert sind. Wenn keine Zertifikatskette mit gültigen Zertifikaten erstellt werden kann, so wird das Zertifikat nicht verwendet. Wenn es sich bei dem Zertifikat um ein selbst signiertes Zertifikat handelt, wird bei Verwendung dieser Option nur die Signatur des Zertifikats überprüft.

7. Überprüfen Sie die Schlüsselzertifikatsinformationen.
8. Klicken Sie auf **Fertig stellen**.

Online Certificate Status Protocol (OCSP)

Unterstützung für OCSP in Sterling B2B Integrator

Bei OCSP (Online Certificate Status Protocol) handelt es sich um eine Gruppe von über ASN.1 definierten Datenstrukturen zum Anfordern und Empfangen von Informationen zum Zertifikatswiderrufstatus. Diese Datenstrukturen können prinzipiell von zahlreichen Transportprotokollen gesendet und empfangen werden. In der Praxis wird jedoch HTTP verwendet.

Ein OCSP-Client sendet Fragen und verarbeitet Antworten. Ein OCSP-Responder beantwortet Fragen und generiert Antworten.

OCSP-Clientfunktionalität

Eine OCSP-Clientimplementierung besteht aus Datenstrukturen zur Verwaltung von Informationen zu OCSP-Respondern, Funktionalität zum Generieren von OCSP-Anforderungen, Funktionalität zur Verarbeitung von OCSP-Antworten und Funktionalität zur Übertragung von OCSP-Anforderungen sowie zum Empfang von OCSP-Antworten.

Eine OCSP-Clientimplementierung besteht aus folgenden Komponenten:

- Datenstrukturen zur Verwaltung von Informationen zu OCSP-Respondern
- Funktionalität zum Generieren von OCSP-Anforderungen
- Funktionalität zur Verarbeitung von OCSP-Antworten
- Funktionalität zur Übertragung von OCSP-Anforderungen und zum Empfang von OCSP-Antworten

Vorgehensweise von Sterling B2B Integrator bei der OCSP-Prüfung

Eine OCSP-Prüfung für ein Zertifikat in Sterling B2B Integrator wird festgelegt, wenn die OCSP-Prüfung in Sterling B2B Integrator als Teil der internen System-APIs implementiert wurde, die von Diensten zum Abrufen von Zertifikaten und Schlüsseln aus der Datenbank verwendet werden.

Informationen zu diesem Vorgang

OCSP-Prüfungen werden von Sterling B2B Integrator ausgeführt, wenn Methoden aufgerufen werden, um Zertifikate und Schlüssel von den Objekten abzurufen, die zu deren Einbindung in der Datenbank verwendet werden.

Die folgenden Schritte erläutern, wie die OCSP-Prüfung in Sterling B2B Integrator implementiert wird:

Vorgehensweise

1. Das System überprüft das Objekt, das das Zertifikat einbindet, um festzustellen, ob die OCSP-Prüfung aktiviert wurde. Dadurch ist es für das System möglich, ohne weitere Datenbankaufrufe zu entscheiden, ob eine OCSP-Prüfung ausgeführt werden soll.
2. Wenn die OCSP-Prüfung aktiviert wird, dann erhält das System den verschlüsselten Ausstellernamen von einem Zertifikat.
3. Das System ermittelt mit SHA1 einen Hashwert für den verschlüsselten Ausstellernamen.
4. Das System versucht, einen Aussteller zu finden, der im System konfiguriert ist und einen Namen aufweist, dessen Hashwert mit dem des Zertifikats übereinstimmt.
5. Wenn kein Aussteller gefunden wird, dann wird keine Prüfung ausgeführt.
6. Wenn ein Aussteller gefunden wird, dann überprüft das System die OCSP-Richtlinie für den Aussteller. Wenn die Richtlinie OCSP-Prüfungen zulässt oder erfordert, dann finden Sie weitere Informationen in der Tabelle CERT_AUTHORITY. Das System versucht, einen OCSP-Responder für den Aussteller zu finden.
7. Wenn kein OCSP-Responder für den Aussteller gefunden wird, dann tritt eine der folgenden Situationen ein:
   - Wenn die Ausstellerrichtlinie so eingestellt ist, dass eine Prüfung immer durchgeführt wird, dann wird eine Ausnahmebedingung ausgelöst und die Prüfung schlägt fehl.
   - Wenn die Ausstellerrichtlinie so eingestellt ist, dass die Prüfung nur dann ausgeführt wird, wenn ein Responder konfiguriert wurde, dann wird die Prüfung nicht ausgeführt.
   - Wenn ein OCSP-Responder für den Aussteller gefunden wird, dann wird eine OCSP-Prüfung ausgeführt.

Datenbanktabellen

Die Datenbanktabellen CERT_AUTHORITY und OCSP_RESPONDER werden hinzugefügt, um zugehörige OCSP-Informationen zu verwalten.

Zur Verwaltung von OCSP-Informationen wurden zwei neue Datenbanktabellen zum Produkt hinzugefügt:

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

Die Tabelle CERT_AUTHORITY enthält Informationen zu Zertifizierungsstellen.

Spalte	Typ	Beschreibung
OBJECT_ID	VARCHAR (255)	Diese GUID (global eindeutige ID) stellt eine eindeutige ID für einen Datensatz dar. Dies ist der Primärschlüssel. Der Wert darf nicht null sein.
NAME	VARCHAR (255)	Ein Name für einen Datensatz. Der Wert null ist zulässig.
CREATE_DATE	DATETIME	Ein Erstellungsdatum für einen Datensatz.
MODIFIED_DATE	DATETIME	Das Datum der letzten Änderung eines Datensatzes.

Spalte	Typ	Beschreibung
MODIFIED_BY	VARCHAR(255)	Informationen zu dem Benutzer, der einen Datensatz geändert hat.
ISSUER_NAME	BLOB	Der RDN (relativ definierter Name) des Ausstellers, der dem zugehörigen Zertifikat entnommen wurde.
HASH_ALG	VARCHAR(128)	Der Hashalgorithmus, der zur Ermittlung des Hashwerts für Name und Schlüssel verwendet wurde. Nur SHA1 wird unterstützt.
RDN_HASH	VARCHAR(255)	Mit BASE64 verschlüsselter SHA1-Hashwert des mit DER codierten RDN des Ausstellers, der dem Zertifikat des Ausstellers entnommen wurde. Diese Spalte ist indexiert.
KEY_HASH	VARCHAR(255)	Mit BASE64 verschlüsselter SHA1-Hashwert des verschlüsselten öffentlichen Schlüssels im Zertifikat des Ausstellers.
CERT_OID	VARCHAR(255)	Die Objekt-ID (OBJECT_ID) des Zertifikats des Ausstellers in der Tabelle CA_CERT_INFO. Jeder Aussteller muss über ein CA-Zertifikat verfügen, das in der Datenbank gespeichert ist. Der Wert null ist nicht zulässig.
OCSP_POLICY	VARCHAR(128)	Die OCSP-Richtlinie für den Aussteller. Dieses Element besteht aus zwei durch Kommas getrennte Werte. Die Werte legen fest, wann OCSP verwendet werden sollte und welche Daten zu überprüfen sind. Folgende Werte sind möglich: **OCSP_When** • Niemals - OCSP niemals verwenden. • Resp – OCSP nur verwenden, wenn ein Responder konfiguriert ist, wenn eine Anforderung abgesetzt wird. • Immer - OCSP immer verwenden, wenn eine Anforderung abgesetzt wird. Dazu muss ein Responder konfiguriert sein. Wenn kein Responder konfiguriert ist, dann schlägt die Zertifikatsüberprüfung fehl. **OCSP_What** • Ohne - Zertifikate werden niemals überprüft. • Endbenutzer - Nur Endbenutzerzertifikate werden überprüft. • Beide - Sowohl Endbenutzer- als auch Zwischenzertifikate werden überprüft. Diese Option wird momentan nicht unterstützt. • Der Wert null ist in dieser Spalte nicht zulässig.
CRL_POLICY	VARCHAR(128)	Wird momentan nicht verwendet.

OCSP_RESPONDER

Die Tabelle OCSP_RESPONDER enthält Informationen über OCSP-Responder.

Spalte	Typ	Beschreibung
OBJECT_ID	VARCHAR (255)	Diese GUID (global eindeutige ID) stellt eine eindeutige ID für einen Datensatz dar. Dies ist der Primärschlüssel. Der Wert darf nicht null sein.
NAME	VARCHAR (255)	Ein Name für einen Datensatz. Der Wert null ist zulässig.
CREATE_DATE	DATETIME	Ein Erstellungsdatum für einen Datensatz.
MODIFIED_DATE	DATETIME	Das Datum der letzten Änderung eines Datensatzes.
MODIFIED_BY	VARCHAR(255)	Informationen zu dem Benutzer, der einen Datensatz geändert hat.
ISSUER_NAME	BLOB	Der RDN (relativ definierter Name) des Ausstellers, der dem zugehörigen Zertifikat entnommen wurde.
HASH_ALG	VARCHAR(128)	Der Hashalgorithmus, der zur Ermittlung des Hashwerts für Name und Schlüssel verwendet wurde. Nur SHA1 wird unterstützt.
RDN_HASH	VARCHAR(255)	Mit BASE64 verschlüsselter SHA1-Hashwert des mit DER codierten RDN des Ausstellers, der dem Zertifikat des Ausstellers entnommen wurde. Diese Spalte ist indexiert.
KEY_HASH	VARCHAR(255)	Mit BASE64 verschlüsselter SHA1-Hashwert des verschlüsselten öffentlichen Schlüssels im Zertifikat des Ausstellers.
CERT_OID	VARCHAR(255)	Die Objekt-ID (OBJECT_ID) des Zertifikats des Ausstellers in der Tabelle CA_CERT_INFO. Jeder Aussteller muss über ein CA-Zertifikat verfügen, das in der Datenbank gespeichert ist. Der Wert null ist nicht zulässig.
CACHE_TTL	VARCHAR(64)	Die Zeitdauer in Sekunden, die OCSP-Antworten im internen Antwortcache verbleiben dürfen. Wenn für die Spalte NULL angegeben ist, dann werden OCSP-Antworten lediglich für eine (1) Sekunde gespeichert, was in der Praxis gleichbedeutend mit der Nicht-Speicherung ist.
TRANS_PROF_OID	VARCHAR(255)	Die Objekt-ID (OBJECT_ID) eines Profils in der GIS-Datenbank. Sie müssen ein Profil für den OCSP-Responder erstellen, das die korrekte URL für den Responder enthält.

Spalte	Typ	Beschreibung
COMM_BP	VARCHAR(255)	Der Name eines Geschäftsprozesses, der zur Kommunikation mit dem OCSP-Responder verwendet wird. Hierbei muss es sich um einen Geschäftsprozess handeln, über den die HTTP-Kommunikation ausgeführt werden kann. Dienste im Geschäftsprozess müssen so konfiguriert werden, dass keine HTTP-Header erforderlich sind bzw. angezeigt werden, wenn Nachrichten gesendet oder empfangen werden. Der Prozess HTTPClientSend, der zum Lieferumfang des Systems gehört, kann verwendet werden und wird empfohlen.
COMM_WAIT	VARCHAR(24)	Die Anzahl der Sekunden, die auf die Kommunikation mit dem OCSP-Responder gewartet wird, bevor ein Fehler angenommen wird.

OCSP-Konfiguration

Sie können eine unbegrenzte Anzahl von Ausstellern und Respondern erstellen, wenn Sie das System für die Verwendung von OCSP konfigurieren.

Informationen zu diesem Vorgang

Wenn Sie das System konfigurieren, dann können Sie eine beliebige Anzahl von Ausstellern und Respondern erstellen.

Gehen Sie wie folgt vor, um das System zur Verwendung von OCSP zu konfigurieren:

Vorgehensweise

1. Überprüfen Sie das Zertifikat für die Zertifizierungsstelle, die die Zertifikate ausgibt, die mit OCSP in Sterling B2B Integrator eingecheckt werden sollen, um zu überprüfen, ob es sich bei dem Zertifikat um ein CA-Zertifikat handelt.
2. Listen Sie die CA-Zertifikate im System auf und rufen Sie die Objekt-ID für das Zertifikat auf, das Sie soeben installiert haben.
3. Wenn das OCSP-Antwortsignaturzertifikat des Ausstellers sich vom Zertifikatausstellungszertifikat des Ausstellers unterscheidet, dann checken Sie das OCSP-Antwortsignaturzertifikat des Ausstellers als vertrauenswürdiges Zertifikat in Sterling B2B Integrator ein.

   Anmerkung: Ab Version 5.2.4.2 können Sie das Stammzertifikat einchecken, welches das Responderzertifikat als CA-Zertifikat und nicht als vertrauenswürdiges Zertifikat ausgestellt hat. Da das Responderzertifikat je nach CA häufig geändert wird, kann es ein Fehlschlagen von OCSP verursachen, bis das Zertifikat durch ein gültiges Zertifikat ersetzt wird. Sie sollten in Zukunft immer ein Stammzertifikat einchecken, da diese selten geändert werden. Beide Typen sind jedoch weiterhin zulässig.
4. Wenn Sie ein zusätzliches OCSP-Signaturzertifikat eingecheckt haben, dann listen Sie die CA-Zertifikate im System auf und rufen Sie die Objekt-ID für das Zertifikat ab, das Sie soeben installiert haben.
5. Wechseln Sie in das Verzeichnis 'bin' der Sterling B2B Integrator-Installation.
6. Starten Sie die Datenbank, sofern dies erforderlich ist.

7. Starten Sie die Bash- oder die Bourne-Shell.
8. Verwenden Sie die Datei 'tmp.sh' als Quelle.
9. Erstellen Sie mit dem Dienstprogramm in der Klasse 'com.sterlingcommerce.security.ocsp.SCICertAuthority' einen Aussteller.
10. Erstellen Sie mit dem Dienstprogramm in der Klasse 'com.sterlingcommerce.security.ocsp.SCIOCSPResponder' einen OCSP-Responder.
11. Aktualisieren Sie die Zertifikate für den Aussteller oder einzelne Zertifikate zum Aktivieren von OCSP. Das Dienstprogramm 'com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo' konfiguriert alle vertrauenswürdigen Zertifikate und Systemzertifikate für einen Aussteller. Das Dienstprogramm 'com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo' konfiguriert ein (1) Systemzertifikat. Das Dienstprogramm 'com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo' konfiguriert ein (1) vertrauenswürdiges Zertifikat.

OCSP-Konfigurationsscripts

Die folgenden Scripts wurden in den OCSP-Hotfix zur Ausführung der OCSP-Konfigurationsdienstprogramme eingebunden. Für jedes Script steht eine UNIX/Linux- und eine Windows-Version zur Verfügung. Die Scripts akzeptieren die gleichen Befehlszeilenargumente wie die Dienstprogramme, die von ihnen aufgerufen werden. Die Scripts sind im Verzeichnis 'bin' der Produktinstallation gespeichert. Die Informationen zu den Befehlszeilenargumenten werden im vorliegenden Abschnitt zur Beschreibung der Scripts lediglich wiederholt.

ManageCertAuthority.sh und ManageCertAuthority.cmd

Argument	Beschreibung
-a, -l, -d	Auszuführende Operation: -a add (Hinzufügen) -l list (Auflisten) -d delete (Löschen) Die Option –l hat keine weiteren Argumente. Die Option –d hat ein einziges Argument: Die Objekt-ID des zu löschenden Datensatzes.
Name	Der Name des Ausstellers. Erforderlich mit -a.
Modified_by	Der Benutzer, der die Identität geändert oder erstellt hat. Erforderlich mit –a.
Hash_alg	Der Hashalgorithmus für den Aussteller. Nur der Wert 'SHA1' wird unterstützt. Erforderlich mit –a.
Certificate_id	Die Objekt-ID des CA-Zertifikats, das dem Aussteller zugeordnet ist. Erforderlich mit –a.

OCSP_policy	Die OCSP-Richtlinienzeichenfolge für den Aussteller. Hierbei handelt es sich um eine durch Kommas begrenzte Zeichenfolge, die im Abschnitt zur Tabelle CERT_AUTHORITY beschrieben wird. Erforderlich mit –a. Für das erste Element der Zeichenfolge sind folgende Werte zulässig: • Niemals - OCSP niemals verwenden. • Resp – OCSP nur verwenden, wenn ein Responder konfiguriert ist, wenn eine Anforderung abgesetzt wird. • Immer - OCSP immer verwenden, wenn eine Anforderung abgesetzt wird. Dazu muss ein Responder konfiguriert sein. Wenn kein Responder konfiguriert ist, dann schlägt die Zertifikatsüberprüfung fehl. Für das zweite Element der Zeichenfolge sind folgende Werte zulässig: **OCSP What** • Ohne - Zertifikate werden niemals überprüft. • Endbenutzer - Nur Endbenutzerzertifikate werden überprüft. • Beide - Sowohl Endbenutzer- als auch Zwischenzertifikate werden überprüft. Wird gegenwärtig nicht unterstützt. Beispiele: • Niemals,Ohne • Immer,Endbenutzer
Crl_policy	Die CRL-Richtlinienzeichenfolge für den Aussteller. Erforderlich mit –a. Ein Wert für dieses Argument ist erforderlich, es wird jedoch momentan nicht verwendet. 'Ohne' wird akzeptiert.
Object_ID	Eine Objekt-ID, die beim Erstellen dieses Datensatzes verwendet wird. Optional mit -a.

ManageOCSPResponder.sh und ManageOCSPResponder.cmd

Argument	Beschreibung
-l	Ruft eine Liste der momentan konfigurierten OCSP-Responder ab. Diese Option hat keine weiteren Argumente.

-d	Löscht den konfigurierten OCSP-Responder mit der angegebenen Objekt-ID für die Responderkonfigurationsdaten. Diese Option hat object_id als zusätzliches Argument.
-u2	Aktualisiert vorhandene Datensätze in der Datenbank mit den korrekten Informationen zum öffentlichen Schlüssel des CA-Zertifikats und zum registrierten Namen des Zertifikatsinhabers des CA-Zertifikats. Dieses Argument muss für alle vorhandenen Datensätze für die Zertifizierungsstelle und die OCSP-Responder ausgeführt werden. Andernfalls müssen Sie die Datensätze löschen und erneut erstellen, um die korrekten Informationen in der Datenbank zu speichern. Diese Option hat object_id als zusätzliches Argument.
-a	Fügt Konfigurationsdaten für einen neuen OCSP-Responder hinzu, die zum Überprüfen des Status von Zertifikaten verwendet werden, die vom angegebenen Aussteller ausgegeben wurden. Die zusätzlichen Argumente lauten wie folgt: 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 und object_id.
name	(Erforderlich mit -a) Der Name des Ausstellers.
modified_by	(Erforderlich mit -a) Der Benutzer, der die Identität geändert oder erstellt hat.
hash_alg	(Erforderlich mit -a) Der Hashalgorithmus für den Aussteller. Nur der Wert 'SHA1' wird unterstützt.
authority_cert_oid	(Erforderlich mit -a) Die Objekt-ID des CA-Zertifikats, das dem Aussteller zugeordnet ist.
response_signing_cert_oid	(Erforderlich mit -a) Die Objekt-ID des Zertifikats, das vom Provider der OCSP-Dienste zum Signieren der Antwort mit dem Status für die Zertifikate verwendet wurde. Dieses Zertifikat muss zum Speicher für digitale CA-Zertifikate oder zum Speicher für vertrauenswürdige digitale Zertifikate hinzugefügt werden. Hierbei handelt es sich um die Systemzertifikat-ID für das Zertifikat in dem im Speicher aufgeführten Format.

resp_signing_cert_in_ca_store	(Erforderlich mit -a) Dieses Flag gibt an, ob der vorherige Wert für das Argument 'response_signing_cert_oid' im Speicher für digitale CA-Zertifikate in Sterling B2B Integrator gefunden wurde.
cache_ttl	(Erforderlich mit -a) Die Lebensdauer in Sekunden für OCSP-Antworten im internen Cache.
trans_prof_oid	(Erforderlich mit -a) Die Objekt-ID für einen Transport, der zur Kommunikation mit dem OCSP-Responder konfiguriert wurde.
comm_bp	(Erforderlich mit -a) Der Name eines Geschäftsprozesses, der zur Kommunikation mit dem OCSP-Responder verwendet wird. Hierbei muss es sich um einen Geschäftsprozess handeln, über den die HTTP-Kommunikation ausgeführt werden kann. Dienste im Geschäftsprozess müssen so konfiguriert werden, dass keine HTTP-Header erforderlich sind bzw. angezeigt werden, wenn Nachrichten gesendet oder empfangen werden. Der Prozess HTTPClientSend, der zum Lieferumfang des Systems gehört, kann verwendet werden und wird empfohlen.
comm_wait	(Erforderlich mit -a) Die Anzahl der Sekunden, die auf die Kommunikation mit dem Responder gewartet wird, bevor ein Fehler angenommen wird.
send_nonce	(Erforderlich mit -a) Gibt an, ob ein NONCE-Wert an den OCSP-Dienst gesendet wird. Der NONCE-Wert wird verwendet, um Attacken durch Nachrichtenaufzeichnung und -wiederholung von bestimmten OCSP-Providern zu verhindern.
require_nonce	(Erforderlich mit -a) Gibt an, ob der Server anfordern soll, dass der OCSP-Dienst einen NONCE-Wert in der Antwort angibt.
object_id	(Optional mit -a) Eine Objekt-ID, die beim Erstellen dieses Datensatzes verwendet wird.

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

Dieses Dienstprogramm dient zum Definieren der OCSP-Informationen in der Datenbank für ein einzelnes Systemzertifikat.

Argument	**Beschreibung**
-o, -n	Gibt an, wie das zweite Argument interpretiert werden soll: -o object_ID -n name
Object_ID/Name	Die Objekt-ID oder der Name des Ausstellers, der in Argument 1 angegeben wurde.

SetSystemCertOCSPInfo.sh und SetTrustedCertOCSPInfo.cmd

Dieses Dienstprogramm dient zum Definieren der OCSP-Informationen in der Datenbank für ein einzelnes Systemzertifikat.

Argument	Beschreibung
-o, -n	Gibt an, wie das zweite Argument interpretiert werden soll: -o object_ID -n name
Object_ID/Name	Die Objekt-ID oder der Name des Ausstellers, der in Argument 1 angegeben wurde.

OCSP-Script ausführen

Im folgenden Beispiel wird die Vorgehensweise zum Ausführen der OCSP-Konfigurationscripts dargestellt. Diese Scripts gehen davon aus, dass Sie bereits die CA-Zertifikate für den Aussteller eingecheckt, die Datenbank gestartet, das Verzeichnis 'bin' in Ihrer Sterling B2B Integrator-Installation aufgerufen und die Datei 'tmp.sh' im Verzeichnis 'bin' als Quelle angegeben haben.

Informationen zu diesem Vorgang

Nach Abruf der Objekt-ID des CA-Zertifikats vom Aussteller wählen Sie in Sterling B2B Integrator im **Verwaltungsmenü** die Optionen **Handelspartner > Digitale CA-Zertifikate** aus. Wählen Sie ein Zertifikat aus. Daraufhin wird das Dialogfeld 'Zertifikatzusammenfassung' aufgerufen, in dem die Zertifikatsinformationen einschließlich der Objekt-ID angegeben sind.

Führen Sie zur Ausführung eines OCSP-Scripts die folgenden Schritte aus. Eine vollständige Liste der OCSP-Scriptbefehle finden Sie unter „OCSP-Konfigurationsscripts” auf Seite 89.

Vorgehensweise

1. Führen Sie den folgenden Befehl aus, um auf dem System einen Aussteller zu erstellen:

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

2. Nach Erstellung eines Ausstellers und eines Profils für die Kommunikation mit einem OCSP-Responder müssen Sie den folgenden Befehl ausführen, um einen OCSP-Responder auf dem System zu erstellen:

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

3. Führen Sie den folgenden Befehl aus, um alle auf dem System verfügbaren Aussteller aufzulisten:

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

   Daraufhin wird die Ausgabe für jeden Aussteller zurückgegeben:

   ```
   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. Verwenden Sie den folgenden Befehl, um OCSP für alle vertrauenswürdigen Zertifikate und Systemzertifikate zu aktivieren, die von dem Aussteller ausgegeben wurden:

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

OCSP-Prüflogik

In den folgenden Schritten wird die Logik der OCSP-Prüfung in Sterling B2B Integrator beschrieben. Wenn der Zertifikatstatus OK ist, dann kann die OCSP-Prüfung erfolgreich ausgeführt werden. Andernfalls schlägt die Prüfung fehl.

Vorgehensweise

1. Wenn eine vorhandene Antwort gefunden wird, deren Lebensdauer noch nicht abgelaufen ist, wird diese Antwort als OCSP-Antwort verwendet.
2. Wenn keine Antwort im Cache gefunden wird oder die Lebensdauer der Antwort im Cache bereits abgelaufen ist, wird eine OCSP-Anforderung erstellt.
3. Wenn das System eine OCSP-Anforderung erstellt, dann startet es den Geschäftsprozess, der für den OCSP-Responder zum Senden der Anforderung und Abrufen der Antwort konfiguriert ist. Anforderungen umfassen einen Nonce-Wert, wenn der Responder so konfiguriert wurde, dass ein solcher Wert gesendet wird.
4. Wenn der Geschäftsprozess erfolgreich abgeschlossen wird, dann versucht das System, das Primärdokument als OCSP-Antwort zu analysieren. Der zum Senden von OCSP-Anforderungen und zum Empfangen von OCSP-Antworten verwendete Geschäftsprozess entfernt die HTTP-Header aus der Antwort.
5. Wenn das Primärdokument als OCSP-Antwort analysiert werden kann, dann überprüft das System den Status der Antwort.
6. Wenn der Antwortstatus angibt, dass die Anforderung eine gültige Antwort generiert hat, dann versucht das System, die Signatur auf der OCSP-Antwort mithilfe des Zertifikats zu überprüfen, das für den OCSP-Responder konfiguriert wurde.
7. Wenn die Signatur überprüft und der Responder so konfiguriert wurde, dass ein Nonce-Wert erforderlich ist, versucht das System, den Nonce-Wert aus der Antwort abzurufen und zu überprüfen.
8. Wenn alle anderen Prüfoperationen erfolgreich durchlaufen wurden, dann sucht das System nach Zertifikatsstatusinformationen für das Zertifikat, für das die Anforderung erstellt und gesendet wurde.
9. Wenn die Statusinformationen gefunden werden, dann aktualisiert das System den internen Cache für eine vorhandene OCSP-Antwort für das Zertifikat.

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) 140-2

Um den Sicherheitsanforderungen von FIPS 200 zu entsprechen, müssen Anwendungen Verschlüsselungsmodule verwenden, die gemäß CMVP (Cryptographic Module Validation Program) zertifiziert wurden und die den Vorgaben von FIPS 140-1 oder 140-2 entsprechen.

Die Mindestanforderungen für die Verwendung einer validierten Verschlüsselung von Anwendungen lauten wie folgt:

- Alle Verschlüsselungsoperationen einschließlich der Schlüsselerstellung müssen von validierten Verschlüsselungsmodulen ausgeführt werden.
- Nur genehmigte Sicherheitsfunktionen sind zulässig.
- Nur genehmigte Schlüsseleinrichtungsverfahren sind zulässig.

FIPS 140-2 mit Sterling B2B Integrator

Bei Certicom Government Service Edition (GSE) handelt es sich um ein gemäß FIPS 140-2 Level 1 zertifiziertes Verschlüsselungsmodul, das zusammen mit Sterling B2B Integrator ausgeliefert wird. GSE ist ein Low-Level-Verschlüsselungstoolkit, das in Java geschrieben ist und verschiedene Sicherheitsfunktionen implementiert, zu denen auch nicht genehmigte Sicherheitsfunktionen gehören.

Wenn sich das System im FIPS-Modus befindet, dann werden die folgenden Tasks ausgeführt:

- Aktivieren der GSE FIPS-Zustandsmaschine und Aufrufen des POST (Power-on Self Test).
- Weiterleiten von Verschlüsselungsfunktionsaufrufen vom Kernsystem zu GSE über eine entsprechende Trichterfunktion.

FIPS während der Installation aktivieren

Während einer neuen Installation müssen Sie, wenn Sie aufgefordert werden anzugeben, ob Sie das System im FIPS-Modus (FIPS = Federal Information Processing Standard) ausführen wollen, die Einstellung TRUE auswählen.

FIPS-Modus manuell aktivieren

Sie können den FIPS-Modus (FIPS = Federal Information Processing Standard) manuell aktivieren, nachdem Sie Sterling B2B Integrator installiert haben. Bevor Sie beginnen, sollten Sie überprüfen, ob Sie über eine Lizenz zum Arbeiten im FIPS-Modus verfügen. Erst dann können Sie diesen Modus aktivieren. Das System überprüft Ihre Lizenz beim Start und führt den Start nicht aus, wenn der FIPS-Modus aktiviert wurde, jedoch keine Lizenz zur Benutzung dieses Modus vorhanden ist.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um den FIPS-Modus manuell zu aktivieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/properties/'.
2. Suchen Sie die Datei 'security.properties'.
3. Öffnen Sie die Datei 'security.properties' in einem Texteditor. Wenn Sie Änderungen an der Datei 'security.properties' durchführen, dann müssen Sie sich

vergewissern, dass auch an der Datei 'security.properties.in' die gleichen Änderungen vorgenommen wurden. Dadurch wird verhindert, dass die angepassten Einstellungen überschrieben werden. Sie sollten zum Anpassen von FIPS die Sicherheitseigenschaftendatei verwenden, anstatt die Eigenschaftendateien direkt zu bearbeiten.

4. Geben Sie die folgende Konfigurationseinstellung an: FIPSMode=true
5. Speichern und schließen Sie die Datei 'security.properties'.
6. Starten Sie Sterling B2B Integrator erneut. Dies ist erforderlich, damit die Änderungen vom System erkannt werden können.

FIPS-Modus inaktivieren

Sie können den FIPS-Modus manuell inaktivieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um den FIPS-Modus (FIPS = Federal Information Processing Standard) manuell zu inaktivieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/properties/'.
2. Suchen Sie die Datei 'security.properties'.
3. Öffnen Sie die Datei 'security.properties' in einem Texteditor.
4. Geben Sie die folgende Konfigurationseinstellung an: FIPSMode=false
5. Speichern und schließen Sie die Datei 'security.properties'.
6. Starten Sie Sterling B2B Integrator erneut. Dies ist erforderlich, damit die Änderungen vom System erkannt werden können.

Proxy-Server

Proxy-Server

Proxy-Server verbessern die Sicherheit Ihres Systems.

HTTP-Proxy-Server konfigurieren

Einen HTTP-Proxy-Server können Sie über das **Verwaltungsmenü** konfigurieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um einen HTTP-Proxy-Server zu konfigurieren:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Operationen** > **Proxy-Server** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Name** den Namen des Proxy-Servers ein.
4. Wählen Sie als **Typ** des Servers **HTTP** aus.
5. Geben Sie im Feld **Host** den Hostnamen ein. IPv6-Adressen sollten in eckige Klammern eingeschlossen werden.
6. Geben Sie die Nummer für den **Port** ein.
7. Geben Sie einen Wert für **Wiederholungszählung** ein.
8. Klicken Sie auf **Weiter**.

9. Gehen Sie wie folgt vor, um die Basisauthentifizierung für den Benutzer als erforderlich zu definieren:
   - Wählen Sie **Ja** aus und klicken Sie dann auf **Weiter**.
   - Wenn Sie 'Nein' (Standardwert) angeben, dann klicken Sie auf **Weiter** und fahren Sie mit Schritt 13 fort.
10. Geben Sie einen Wert für **Benutzer-ID für Authentifizierung** ein.
11. Geben Sie das **Kennwort für Authentifizierung** ein.
12. Klicken Sie auf **Weiter**.
13. Überprüfen Sie die Einstellungen für den Proxy-Server.
14. Klicken Sie auf **Fertig stellen**.

SSP-Proxy-Server konfigurieren

Einen SSP-Proxy-Server können Sie über das **Verwaltungsmenü** konfigurieren.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um einen SSP-Proxy-Server zu konfigurieren:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Operationen** > **Proxy-Server** aus.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie im Feld **Name** den Namen des Proxy-Servers ein.
4. Wählen Sie als **Typ** des Servers **SSP** aus.
5. Geben Sie im Feld **Host** den Hostnamen ein. IPv6-Adressen sollten in eckige Klammern eingeschlossen werden.
6. Geben Sie die Nummer für den **Port** ein.
7. Geben Sie einen Wert für **Wiederholungszählung** ein.
8. Klicken Sie auf **Weiter**.
9. Wenn für den Benutzer die Basisauthentifizierung erforderlich ist, dann wählen Sie 'Ja' oder 'Nein' aus.
10. Wenn SSL erforderlich ist, dann wählen Sie 'Ja' oder 'Nein' aus.
11. Klicken Sie auf **Weiter**.
12. Wenn Sie für den aktuellen Benutzer die Basisauthentifizierung ausgewählt haben, dann müssen Sie die **Benutzer-ID für Authentifizierung** und das **Kennwort für Authentifizierung** auswählen und dann auf **Weiter** klicken. Wenn Sie diese Authentifizierung nicht benötigen, wird diese Seite nicht angezeigt.
13. Wenn Sie für 'SSL erforderlich?' die Einstellung 'Ja' auswählen, dann müssen Sie auch **Verschlüsselungsstärke**, **CA-Zertifikate** und **Schlüsselzertifikate** auswählen und dann auf **Weiter** klicken. Wenn SSL nicht erforderlich ist, wird diese Seite nicht angezeigt.
14. Klicken Sie auf **Weiter**.
15. Überprüfen Sie die Einstellungen für den Proxy-Server.
16. Klicken Sie auf **Fertig stellen**.

Proxy-Server für SSL konfigurieren

Sie können SSL mit Ihrer SSP-Proxy-Server-Konfiguration verwenden, indem Sie ein SSL-Zertifikat erstellen oder importieren und für **SSL verwenden** in der entsprechenden Adapterkonfiguration die Einstellung **Muss** festlegen.

Informationen zu diesem Vorgang

Wenn Sie sich für die Verwendung von SSL in Ihrer SSP-Proxy-Server-Konfiguration entscheiden, dann müssen Sie die folgenden Arbeitsschritte ausführen:

Vorgehensweise

1. Erstellen eines SSL-Zertifikats oder Importieren des Zertifikats aus der Zertifizierungsstelle in Sterling B2B Integrator.
2. Festlegen der Einstellung **Muss** im Feld **SSL verwenden** der entsprechenden Adapterkonfiguration.

Proxy-Server bearbeiten

Eine Proxy-Server-Konfiguration können Sie über das **Verwaltungsmenü** bearbeiten.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um eine Proxy-Server-Konfiguration zu bearbeiten:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Operationen** > **Proxy-Server** aus.
2. Klicken Sie für den zu bearbeitenden Proxy-Server auf **Bearbeiten**.
3. Aktualisieren Sie die Felder entsprechend Ihren Anforderungen.
4. Klicken Sie auf **Weiter**.
5. Überprüfen Sie die Einstellungen für den Proxy-Server.
6. Klicken Sie auf **Fertig stellen**.

Proxy-Server löschen

Informationen zu diesem Vorgang

Das Löschen einer Proxy-Server-Konfiguration kann zu Fehlern bei bestimmten Funktionen von Sterling B2B Integrator führen. Bestimmte Adapter und Dienste müssen eventuell erneut konfiguriert werden, um den ordnungsgemäßen Betrieb ohne die gelöschte Proxy-Server-Konfiguration zu gewährleisten.

Gehen Sie wie folgt vor, um eine Proxy-Server-Konfiguration zu löschen:

Vorgehensweise

1. Wählen Sie im **Verwaltungsmenü** die Optionen **Operationen** > **Proxy-Server** aus.
2. Klicken Sie für den zu bearbeitenden Proxy-Server auf **Löschen**.
3. Überprüfen Sie die Einstellungen für den Proxy-Server.
4. Klicken Sie auf **Löschen**.

SSL

Informationen zur Implementierung von SSL in Sterling B2B Integrator

Secure Sockets Layer (SSL) ist ein Protokoll, das die sichere Kommunikation über das Internet ermöglicht. Es verwendet sowohl die symmetrische als auch die asymmetrische Verschlüsselung.

Das SSL-Sicherheitsprotokoll stellt die Serverauthentifizierung und die Clientauthentifizierung in Sterling B2B Integrator zur Verfügung:

- Die Serverauthentifizierung wird ausgeführt, wenn ein Client eine Verbindung zum Server herstellt. Nach dem Ausgangshandshake sendet der Server sein digitales Zertifikat an den Client. Der Client überprüft das Serverzertifikat oder die entsprechende Zertifikatskette.
- Die Clientauthentifizierung wird ausgeführt, wenn ein Server während des Handshakes eine Zertifikatsanforderung an einen Client sendet. Wenn das Clientzertifikat oder die entsprechende Zertifikatskette überprüft wird und die Zertifikatsüberprüfungsnachricht verifiziert wird, dann wird das Handshake fortgesetzt.
- Die optionale zusätzliche Authentifizierung wird durch Überprüfung des allgemeinen Namens im Zertifikat anhand des vollständig qualifizierten Domänennamens des Servers aus einem DNS-Umkehrverzeichnis (Reverse Domain Name Server Lookup) durchgeführt, aus dem der vollständig qualifizierte Domänenname des Servers abgerufen werden kann.

Typen der Vertrauenswürdigkeit

Für SSL-Zertifikate werden zwei Typen der Vertrauenswürdigkeit in Sterling B2B Integrator unterstützt:

- CA Trust – Eine hierarchische Vertrauensstruktur auf der Basis eines Stammzertifikats, das zum Ausstellen anderer Zertifikate verwendet wird. Dies ist das Standard-Trust-Modell für SSL-Zertifikate.
- Direkte Vertrauensstellung - Die direkte Vertrauensstellung selbst signierter Zertifikate, bei denen eine Verteilung über sichere externe Mechanismen angenommen wird. Die direkte Vertrauensstellung und die selbst signierten Zertifikate sind nicht Teil des SSL-Standards, werden jedoch häufig in bestimmten Handelsgemeinschaften verwendet.

SSL-Zertifikate

Um über SSL zu kommunizieren, müssen Sie die teilnehmenden Systeme zur Unterstützung der Serverauthentifizierung oder der Client/Serverauthentifizierung konfigurieren. Um die Authentifizierung über einen Server auszuführen, benötigen Sie ein Zertifikat einer Rootzertifizierungsstelle (CA) und die Gruppe der Zwischenzertifikate in der Kette oder (wenn der Server ein selbst signiertes Zertifikat verwendet) eine Kopie des selbst signierten Zertifikats.

Zur Unterstützung der Client/Serverauthentifizierung benötigen Sie ein CA-Zertifikat oder ein selbst signiertes Zertifikat sowie ein Systemzertifikat.

Sie können ein SSL-Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle anfordern, indem Sie eine CSR (Certificate Signing Request; Zertifikatssignieranfor-

derung) für die Zertifizierungsstelle bereitstellen. Das SSL-Zertifikat bindet den öffentlichen Schlüssel und den SSL-Server oder -Client.

Wenn Sie die Client/Serverauthentifizierung verwenden möchten, dann konfigurieren Sie ein Systemzertifikat. Sie können Systemzertifikate auf die folgenden Arten erstellen:

- Einchecken einer vorhandenen Schlüsselzertifikatsdatei oder PKCS12-Datei.
- Generieren eines selbst signierten Systemzertifikats.
- Verwenden von Key Management Utility (iKeyman) zum Generieren einer CSR und Abrufen eines Zertifikats von der Zertifizierungsstelle. Informationen zu iKeyman finden Sie in „IBM Key Management Utility (iKeyman)" auf Seite 66.

Cipher-Suites

Bevor Sie Sterling B2B Integrator verwenden, sollten Sie die verfügbaren, vordefinierten Cipher-Listen prüfen und diese entsprechend den Sicherheitsanforderungen Ihres Unternehmens anpassen.

Die Cipher-Suites von IBM SDK, Java Technology Edition, Version 7 finden Sie hier: http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html. Für andere unterstützte JDKs in Sterling B2B Integrator finden Sie in der Dokumentation des JDK-Herstellers entsprechende Listen der unterstützten Cipher-Suites.

Cipher-Stärken werden in `security.properties` or in `customer_overrides.properties` konfiguriert. Die Stufeen der verfügbaren Cipher-Suites sind:

- AllCipherSuite (UI-Auswahl ist **ALL**) - umfasst alles, was in WEAK und STRONG aufgelistet ist.
- WeakCipherSuite (UI-Auswahl ist **WEAK**) - Fügen Sie unterstützte schwache Cipher-Suites hinzu, die Sie mit Sterling B2B Integrator verwenden wollen
- StrongCipherSuite (UI-Auswahl ist **STRONG**) - Fügen Sie unterstützte starke Cipher-Suites hinzu, die Sie mit Sterling B2B Integrator verwenden wollen
- CipherSuiteDefault (verfügbar in V5.2.6 und höher) - Standardeinstellung; umfasst eine Untermenge an unterstützten Verschlüsselungscodes für IBM JDK7. Wird verwendet, wenn WeakCipherSuite und StrongCipherSuite leer sind.

Clientadapter für SSL

FTP-Clientadapter, HTTP-Clientadapter und Sterling Connect:Direct FTP+ Requester Adapter (mit Secure+-Option) bieten Unterstützung für SSL.

Die folgenden Clientadapter bieten Unterstützung für SSL (Secure Sockets Layer):

- FTP-Clientadapter
- HTTP-Clientadapter
- Sterling Connect:Direct FTP+ Requester Adapter (mit Secure+-Option)

Parameter für SSL können im Profil des Handelspartners oder für den Adapter gesetzt werden. Für den FTP-Clientadapter werden diese Parameter im Dienst für den FTP-Client-Sitzungsbeginn gesetzt. Für den HTTP-Clientadapter werden diese Parameter im Dienst für den HTTP-Client-Sitzungsbeginn gesetzt. Parameter, die im Dienst für den Sitzungsbeginn gesetzt werden, überschreiben Einstellungen in einem Handelspartnerprofil.

Die Parameter in der folgenden Tabelle steuern SSL aus der Clientperspektive. Weitere Informationen hierzu finden Sie in der Dokumentation zu dem jeweiligen Adapter oder Dienst, der von Ihnen konfiguriert wird.

Parameter	Beschreibung
SSL	Legt die SSL-Socketvereinbarung fest.
CACertificateId (CA-Zertifikats-ID) (trusted_root)	Liste der vertrauenswürdigen CA-Zertifikate einer öffentlichen Zertifizierungsstelle. In den Prozessdaten wird dieser Parameter als Objekt-ID angezeigt.
CipherStrength	Die Stufe der Verschlüsselung, die auf die Daten angewendet werden soll, die über die Socketverbindung übertragen werden.
SystemCertificateId	Wählen Sie einen Eintrag in der Liste der verfügbaren Systemzertifikate aus. Dieses Zertifikat bestätigt die Identität des Clients gegenüber dem Server.

Serveradapter für SSL

FTP-, HTTP-, Sterling Connect:Direct-Serveradapter (mit Secure+-Option) Option) und SMTP-Sendeadapter bieten Unterstützung für SSL.

Die folgenden Serveradapter bieten Unterstützung für SSL (Secure Sockets Layer):

- FTP-Serveradapter
- HTTP-Serveradapter
- Sterling Connect:Direct-Serveradapter (mit Secure+-Option)
- SMTP-Sendeadapter

Die Parameter in der folgenden Tabelle steuern SSL aus der Serverperspektive. Weitere Informationen hierzu finden Sie in der Dokumentation zu dem jeweiligen Adapter oder Dienst, der von Ihnen konfiguriert wird.

Parameter	Beschreibung
SSL	Gibt an, ob SSL aktiv ist.
Kennphrase für Schlüsselzertifikat	Das Kennwort zum Schutz des Serverschlüsselzertifikats. Diese Kennphrase wird intern vom System zum Initialisieren der SSL-Bibliotheken verwendet.
CipherStrength (Verschlüsselungsstärke)	Die Stärke der für die Datenverschlüsselung verwendeten Algorithmen.
Schlüsselzertifikat (Systemspeicher)	Privater Schlüssel und privates Zertifikat für die Serverauthentifizierung.
CA-Zertifikat	Das zum Überprüfen des Zertifikats eines Clients verwendete Zertifikat (sofern vorhanden).

Zertifikat einchecken

Zur Unterstützung der Client/Server-Authentifizierung benötigen Sie ein CA-Zertifikat oder en selbst signiertes Zertifikat sowie ein Systemzertifikat.

Informationen zu diesem Vorgang

Sie können ein CA-Zertifikat oder ein selbst signiertes Zertifikat in einen CA-Zertifikatsspeicher einchecken, indem Sie im **Verwaltungsmenü** die Optionen **Handels-**

partner > **Digitale Zertifikate** > **CA** > **Neues Zertifikat einchecken** auswählen.

Selbst signierte Zertifikate zu Testzwecken erstellen

Sie können zum Testen selbst signierte Zertifikate verwenden. Sie können in Sterling B2B Integrator generiert und verwaltet werden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein selbst signiertes Zertifikat zu erstellen:

Vorgehensweise

1. Wählen Sie **Handelspartner** > **Digitale Zertifikate** > **Systemzertifikate** > **Selbst signiertes Zertifikat erstellen** aus.
2. Nach der Erstellung müssen Sie das Zertifikat suchen und in eine Datei auschecken.
3. Checken Sie das Zertifikat anschließend als CA-Zertifikat wieder in Sterling B2B Integrator ein, indem Sie **Handelspartner** > **Digitale Zertifikate** > **CA** > **Neues Zertifikat einchecken** auswählen.

SSL/TLS-Neuvereinbarung (V5.2.6 oder höher)

Sterling B2B Integrator verwendet IBM JSSE-Parameter, um zu steuern, wie restriktiv die SSL/TLS-Neuvereinbarung (Renegotiation) sein soll. Die folgenden Parameter sind zur Aktualisierung in der Datei `security.properties` verfügbar.

Parametername	Definition	Gültige Werte
com.ibm.jsse2. extended. renegotiation.indicator	Verwenden Sie diese Eigenschaft, um alle Vereinbarungen zur Verwendung von RFC 5746 zu zwingen (nicht nur Neuvereinbarungen). Diese Vereinbarung ist nur dann praktisch, nachdem alle erforderlichen Kommunikationspartner RFC 5746 implementiert haben. Die Standardeinstellung ist OPTIONAL.	Folgende Werte sind gültig: • BOTH - Bewirkt, dass der IBM JSSE2-Server oder IBM JSSE2-Client nur dann die Verbindung herstellt, wenn der Peer die Unterstützung für die RFC 5746-Neuvereinbarung angezeigt hat. Hinweis: Das Setzen dieser Eigenschaft auf BOTH hat Interoperabilitätsprobleme bei Clients oder Servern zur Folge, die nicht auf die Unterstützung von RFC 5746 aktualisiert wurden. • CLIENT - Bewirkt, dass der IBM JSSE2-Client nur dann die Verbindung herstellt, wenn der Server die Unterstützung für die RFC 5746-Neuvereinbarung angezeigt hat. Hinweis: Das Setzen dieser Eigenschaft auf CLIENT hat Interoperabilitätsprobleme bei Servern zur Folge, die nicht auf die Unterstützung von RFC 5746 aktualisiert wurden. • OPTIONAL - Diese Einstellung ist die Standardeinstellung. Die Verwendung dieser Option bedeutet, dass der IBM JSSE2-Server oder der IBM JSSE2-Client den Neuvereinbarungsindikator während des ursprünglichen Handshakes nicht erfordern. • SERVER - Bewirkt, dass der IBM JSSE2-Server nur dann die Verbindung herstellt, wenn der Client die Unterstützung für die RFC 5746-Neuvereinbarung angezeigt hat. Hinweis: Das Setzen dieser Eigenschaft auf SERVER hat Interoperabilitätsprobleme bei Clients zur Folge, die nicht auf die Unterstützung von RFC 5746 aktualisiert wurden.

Parametername	Definition	Gültige Werte
com.ibm.jsse2.renegotiate	Verwenden Sie diese Eigenschaft, um die Fähigkeit der Neuvereinbarung von IBM JSSE2 zu ändern. Der Standardwert ist NONE.	Folgende Werte sind gültig: • ABBREVIATED - Diese Einstellung setzt alles außer Kraft und erlaubt den nicht gesicherten, abgekürzten Handshake während der Neuvereinbarung, wenn die Sitzungskontinuität bewährt ist. RFC 5746-Neuvereinbarungen sind zulässig. • ALL - Diese Einstellung setzt alles außer Kraft und erlaubt den nicht gesicherten, vollständigen Handshake während der Neuvereinbarung. RFC 5746-Neuvereinbarungen sind zulässig. • DISABLED - Diese Einstellung setzt alles außer Kraft und inaktiviert alle nicht sicheren RFC 5746-Neuvereinbarungen. • NONE - Diese Einstellung ist die Standardeinstellung. Es sind keine nicht gesicherten Handshake-Neuvereinbarungen zulässig. Nur RFC 5746-Neuvereinbarungen sind zulässig.

Parametername	Definition	Gültige Werte
com.ibm.jsse2. renegotiation .peer.cert.check	Verwenden Sie diese Eigenschaft, um die Fähigkeit der Neuvereinbarung von IBM JSSE2 zu so zu ändern, dass die Peer-Unterstützung erforderlich ist (spezifiziert in RCF 5746). Diese Anforderung ist nur dann praktisch, nachdem alle erforderlichen Kommunikationspartner RFC 5746 implementiert haben. Der Standardwert lautet 'OFF'.	Folgende Werte sind gültig: • OFF - Diese Einstellung ist die Standardeinstellung. Stoppt, wenn der IBM JSSE2-Client oder der IBM JSSE2-Server einen Identifizierungs-Check gegen das Zertifikat vom Peer durchführen. Das Ergebnis ist, dass das Peerzertifikat such während der Neuvereinbarung ändern darf. • ON - Diese Einstellung bewirkt, dass der IBM JSSE2-Client oder der IBM JSSE2-Server einen Abgleich gegen das Zertifikat vom Peer durchführen. Der Grund ist sicherzustellen, dass sich das Zertifikat während der Neuvereinbarung nicht ändert. Der Abgleich ist sowohl auf sichere als auch auch auf nicht sichere Neuvereinbarungen anwendbar.

Fehler bei SSL beheben

Wenn eine Fehlernachricht ausgegeben wird, können Sie Fehler bei SSL beheben.

Fehlernachrichten zu beschädigten oder unbrauchbaren Zertifikaten

Wenn Sie die Fehlernachricht

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

erhalten, dann lauten die Informationen aus dem Perimeterprotokoll wie folgt:

```
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)
```

Wenn Sie das Zertifikat einchecken, dann wird in Sterling B2B Integrator in der Benennungsanzeige der Statuswert 'Invalid Signature' anzeigt. Wenn ein Geschäftsprozess, der ein abgehendes HTTP-POST mit SSL durchführt, im HTTP-Methodendienst mit einem Fehler fehlschlägt, dann wird die folgende Nachricht angezeigt:

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

Fordern Sie das entsprechende CA-Zertifikat für den Handelspartner an. Wenn der Handelspartner ein selbst signiertes Zertifikat verwendet, dann kann das Zertifikat selbst als CA-Zertifikat verwendet werden.

Zertifizierungsstelle und direkte Vertrauensstellung

Wenn Sterling B2B Integrator als Client arbeitet, der Server über ein Zertifikat verfügt, das von einer Zertifizierungsstelle ausgegeben wurde, und dieses Zertifikat den DNS-Namen des Servers im registrierten Namen des Zertifikatsinhabers enthält, dann können Sie das CA-Stammzertifikat im CA-Speicher speichern und als vertrauenswürdig einstufen. Wenn SSL weiterhin nicht arbeitet, dann verwenden Sie eine direkte Vertrauensstellung. Speichern Sie das Serverzertifikat im CA-Speicher und geben Sie es als vertrauenswürdig an.

Wenn der Server ein selbst signiertes Zertifikat verwendet, dann speichern Sie dieses Zertifikat im CA-Speicher und geben Sie es als vertrauenswürdig an. Auch in diesem Fall verwenden Sie die direkte Vertrauensstellung.

SSL ohne Zertifikat verwenden

Sie können SSL-fähige Adapter nicht ohne das erforderliche Zertifikat oder Systemzertifikat verwenden.

SSL arbeitet nicht mit einer CBC-bassierten Cipher-Suite

Wenn Sie die CBC-Mode Cipher Suite ausgewählt haben und SSL nicht arbeitet, müssen die den SSL-Schutz ausschalten.

Führen Sie anschließend für V5.2.5 die folgenden Schritte aus:

1. Öffnen Sie die Datei tmp.sh zur Bearbeitung.
2. Suchen Sie das Server-Flag für das Betriebssystem, das Sie konfigurieren, und fügen Sie den folgenden Wert hinzu:

   ```
   -DDisableSSLEmptyRecords=true
   ```
3. Speichern und schließen Sie die Datei.

Führen Sie für V5.2.5 und niedriger die folgenden Schritte aus:

1. Suchen Sie im Verzeichnis *<B2Bi Install>*/bin nach `InstallNoappsWindowsService.cmd.in` und `InstallContainerWindowsService.cmd.in` für Windows; suchen Sie nach `tmp.sh_platform_ifcresources_ext.in` für alle anderen Betriebssysteme.
2. Bearbeiten Sie die Datei, um alle Instanzen der folgenden Eigenschaft in 'false' zu ändern:

   ```
   jsse.enableCBCProtection=true
   ```
3. Führen Sie das Script `setupfiles` aus.

HTTPS-Konfiguration für GPM

Der sichere HTTP-Zugriff via SSL wird bereits für die meisten Webanwendungen in Sterling B2B Integrator auf dem HTTP-Basisport + 1 unterstützt.

Diese SSL-Erweiterung bietet Folgendes:

- Aktivierung von HTTPS (HTTP w/ SSL-Verschlüsselung) für den grafischen Prozessmodellierer (GPM).
- Ermöglichung der Inaktivierung und Umleitung von Webanwendungen vom HTTP-Basisport auf einen anderen Port (via HTTPS).
- Unterstützung des sicheren Zugriffs auf Webanwendungen durch Implementierung der Webanwendungen auf einer Instanz des sicheren HTTP-Serveradapters.
- Reduzierung der Sicherheitsrisiken.

Wenn Sie diese Funktion verwenden, müssen Sie den grafischen Prozessmodellierer (GPM) zur Kommunikation mit der Dashboard-Webanwendung via HTTPS und nicht via HTTP konfigurieren. Der Zugriff auf Webanwendungen, die über einen sicheren HTTP-Serveradapter implementiert werden, benötigt möglicherweise mehr Zeit als der Zugriff über den Basisport.

Anmerkung: In V5.2.6 und höher ist das Standardsicherheitsprotokoll TLS 1.2 (für den Basis-HTTP-Port + 1.). Bei Bedarf können Sie dies in TLS 1.1 oder TLS 1.0 ändenr, indem Sie den Parameter **jsseProtocol** in `properties_platform_ifcresources_ext` aktualisieren. Gültiger Werte umfassen die folgenden Parameter:

- **TLS1-TLS1.1** - für TLS1.0 und TLS1.1
- **TLS1.1-TLS1.2** - für TLS1.1 und TLS1.2
- **TLS1** - nur für TLS1.0
- **TLS1.1** nur für TLS1.1
- **TLS1.2** - nur für TLS1.2

Neue SSL-Parameter

Für die erweiterte SSL-Funktion wurden mehrere neue Parameter hinzugefügt. Sie müssen diese Parameter konfigurieren, um die SSL-Kommunikation zwischen dem grafischen Prozessmodellierer (Graphical Process Modeler, GPM) und dem Server zu ermöglichen. Diese neuen Parameter müssen in den zugehörigen Eigenschaftendateien definiert sein.

Alle angepassten Eigenschaften für Ihre Umgebung sollten in der Datei 'customer_overrides.properties' definiert werden, sodass sie während der Installation eines Upgrades oder Patches nicht überschrieben werden. Eigenschaften, die in der Datei 'sandbox.cfg' definiert sind, dürfen nicht in der Datei 'customer_overrides-.properties' definiert werden, da sie in 'customer_overrides.properties' ignoriert werden. Diese Eigenschaften sind die einzigen, die nicht in der Datei 'customer_overrides.properties' definiert werden.

In der folgenden Tabelle werden die neuen SSL-Parameter beschrieben und es wird der Name der Eigenschaftendatei aufgeführt, in der der Parameter zu finden ist.

Parametername	Definition	Eigenschaftendatei
WEBAPP_LIST_PORT	Gibt den Port an, der vom GPM-Client für die Kommunikation mit dem Server verwendet werden soll. Standardmäßig wird während der Installation der Basisport eingestellt. Wenn die Dashboard- und GPM-Webanwendungen auf einer Instanz des sicheren HTTP-Serveradapters implementiert wurden, dann sollte dieser Parameter geändert werden, um mit dem Port der Instanz des sicheren HTTP-Serveradapters übereinzustimmen. Wenn der SSL-Basisport (HTTP-Basisport +1) für die sichere Implementierung des GPM und des Dashboards verwendet wird, dann sollte dieser Parameter so geändert werden, dass er mit dem SSL-Basisport (SSL_PORT in 'sandbox.cfg') übereinstimmt.	Datei 'sandbox.cfg'
WEBAPP_PROTOCOL	Gibt das Protokoll an, das zur Kommunikation mit der Dashboard-Webanwendung (http/https) verwendet werden soll.	Datei 'sandbox.cfg'

Parametername	Definition	Eigenschaftendatei
SKIP_BASEPORT_ DEPLOYMENT_WARS	Gibt an, welche Webanwendungen während der Implementierung der WAR-Dateien auf dem Basisport übersprungen werden sollen. Die Liste der WAR-Dateien ist durch Kommas getrennt, es muss die Groß-/ Kleinschreibung beachtet werden und das Suffix .war wird nicht angegeben. In der Standardeinstellung werden WAR-Dateien nicht übersprungen. Wenn die Dashboard- und GPM-Webanwendungen erfolgreich auf einem sicheren HTTP-Serveradapter implementiert wurden, dann kann dieser Parameter auf 'c=admin,dashboard,gbm' gesetzt werden, um den Zugriff auf diese Webanwendungen am Basisport zu entfernen. Die vollständige Liste umfasst die folgenden Webanwendungen: • myaft • portlets Der Wert ALL kann als Platzhalter verwendet werden, um anzugeben, dass alle WAR-Dateien, die über den HTTP-Basisport implementiert werden, übersprungen werden sollen. Dies ist möglicherweise nicht erforderlich, wenn der Basisport für den externen Zugriff blockiert ist. Der Wert ALL darf nicht zusammen mit einem anderen Wert verwendet werden.	customer_overrides.properties
HTTPS_REDIRECT_WARS	Gibt die WAR-Dateien an, die automatisch vom HTTP-Basisport an den Port des sicheren HTTP-Serveradapters oder den SSL-Basisport umgeleitet werden. Der Wert ALL kann zum Umleiten aller übersprungenen WAR-Dateien am HTTP-Basisport auf HTTPS_LIST_PORT (Port des sicheren HTTP-Serveradapters oder SSL-Basisport) verwendet werden. Der Wert ALL darf nicht zusammen mit einem anderen Wert verwendet werden.	customer_overrides.properties

Parametername	Definition	Eigenschaftendatei
HTTPS_LIST_PORT	Gibt den Port des umgeleiteten Ziels für Anforderungen an, die für den HTTP-Basisport abgesetzt wurden. Dieser Parameter sollte auf den Wert für den Port des sicheren HTTP-Serveradapters oder des SSL-Basisports gesetzt werden.	customer_overrides.properties
HTTPS_CLIENT_CERTS	Eine durch Kommas getrennte Liste von Systemzertifikaten, deren öffentliche Schlüssel zum Standardtruststore hinzugefügt werden müssen. Diese Zertifikate werden für die clientseitige Überprüfung während des SSL-Handshakes verwendet, wenn HTTPS-Aufrufe vom ASI-Server (ASI = Application Server-independent) an sich selbst gesendet werden. Dieser Parameter benötigt Serverzertifikatschlüssel, für die die Option **SubjectAltName** angegeben ist. Wenn Sie bereits vorhandene Schlüssel ohne diesen Parameter verwenden, dann schlägt die Ausführung dieser Funktion fehl und es werden nur schwer nachvollziehbare Nachrichten ausgegeben. **Anmerkung:** Das Zertifikat, das für HTTPS am Port 'Basisport+1' (sslCert) konfiguriert wurde, wird automatisch zum Truststore hinzugefügt und muss nicht zu dieser Liste hinzugefügt werden.	customer_overrides.properties

Wenn Sie diese Funktion konfigurieren und lediglich SKIP_BASEPORT_DEPLOYMENT_WARS, aber nicht HTTPS_REDIRECT_WARS und HTTPS_LIST_PORT definieren, dann kann auf die Webanwendungen über den Basisport nicht zugegriffen werden und der Benutzer wird nicht automatisch auf den HTTPS-Port umgeleitet. Dies ist ein zulässiges Szenario, wenn der Benutzer aus Sicherheitsgründen die automatische Umleitung nicht verwenden will. Die Webanwendungen sind weiterhin verfügbar, wenn der Zugriff über den Port des sicheren HTTP-Serveradapters oder den SSL-Basisport erfolgt.

Automatische Umleitung zu HTTPS aktivieren

Sie können die automatische Umleitung zu HTTPS aktivieren.

Informationen zu diesem Vorgang

Diese Unterstützung wurde hinzugefügt, um das Konfigurieren der automatischen Umleitung zu HTTPS für Webanwendungen zu ermöglichen, die auf einem sicheren Port (HTTP-Serveradapter oder SSL-Basisport) implementiert sind und auf dem Basisport übersprungen werden. Dies ist eine optionale, jedoch dringend empfohlene Konfigurationsmaßnahme.

Anmerkung: Alle angepassten Eigenschaften für Ihre Umgebung sollten in der Datei 'customer_overrides.properties' definiert werden, sodass sie während der Installation eines Upgrades oder Patches nicht überschrieben werden.

Gehen Sie wie folgt vor, um die automatische Umleitung auf HTTPS zu aktivieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/<installationsverzeichnis>/install/properties'.
2. Öffnen Sie die Datei 'customer_overrides.properties' und definieren Sie die folgenden Parameterwerte wie im hier aufgeführten Beispiel dargestellt:

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

   Diese Parameter sind zur automatischen Umleitung eines Benutzers auf die HTTPS-Instanz der Webanwendung konfiguriert.

   Anmerkung: Die Datei 'customer_overrides.properties' gehört nicht zum Standardsystemcode. Sie muss nach der Erstinstallation des System erstellt und mit den für Ihre Umgebungen verfügbaren Daten gefüllt werden.
3. Speichern und schließen Sie die Datei.

Beispielimplementierung

Beispielimplementierung in der Datei 'customer_overrides.properties':

```
 ## 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>
```

Anmerkung: Wenn Sie mit einer Instanz des sicheren HTTP-Serveradapters arbeiten, dann wird bei der Konfiguration vorausgesetzt, dass alle WAR-Dateien, die als HTTPS_REDIRECT_WARS angegeben wurden, in derselben Instanz des HTTP-Serveradapters implementiert werden.

HTTPS_CLIENT_CERTS

Wenn eine Instanz des sicheren HTTP-Serveradapters verwendet wird, muss das SSL-Zertifikat, das zum Konfigurieren der Instanz des sicheren HTTP-Serveradapters verwendet wurde, zur Liste der vertrauenswürdigen Zertifikate hinzugefügt werden.

Dies ist erforderlich, weil einige der Dashboardanzeigen HTTPS-Aufrufe an den ASI-Server zurücksenden. Damit diese Aufrufe das SSL-Handshake erfolgreich ausführen können, müssen die Zertifikate im Truststore auf dem ASI-Server konfiguriert werden. Dieser Arbeitsschritt wird durchgeführt, indem der Zertifikatsname in der Liste HTTPS_CLIENT_CERTS angegeben wird.

Diese Systemzertifikate müssen über die DNS-Namen und IP-Adresse(n) verfügen, die bei der Erstellung des Systemzertifikats als alternative Namen angegeben wurden. Die von JDK bereitgestellte Standardversion der SSL-Hostnamenüberprüfung setzt voraus, dass der Name des vom SSL-Server angegebenen Zertifikats mit dem Hostnamen übereinstimmt, der in der HTTP-URL verwendet wird, oder mit einer

der Zeichenfolgen identisch ist, die im Attribut 'SubjectAltName' im Zertifikat angegeben sind. Einige der Anzeigen im Dashboard sind ohne die Konfiguration von 'SubjectAltName' nicht funktionsfähig.

Alternative Namen werden über die Felder 'Kommagetrennte Liste von IP-Adressen' und 'Kommagetrennte Liste von DNS-Namen' im Erstellungsassistenten für Systemzertifikate (**Handelspartner** > **Digitale Zertifikate** > **System**) konfiguriert.

HTTPS-Unterstützung für GPM

Java Web Start (JavaWS) wird verwendet, um den grafischen Prozessmodellierer (Graphical Process Modeler, GPM) über HTTPS zu starten. Das Produkt bietet ähnlich wie Browser Unterstützung für HTTPS und den dynamischen Import von Zertifikaten.

Während des SSL-Handshakes stellt der Server seine Zertifikate zur Verfügung und JavaWS führt die Überprüfung der Vertrauenswürdigkeit durch. Wenn das Zertifikat von JavaWS nicht überprüft werden kann, dann wird der Benutzer aufgefordert, das Zertifikat entweder anzunehmen oder zurückzuweisen. SSL-Zertifikate können von JavaWS nicht automatisch überprüft werden und müssen deshalb vom Benutzer überprüft werden.

Zertifikate für Java Web Start importieren

Wenn Sie eine Systemanfrage wegen eines nicht vertrauenswürdigen Zertifikats während der JavaWS-Operation (JavaWS = Java Web Start) vermeiden möchten, können Sie die Zertifikate in den Speicher der lokalen Maschine importieren, bevor Sie den grafischen Prozessmodellierer (Graphical Process Modeler, GPM) starten.

Informationen zu diesem Vorgang

Auf diese Weise können Sie Unklarheiten beim Benutzer für den Fall reduzieren, dass das SSL-Zertifikat, das dem sicheren HTTP-Serveradapter oder dem SSL-Basisport zugeordnet ist, von der lokalen Maschine des Benutzers als nicht vertrauenswürdig eingestuft wird.

Gehen Sie wie folgt vor, um vertrauenswürdige Stammzertifikate in JavaWS zu importieren:

Vorgehensweise

1. Speichern Sie das vertrauenswürdige Stammzertifikat in einer Datei auf Ihrem lokalen Computer.
2. Öffnen Sie die **Java-Steuerkonsole** auf Ihrem lokalen Computer (javaws.exe unter `jre\bin`).
3. Öffnen Sie die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate**.
4. Klicken Sie auf **Importieren**, um das System nach einem vertrauenswürdigen Stammzertifikat zu durchsuchen, und wählen Sie es aus.
5. Klicken Sie auf **Öffnen**, um das neue vertrauenswürdige Stammzertifikat zu importieren. Nach dem Einchecken des vertrauenswürdigen Stammzertifikats verwendet JavaWS es zur Überprüfung der Vertrauenswürdigkeit während des SSL-Handshakes.

Über SSL-Basisport von HTTP zu HTTPS wechseln

Über den SSL-Basisport können Sie von HTTP zu HTTPS wechseln.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um über den SSL-Basisport von HTTP zu HTTPS zu wechseln:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/installationsverzeichnis/install/properties'.
2. Öffnen Sie die Datei 'sandbox.cfg'.
3. Ändern Sie die folgenden Parameter:

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

   Diese Parameter werden vom grafischen Prozessmodellierer (GPM) für die Kommunikation mit dem Server verwendet.
4. (Optional, Empfohlen) Wenn Sie den Zugriff auf die Dashboard- und GPM-Webanwendungen über den Basisport inaktivieren und die automatische Umleitung auf den HTTPS-Port konfigurieren wollen, dann geben Sie die folgenden Parameter in der Datei 'customer_overrides.properties' an:

```
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>
```

   Beispiel:

```
## 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. Speichern und schließen Sie die Datei.
6. Navigieren Sie zum Verzeichnis '/installationsverzeichnis/install/bin'.
7. Stoppen Sie Sterling B2B Integrator.
8. Wenden Sie die Konfigurationsänderungen an. Geben Sie `./setupfiles.sh` ein.
9. Implementieren Sie die neue Konfiguration. Geben Sie `./deployer.sh` ein.
10. Starten Sie Sterling B2B Integrator.
11. (Optional) Wenn Sie den Zugriff auf die Dashboard- und GPM-Webanwendungen über den Basisport (Schritt 4) inaktiviert haben, dann überprüfen Sie die von Ihnen vorgenommenen Änderungen. Sie können z. B. Folgendes überprüfen:
    - Der Zugriff auf die Dashboard-Webanwendung über 'http://host:baseport/dashboard' ist nicht möglich oder es erfolgt eine automatische Umleitung auf 'https://host:<base_port + 1>/dashboard'.
    - Der Zugriff auf die GPM-Webanwendung über 'http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp' ist nicht möglich oder es erfolgt eine automatische Umleitung auf 'https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp'.

Über sicheren HTTP-Serveradapter von HTTP zu HTTPS wechseln

Über einen sicheren HTTP-Serveradapter können Sie vom HTTP- in den HTTPS-Modus wechseln.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um vom HTTP- zum HTTPS-Modus zu wechseln:

Vorgehensweise

1. Erstellen Sie eine neue Instanz des HTTP-Serveradapters, für die SSL aktiviert wurde. Sie müssen die folgenden Parameter wie angegeben konfigurieren:
   - **Benutzerauthentifizierung erforderlich** wird auf **Nein** gesetzt.
   - **SSL verwenden** wird auf **Muss** gesetzt.
2. Implementieren Sie die erforderlichen WAR-Dateien auf der Instanz des HTTP-Serveradapters, auf der SSL aktiviert wurde.

   Anmerkung: Alle WAR-Dateien müssen im Verzeichnis `/installationsverzeichnis/install/noapp/deploy` ausgewählt werden, wenn Sie die Instanz des HTTP-Serveradapters konfigurieren. Darüber hinaus muss der Kontextname der Webanwendung für die Verwaltung mit dem Parameter ADMIN_CONTEXT_PATH in der Datei `/installationsverzeichnis/install/properties/sandbox.cfg` übereinstimmen. Für alle anderen Webanwendungen sollte der Kontextname mit dem Namen der WAR-Datei ohne die Erweiterung '.war' übereinstimmen.

   Dies ist erforderlich, damit alle über ein Patch oder Hotfix vorgenommenen Änderungen automatisch in der Implementierung des HTTP-Serveradapters nachvollzogen werden.

   Die erforderlichen WAR-Dateien lauten wie folgt:
   - admin.war
   - dashboard.war
   - gbm.war
   - myaft.war
   - portlets.war

   Möglicherweise sind weitere WAR-Dateien erforderlich, um die neue Funktionalität zu unterstützen, die Sie dem Dashboard hinzugefügt haben.
3. Öffnen Sie die Datei 'sandbox.cfg' und ändern Sie die folgenden Parameter:

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

   Diese Parameter werden vom grafischen Prozessmodellierer (GPM) für die Kommunikation mit dem Server verwendet.
4. (Optional, Empfohlen) Wenn Sie die Implementierung der Dashboard- und GPM-Webanwendungen über den Basisport inaktivieren wollen, dann geben Sie die folgenden Parameter in der Datei 'customer_overrides.properties' an:

```
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>
```

   Beispiel:

```
## 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. Wenn Sie für diese Funktionalität ein anderes Zertifikat verwenden möchten, müssen Sie in `/install_dir/install/properties/customer_overrides.properties` die folgende Zeile einfügen: *noapp.sslCert={mention_name_of_your_own_cert}*. Wenn Sie kein anderes Zertifikat angeben, verwendet die Funktionalität 'ASISslCert'.
6. (Optional) Wenn Sie Cookies über ein sicheres Protokoll wie z. B. HTTPS vom Browser senden möchten, navigieren Sie zu `/install_dir/install/properties` und geben den folgenden Parameter in der Datei 'customer_overrides.properties' an:

   ```
   ## sending cookies as secure over https
   http.useSecureCookie=true
   ```
7. Navigieren Sie zum Verzeichnis '`/installationsverzeichnis/install/bin`'.
8. Stoppen Sie Sterling B2B Integrator.
9. Wenden Sie die Konfigurationsänderungen an. Geben Sie `./setupfiles.sh` ein.
10. Implementieren Sie die neue Konfiguration. Geben Sie `./deployer.sh` ein.
11. Starten Sie Sterling B2B Integrator.
12. 11. Überprüfen Sie, ob die Dashboard-Webanwendung über den HTTP-Serveradapter aufgerufen werden kann, indem Sie auf 'https://host:<*secure_http_server_adapter_port*>/dashboard' zugreifen.
13. Überprüfen Sie, ob die GPM-Webanwendung über den sicheren HTTP-Serveradapter aufgerufen werden kann, indem Sie auf 'https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp' zugreifen.
14. Speichern und schließen Sie die Datei.
15. Wenn Sie die Implementierung der Dashboard- und GPM-Webanwendungen über den Basisport (Schritt 4) inaktiviert haben, stellen Sie Folgendes sicher:
    - Der Zugriff auf die Dashboard-Webanwendung über 'http://host:baseport/dashboard' wird automatisch auf 'https://host:<*secure_http_server_adapter_port*>/dashboard' umgeleitet.
    - Der Zugriff auf die GPM-Webanwendung über 'http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp' wird automatisch auf 'https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp' umgeleitet.

Vom HTTPS- in den HTTP-Modus wechseln

Sie können vom HTTPS- in den HTTP-Modus wechseln.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um vom HTTPS- zum HTTP-Modus zu wechseln:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/installationsverzeichnis/install/properties'.
2. Öffnen Sie die Datei **sandbox.cfg**.
3. Ändern Sie die folgenden Parameter:

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

4. Speichern und schließen Sie die Datei.
5. (Optional) Wenn die Implementierung der Dashboard- und GPM-Webanwendungen am Basisport inaktiviert wurde, als in den HTTPS-Modus umgeschaltet wurde, müssen Sie die Datei 'customer_overrides.properties' öffnen und die folgenden Parameter auf Kommentar setzen, sodass sie nicht angewendet werden:

```
## 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. (Optional) Speichern und schließen Sie die Datei.
7. Navigieren Sie zum Verzeichnis '/installationsverzeichnis/install/bin'.
8. Stoppen Sie Sterling B2B Integrator.
9. Wenden Sie die Konfigurationsänderungen an. Geben Sie `./setupfiles.sh` ein.
10. Implementieren Sie die neue Konfiguration. Geben Sie `./deployer.sh` ein.
11. Starten Sie Sterling B2B Integrator.
12. Stellen Sie Folgendes sicher:
    - Auf die Dashboard-Webanwendung kann über die Adresse 'http://host:baseport/dashboard' zugegriffen werden.
    - Auf die GPM-Webanwendung kann über die Adresse 'http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp' zugegriffen werden.
13. (Optional) Deimplementieren Sie die Webanwendungen auf der SSL-fähigen Instanz des HTTP-Serveradapters.

Hardware Security Module (HSM) V5.2.3 - 5.2.5

Hardwaresicherheitsmodul (HSM)

Beim HSM (Hardwaresicherheitsmodul) handelt es sich um eine hardwarebasierte Sicherheitseinheit, die zum Generieren, Speichern und Schützen von Chiffrierschlüsseln dient. Sie können Systemzertifikate mithilfe von Sterling B2B Integrator in einer Datenbank speichern oder ein Hardwaresicherheitsmodul zur Speicherung verwenden.

Sterling B2B Integrator unterstützt die folgenden HSM-Einheiten:

- SafeNet Eracom ProtectServer Orange External
- ProtectServer Gold PCI-Einheiten

Das Hardwaresicherheitsmodul kann zur Ausführung folgender Tasks verwendet werden:

- Systemzertifikate im HSM erstellen
- Systemzertifikate aus Sterling B2B Integrator importieren
- Systemzertifikate aus Sterling B2B Integrator exportieren

- Systemzertifikate aus dem Hardwaresicherheitsmodul entfernen
- Systemzertifikatdetails für Zertifikate im Hardwaresicherheitsmodul anzeigen

Sterling B2B Integrator-Funktionen für HSM-Unterstützung

Für jedes Schlüsselpaar und jedes Zertifikat wird in der Tabelle CERTS_AND_PRI-_KEY von Sterling B2B Integrator ein Eintrag gespeichert.

Dieser Eintrag enthält Informationen zu folgenden Bereichen:

- Schlüssel und Zertifikate einschließlich ihres Gültigkeitszeitraums, der Seriennummer, der geltenden Nutzungsbeschränkungen, der Angaben zum Aussteller und zum Betreff, der von der Benutzerschnittstelle zur Anzeige für den Benutzer verwendet wird, ohne dass Zugriff auf den Schlüssel oder das Zertifikat bestehen muss.
- Normalisierungen des definierten Namens, die vom System bei Suchvorgängen verwendet werden.
- Änderungen am Datensatz.
- Statusinformationen zum Zertifikatswiderruf.
- Typ des Keystores (Schlüsselspeichers).
- Verweise auf ein binäres Schlüsselspeicherobjekt in DATA_TABLE. Wenn ein Software-Keystore verwendet wird, dann enthält das Referenzobjekt möglicherweise Schlüsseldaten. Im Falle eines HSM (Hardwaresicherheitsmodul) enthält es entweder Referenzinformationen (nCipher) oder einen Platzhalter (Eracom).

Parameter für HSM-Systemzertifikat

Die folgende Tabelle enthält die Parameter für die Befehle 'CreateSystemCert', 'ImportSystemCert' und 'ExportSystemCert'.

Parameter	Beschreibung
autogen	Gibt an, ob vom System generierte Informationen für die Steuerung des Zugriffs auf den Schlüssel und den Keystore verwendet werden sollen. Dieser Parameter muss für Schlüssel in HSMs auf den Wert 'false' gesetzt werden.
alias	Der Name des Schlüssels, der im HSM (Hardware Security Module; Hardwaresicherheitsmodul) gespeichert ist. Verwenden Sie nur solche Aliasnamen, die die Zeichen a - z, A - Z, 0 - 9 oder Bindestriche (-) enthalten und deren Gesamtlänge die Länge der GUID (global eindeutige ID) für das System nicht überschreitet.
Certtype	Der Typ des zu importierenden Zertifikats. Das System unterstützt die folgenden vier Zertifikatsdateitypen: pkcs12, pkcs8, pem und keystore. Sterling B2B Integrator unterstützt nur PEM-Schlüssel, die mit DES oder 3DES verschlüsselt wurden. Verwenden Sie 'keystore', um den Keystore aufzulisten oder zu importieren.
certname	Der Name, der dem Zertifikat in der Sterling B2B Integrator-Datenbank zugeordnet wird.
file	Die Keycert- oder PEM-Datei, die importiert werden soll.
keyname	Der Name des Sterling B2B Integrator-Systemschlüssels, der erstellt werden soll.
keypass	Die PIN für das Token, das zum Schutz des SafeNet Eracom-Hardwaresicherheitsmoduls verwendet wird, in dem der Keystore enthalten ist.

Parameter	Beschreibung
key passphrase	Die Kennphrase für den privaten Schlüssel. Dieser Wert ist in der Befehlszeile optional. Wenn Sie ihn nicht angeben, dann werden Sie vom System zur Eingabe aufgefordert. Die PIN für das Token im SafeNet Eracom-Hardwaresicherheitsmodul, in dem der Keystore enthalten ist.
keysize	Die Länge (in Bit) des RSA-Modulus. Zulässige Werte sind 768, 1024, 2048, 3072 und 4096.
keystoretype	Der Typ des zu importierenden Keystores. Der zulässige Wert ist CRYPTOKI.
keystoreprovider	Der Provider-Typ. SafeNet Eracom ist das einzige unterstützte Hardwaresicherheitsmodul. ERACOM oder ERACOM.n (wenn Sie Zertifikate in einen anderen als den Standardslot 0 importieren).
keytype	Der Algorithmus mit öffentlichem Schlüssel. RSA ist der einzige unterstützte Algorithmus.
ObjectID	Die ID des Systemzertifikats.
pkcs12file	Die zu importierende PKCS12-Datei.
password	Die Speicherkennphrase für die Keycert- oder PEM-Datei.
pkcs12storepass	Die Speicherkennphrase für die PKCS12-Datei.
pkcs12keypass	Die Schlüsselkennphrase, die zur Verschlüsselung des privaten Schlüssels in der PKCS12-Datei verwendet wird.
provider	Der Provider des Keystoretyps. ERACOM oder ERACOM.n (wenn Sie Zertifikate in einen anderen als den Standardslot 0 importieren).
rfc1779rdnsequence	Das Feld für die Zeichenfolge des definierten Namens enthält die Felder, die in der Spalte 'Gültige Werte' angegeben sind. Nur das Feld 'CN' ist erforderlich. Trennen Sie die einzelnen Felder durch ein Komma. Folgende Werte sind gültig: • CN = CommonName (allgemeiner Name) • O = Organization (Organisation) • OU = Organization Unit (Organisationseinheit) • L = Location (Position) • ST = State (Staat) • C = Country (Land; geben Sie einen aus zwei Buchstaben bestehenden ISO3166-1 Alpha-2-Code an)
storetype	Der Keystoretyp. CRYPTOKI ist der einzige unterstützte Keystoretyp.
signingbit	Setzt das Bit für die Signierschlüsselverwendung für das selbst signierte Zertifikat. Gültige Werte sind 'true' (wahr) und 'false' (falsch).
serial	Die Seriennummer des Zertifikats.
system passphrase	Die Sterling B2B Integrator-Systemkennphrase. Dieser Wert ist in der Befehlszeile optional.
store passphrase	Die Kennphrase für den Zugriff auf den Keystore. Die PIN für das Token in dem SafeNet Eracom-Hardwaresicherheitsmodul, in dem der Keystore gespeichert wird. Dieser Wert ist in der Befehlszeile optional.
systempass	Die Sterling B2B Integrator-Systemkennphrase.

Parameter	Beschreibung
storepass	Die PIN für das Token, das zum Schutz des SafeNet Eracom-Hardwaresicherheitsmoduls verwendet wird, in dem der Keystore enthalten ist.
totrusttable	Gibt an, ob das Zertifikat zur Tabelle der vertrauenswürdigen Zertifikate hinzugefügt wird. Gültige Werte sind 'true' (wahr) und 'false' (falsch).
validityindays	Die Zeitdauer in Tagen, die das Zertifikat gültig ist.

SafeNet Eracom-Hardwaresicherheitsmodul

Bevor Sie ein Hardwaresicherheitsmodul (HSM) mit Sterling B2B Integrator verwenden können, müssen Sie Sterling B2B Integrator zur Verwendung und Erkennung des SafeNet Eracom-HSM konfigurieren.

Zum Installieren und Einrichten des SafeNet Eracom-HSM befolgen Sie die Anweisungen, die vom Anbieter der Einheit bereitgestellt werden. Stellen Sie sicher, dass Java Runtime auf Ihrem System installiert ist. Verwenden Sie den Provider des Slots, in dem die Sterling B2B Integrator-Schlüssel gespeichert werden, wenn Sie die Dienstprogramme einrichten und verwenden wollen. Nach Erstellung einer PIN für den SafeNet Eracom-Slot darf diese PIN nicht mehr geändert werden. Sterling B2B Integrator kann nicht auf einen Schlüssel im HSM zugreifen, wenn Sie die PIN geändert haben.

Die SafeNet Eracom-Architektur unterteilt das HSM in mehrere Slots (Bereiche). Sie müssen Karten oder HSMs nach den Anweisungen des jeweiligen Anbieters installieren und konfigurieren. Jeder Slot verfügt über einen zugehörigen Sicherheitsprovider und kann über eine separate PIN (persönliche Identifikationsnummer) geschützt werden. Sie können einen separaten Slot im HSM für Sterling B2B Integrator erstellen und den Slot mit einer eindeutigen PIN schützen. Der Provider für den Standardslot 0 ist ERACOM. Provider für zusätzliche Slots haben den Namen ERACOM.*n*. Hierbei steht *n* für die Nummer des Slots. Vergewissern Sie sich, dass auf Ihrem System die Komponenten von Java Runtime verfügbar sind, damit die Interaktion mit der Einheit möglich ist.

Sterling B2B Integrator zur Verwendung des SafeNet Eracom-Hardwaresicherheitsmoduls konfigurieren

Sie können Sterling B2B Integrator zur Verwendung des SafeNet Eracom-Hardwaresicherheitsmoduls konfigurieren.

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Fügen Sie die folgenden Zeilen zu den Dateien 'tmp.sh' und 'tmp.sh.in' hinzu:

   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib
   export LD_LIBRARY_PATH
   ```
3. Wenn Sie einen netzbasierten Server konfigurieren, dann fügen Sie die folgenden Zeilen zu den Dateien 'tmp.sh' und 'tmp.sh.in' hinzu. Dabei steht *netzeinheiten_IP_ODER_hostname* für die IP-Adresse oder den vollständig qualifizierten Domänennamen des netzbasierten SafeNet Eracom-Servers:

   ```
   ET_HSM_NETCLIENT_SERVERLIST=netzeinheiten_IP_ODER_hostname
   export ET_HSM_NETCLIENT_SERVERLIST
   ```
4. Kopieren Sie die Datei 'jprov.jar' vom Verzeichnis '/opt/Eracom/lib' in das Verzeichnis '/*installationsverzeichnis*/install/jdk/jre/lib/ext'.

5. Fügen Sie eine Definition für jeden Sicherheitsprovider zur Datei '/*installationsverzeichnis*/install/bin/jdk/jre/lib/security/java.security' hinzu. Ermitteln Sie zum Hinzufügen einer Definition die Nummer, die dem Certicom-Provider zugeordnet ist, und weisen Sie für den SafeNet Eracom-Provider den Wert n+1 zu. Bei allen anderen Providern, die nach dem SafeNet Eracom-Provider angegeben werden, müssen Sie die Nummer für 'security.provider' um den Wert '1' erhöhen.

   ```
   security.provider.n=com.certicom.ecc.jcae.Certicom
   security.provider.n+1=au.com.eracom.crypto.provider.ERACOMProvider
   ```

   Wenn Sie im SafeNet Eracom-Hardwaresicherheitsmodul einen anderen Slot als den Slot mit der Nummer null verwenden, dann geben Sie den Slot wie folgt an. Dabei steht *x* für die Nummer des Slots:

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

6. Definieren Sie den Wert für TLSProviderPolicy in der Datei '/*installationsverzeichnis*/install/properties/security.properties'.
   - Wenn der Provider im Slot 0 definiert ist, dann müssen Sie sicherstellen, dass die einzige nicht auf Kommentar gesetzte Zeile für den Parameter TLSProviderPolicy wie folgt lautet:

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

   - Wenn der Provider in einem anderen Slot als Slot 0 definiert ist, dann ändern Sie den Parameter TLSProviderPolicy wie folgt. Dabei steht *x* für den Slot, den Sie konfigurieren:

```
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. Definieren Sie den Befehl KeyStoreProviderKey in der Datei '/*installationsverzeichnis*/install/properties/security.properties':
   - Wenn der Provider im Slot 0 definiert ist, dann müssen Sie sicherstellen, dass KeyStoreProviderMap wie folgt definiert ist:

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

   - Wenn der Provider in einem anderen Slot als Slot 0 definiert ist, dann ändern Sie den Parameter KeyStoreProviderMap wie folgt. Dabei steht *x* für die Slotnummer:

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

Unterstützte nCipher- und SafeNet/Eracom-Netzeinheiten und -PCI-Einheiten

Sterling B2B Integrator unterstützt momentan zusätzlich zu nCipher die SafeNet/Eracom ProtectServer Orange-PCI-Karte und die Orange External-Netzeinheit.

Folgende Komponenten werden unterstützt:

Hersteller	Unterstützte Einheitentypen
nCipher	• nShield-Serie der PCI-Karten • NetHSM-Netzeinheiten

Hersteller	Unterstützte Einheitentypen
SafeNet/Eracom	• ProtectServer Gold-PCI-Karte • ProtectServer Orange-PCI-Karte • ProtectServer Orange External-Netzeinheit

Hardwaresicherheitsmodul verwenden

Systemzertifikate zur Speicherung im Hardwaresicherheitsmodul erstellen

Sie können ein selbst signiertes Systemzertifikat erstellen und es Hardwaresicherheitsmodul (HSM) speichern.

Vorbereitende Schritte

Vorbemerkungen:

- Stoppen Sie Sterling B2B Integrator.
- Vergewissern Sie sich, dass die Sterling B2B Integrator-Datenbank aktiv ist.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein selbst signiertes Systemzertifikat zur Speicherung im Hardwaresicherheitsmodul (HSM) zu erstellen:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase]  [store passphrase] [key passphrase]`
3. Wenn Sie die Kennphrase des Systems, des Speichers und des Schlüssels in der Befehlszeile nicht angegeben haben, dann werden Sie zur Eingabe dieser Daten aufgefordert.

Im HSM gespeicherte Systemzertifikate auflisten

Sie können Informationen zu Systemzertifikaten auflisten, die im HSM (Hardwaresicherheitsmodul) gespeichert sind.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Informationen zu Systemzertifikaten aufzulisten, die im HSM (Hardwaresicherheitsmodul) gespeichert sind:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Beispiel

Im Folgenden ist ein Beispiel für die Befehlsausgabe aufgeführt:

```
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
```

HSM-Systemzertifikat in Sterling B2B Integrator-Datenbank importieren

Verwenden Sie diese Vorgehensweise, wenn ein Schlüssel und ein Zertifikat im HSM (Hardwaresicherheitsmodul) vorhanden sind und unabhängig von Sterling B2B Integrator zum HSM hinzugefügt wurden. Sie müssen die Informationen für ein Systemzertifikat, das in einem HSM gespeichert ist, in die Datenbank importieren, bevor es von Sterling B2B Integrator benutzt werden kann.

Informationen zu diesem Vorgang

Abhängig von der Methode, die Sie zum Hinzufügen des privaten Schlüssels und des Zertifikats zum HSM angewendet haben, werden in der Listenfunktion möglicherweise doppelte Einträge für ein einzelnes Paar aus Schlüssel und Zertifikat angezeigt.

Sie müssen den Alias des Systemzertifikats anfordern, bevor Sie Informationen zu einem Systemzertifikat in die Datenbank importieren können.

Gehen Sie wie folgt vor, um das Systemzertifikat zu importieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

Im HSM gespeicherte Systemzertifikate entfernen

Sie können das Systemzertifikat permanent aus dem Hardwaresicherheitsmodul (HSM) löschen. Die Daten zum privaten Schlüssel, die es enthält, können nicht wiederhergestellt werden.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein im HSM gespeichertes Systemzertifikat zu entfernen:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./RemoveSystemCert.sh -r` *xxxx*
   Hierbei steht *xxxx* für die Objekt-ID des zu entfernenden Zertifikats.

Systemzertifikate exportieren

Sie können Systemzertifikate aus Sterling B2B Integrator exportieren, sodass sie in das Hardwaresicherheitsmodul importiert werden können.

Informationen zu diesem Vorgang

Systemzertifikate in einem Hardwaresicherheitsmodul können nicht mit 'ExportSystemCert.sh' exportiert werden.

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Geben Sie Ihre Kennphrase ein.

Beispiel: HSM-Systemzertifikat

Sie können ein Systemzertifikat im Keycert-, PKCS12- oder PEM-Format in das Hardwaresicherheitsmodul (HSM) importieren. Durch den Import eines Systemzertifikats werden der Schlüssel und das Zertifikat zum HSM hinzugefügt und es wird ein entsprechender Eintrag in der Sterling B2B Integrator-Datenbank erstellt.

Wenn Sie ein PEM-Zertifikat und einen entsprechenden Schlüssel importieren, dann müssen Sie sicherstellen, dass der private Schlüssel im DES- oder im Triple DES-Verschlüsselungsformat erstellt wurde.

Im Folgenden ist ein Beispiel für einen privaten PEM-Schlüssel aufgeführt, der im Triple DES-Format erstellt wurde:

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

Dienstprogramme zur Verwaltung von Systemzertifikaten

HSM-Schlüsselpaare und Zertifikatssignieranforderungen

Das Dienstprogramm GenCSR generiert ein Schlüsselpaar in einem HSM (Hardwaresicherheitsmodul) und erstellt eine PKCS10-Zertifikatssignieranforderung (CSR = Certificate Signing Request) mit einem öffentlichen Schlüssel anhand dieses Schlüsselpaars. Sie können dann die CSR an eine Zertifizierungsstelle (CA = Certificate Authority) übergeben.

Wenn Sie ein von einer Zertifizierungsstelle ausgestelltes Zertifikat erhalten, dann können Sie GenCSR verwenden, um das Zertifikat zu aktualisieren. Das Systemzertifikat ist in Sterling B2B Integrator erst dann verfügbar, wenn eine Aktualisierung mit einem von einer Zertifizierungsstelle ausgestellten Zertifikat durchgeführt wurde.

Sie können dieses Dienstprogramm auch verwenden, um eine Liste von CSRs anzuzeigen, Informationen zu einer CSR in eine Datei zu schreiben, eine CSR zu löschen oder um Informationen zu einem von einer Zertifizierungsstelle ausgestellten Zertifikat, das im Hardwaresicherheitsmodul gespeichert ist, in eine Datei zu schreiben. Informationen zu Zertifikatssignieranforderungen werden in der Sterling B2B Integrator-Datenbank verwaltet, während die eigentlichen Schlüssel im HSM gespeichert werden.

Zur Verwendung des Dienstprogramms müssen Sie zuerst feststellen, welche Aktion Sie ausführen möchten. Anschließend können Sie das Dienstprogramm GenCSR verwenden und die Aktion in der Befehlszeile angeben. Für jede Aktion müssen Sie die Argumente, die für die Aktion erforderlich sind, in der Eigenschaftendatei angeben. Ein Beispiel für eine Eigenschaftendatei mit dem Namen 'csr.properties.sample' wird im Verzeichnis '/*installationsverzeichnis*/install/properties' bereitgestellt.

Das Dienstprogramm GenCSR befindet sich im Verzeichnis '/*installationsverzeichnis*/install/bin'.

Die Befehlssyntax lautet wie folgt: `GenCSR.sh -a ACTION -p PROPERTIES`

GenCSR-Parameter

In der folgenden Tabelle sind die Parameter aufgelistet, die bei Verwendung des Scripts GenCSR verwendet werden.

Parameter	Beschreibung	Gültige Werte
-a ACTION	Die auszuführende Aktion.	Die folgenden Aktionen sind zulässig: • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	Die Eigenschaftendatei, die zusätzliche Parameter enthält, die für die Aktionen benötigt werden. Sie müssen den Pfad zu der Eigenschaftendatei angeben.	Der Name einer Eigenschaftendatei. Beispiel: `csr_create.properties`

HSM-Keystore mit von einer Zertifizierungsstelle ausgestellten Zertifikaten aktualisieren

Mit dem Dienstprogramm GenCSR und dem Argument 'update' können Sie Informationen zu einem von einer Zertifizierungsstelle ausgestellten Zertifikat im HSM-Keystore speichern.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'csr_update.properties' korrekt konfiguriert ist.

   In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'csr_update.properties' für das Argument 'update' benötigt werden.

Parameter	Beschreibung	Gültige Werte
provider	Der Name des Keystore-Providers.	ERACOM oder ERACOM.n
keystoretype	Der Name des verwendeten Keystores.	CRYPTOKI
certificate.request.Name	Der Name der zu aktualisierenden CSR (Certificate Signing Request; Zertifikatssignieranforderung).	Der Name, der einer CSR zugeordnet ist.

Parameter	Beschreibung	Gültige Werte
add.trusted	Gibt an, ob die Zertifikatsinformationen zur Tabelle der vertrauenswürdigen Zertifikate hinzugefügt werden sollen.	True | false
ca.cert.file	Der Pfad und der Dateiname der Datei, in die die Informationen zu dem von einer Zertifizierungsstelle ausgestellten Zertifikat geschrieben werden sollen.	Der gültige Pfad und Dateiname einer von einer Zertifizierungsstelle ausgestellten Zertifikatsdatei.

2. Aktualisieren Sie den HSM-Keystore.

   Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Zertifikatssignieranforderungen auflisten

Mit dem Dienstprogramm GenCSR können Sie unter Verwendung des Arguments 'list' Zertifikatssignieranforderungen (CSRs = Certificate Signing Requests) in der HSM-Datenbank anzeigen. Für das Argument 'list' ist keine Konfiguration der Eigenschaftendatei erforderlich.

Informationen zu diesem Vorgang

Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a list`

Zertifikatssignieranforderung löschen

Mit dem Dienstprogramm GenCSR können Sie unter Verwendung des Arguments 'delete' eine Zertifikatssignieranforderung (CSR = Certificate Signing Request) löschen. Dieses Dienstprogramm löscht ausschließlich die CSR. Systemzertifikate, die mit einem von der Zertifizierungsstelle ausgestellten Zertifikat aktualisiert werden, werden hingegen nicht gelöscht.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'cacert.properties' korrekt konfiguriert wurde. Sie müssen die Eigenschaftendatei konfigurieren, bevor Sie das Argument 'delete' verwenden. In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'cacert.properties' für das Argument 'delete' benötigt werden.

Parameter	Beschreibung	Gültige Werte
certificate.request.Name	Der Name der zu löschenden CSR.	Name einer CSR
keystoretype	Der Name des verwendeten Keystores.	CRYPTOKI
provider	Der Name des Keystore-Providers.	ERACOM[.N]

2. Löschen Sie die CSR. Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a delete -p ../properties/cacert.properties`

CSR-Informationen im PKCS10-Format schreiben

Mit dem Dienstprogramm GenCSR und dem Argument 'getpkcs10' können Sie eine CSR (Certificate Signing Request; Zertifikatssignieranforderung) im PKCS10-Format in die angegebene Datei schreiben.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'csr_getpkcs10.properties' korrekt konfiguriert ist.

   In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'csr_getpkcs10.properties' für das Argument 'getpkcs10' benötigt werden. Sie müssen die Eigenschaftendatei konfigurieren, bevor Sie das Argument 'getpkcs10' verwenden.

Parameter	Beschreibung	Gültige Werte
certificate.request.Name	Der Name der CSR.	Der Name, der einer CSR zugeordnet ist.
keystoretype	Der Name des verwendeten Keystores.	CRYPTOKI
csr.file	Der vollständig qualifizierte Pfad zu der Datei, in die die Informationen zur CSR geschrieben werden sollen.	Der Pfad und der Dateiname einer Datei, in die die CSR-Informationen geschrieben werden sollen.

2. Schreiben Sie die CSR in eine Datei.

   Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Systemzertifikate in HSM verschieben

Sie können selbst signierte Zertifikate oder von einer Zertifizierungsstelle ausgestellte Zertifikate von der Datenbank in das HSM (Hardwaresicherheitsmodul) verschieben.

Informationen zu diesem Vorgang

Die erneute Generierung von Schlüsseln und Zertifikaten mit 'CreateSystemCert.sh' oder 'GenCSR.sh' ist der sicherere Weg.

Gehen Sie wie folgt vor, um selbst signierte Zertifikate oder von einer Zertifizierungsstelle ausgestellte Zertifikate von der Datenbank in das HSM (Hardwaresicherheitsmodul) zu verschieben:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Stoppen Sie Sterling B2B Integrator.
3. Starten Sie die Datenbank.
4. Exportieren Sie das Systemzertifikat in eine PKCS12-Datei:

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

5. Suchen Sie die Objekt-ID des zu entfernenden Systemzertifikats. Geben Sie Folgendes ein:

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

6. Entfernen Sie das Systemzertifikat aus der Datenbank. Geben Sie Folgendes ein:

`RemoveSystemCert.sh -r` *xxxx*. Hierbei steht *xxxx* für die Objekt-ID des Zertifikats, das Sie entfernen möchten.

7. Gehen Sie wie folgt vor, um das in das HSM exportierte Systemzertifikat zu importieren und einen entsprechenden Datenbankeintrag zu erstellen:

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

   Anmerkung: Wenn Sie die Zertifikate 'OpsDrv', 'OpsKey' und 'UIKey' in das HSM verschieben, dann verwenden Sie die exakten Namen. Andernfalls ist die ordnungsgemäße Funktionsweise von Sterling B2B Integrator nicht gewährleistet. Bei allen anderen Systemzertifikaten ist der Name nicht kritisch. Wenn Sie andere Systemzertifikate als 'OpsDrv', 'OpsKey' und 'UIKey' verschieben, dann ändert sich die von den Diensten und Adaptern verwendete Objekt-ID. Konfigurieren Sie alle Dienste, die die verschobenen Systemzertifikate verwenden, neu.

Von Zertifizierungsstelle ausgestelltes Zertifikat in Datei schreiben

Mit dem Dienstprogramm GenCSR und dem Argument 'getcacert' können Sie Zertifikate, die von einer Zertifizierungsstelle ausgestellt werden, in eine Datei schreiben.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'getcacert.properties' korrekt konfiguriert wurde.

   In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'getcacert.properties' für die Aktion 'getcacert' benötigt werden. Sie müssen die Datei 'getcacert.properties' konfigurieren, bevor Sie das Argument 'getcacert' verwenden.

Parameter	Beschreibung	Gültige Werte
certificate.request.Name	Der Name der CSR (Certificate Signing Request; Zertifikatssignieranforderung).	Zertifikatsname
keystoretype	Der Name des verwendeten Keystores.	CRYPTOKI
ca.cert.file	Der vollständig qualifizierte Pfad zu der Datei, in die die Informationen zum CA-Zertifikat geschrieben werden sollen.	Der Name und Pfad der Datei für das CA-Zertifikat.

2. Schreiben Sie das Zertifikat in eine Datei.

   Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Interne Systemzertifikate (OpsDrv, OpsKey, UIKey) im HSM generieren

Zusammen mit Sterling B2B Integrator werden drei Systemzertifikate installiert, die dazu dienen, die internen Operationen zu sichern. Das Verschieben dieser Zertifikate in das HSM (Hardwaresicherheitsmodul) bietet nur geringe Sicherheitsvorteile. Ihre Sicherheitsrichtlinie schreibt möglicherweise vor, dass alle Zertifikate, die private Schlüssel enthalten, im HSM gespeichert werden müssen.

Informationen zu diesem Vorgang

Wenn Sie die internen Systemzertifikate von Sterling B2B Integrator mit dem Namen 'OpsDrv', 'OpsKey' und 'UIKey' im HSM erstellen, dann verwenden Sie die exakten Namen. Andernfalls ist die ordnungsgemäße Funktionsweise von Sterling B2B Integrator nicht gewährleistet.

Gehen Sie wie folgt vor, um interne Systemzertifikate zu generieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie `./RemoveSystemCert.sh -l` ein, um Zertifikate in der Datenbank anzuzeigen. Notieren Sie die Objekt-ID für jedes Systemzertifikat.
3. Geben Sie zum Löschen der Systemzertifikate aus der Datenbank für jedes Zertifikat den folgenden Befehl ein: `./RemoveSystemCert.sh -r` *xxxx*. Hierbei steht *xxxx* für die Objekt-ID des Zertifikats, das entfernt werden soll.
4. Geben Sie Folgendes ein, um das Systemzertifikat im HSM für jedes Zertifikat zu generieren:

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

nCipher und SafeNet Eracom verwenden

Zuordnung des Keystore-Providers

Sterling B2B Integrator verfügt über den Keystoretyp, der bei den Providern von Verschlüsselungsdiensten eindeutig ist; daher kann das Produkt eine Zuordnung zwischen Keystoretypen und -providern herstellen, die zur Implementierung des Keystoreobjekts selbst, der verwendeten Signaturalgorithmen und des Schlüsseltransportalgorithmus erforderlich sind.

Der Schlüssel und das Abstraktionsobjekt für die Schlüsselinformationen enthalten diese Informationen mit einem Verweis auf com.sterlingcommerce.security.PrivateKeyInfo.

Hierdurch kann Sterling B2B Integrator eine Kombination von Schlüsseln für HSMs (Hardwaresicherheitsmodule) und Softwarespeicher in der Datenbank gleichzeitig verwenden, ohne dass hierzu zusätzliche Konfigurationsmaßnahmen erforderlich sind, die über das einleitende Laden des Schlüssels oder der Schlüsselinformationen in die Datenbank hinausgehen. Für Sterling B2B Integrator sind alle Schlüssel unabhängig von ihrem Speicherort identisch.

Die Zuordnung wird als Eigenschaft mit dem Namen KeyStoreProviderMap in der Datei 'security.properties' implementiert. Sie besteht aus einer Gruppe von Einträgen, die durch Strichpunkte (;) begrenzt ist. Jeder Eintrag verfügt über sechs Elemente, die durch Kommas begrenzt sind. Das Format lautet wie folgt:

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

Die Elemente werden in der folgenden Tabelle beschrieben:

Element	Beschreibung	Zusätzliche Informationen
KeyStoreType	Der Zeichenfolgetyp des Keystores.	

Element	Beschreibung	Zusätzliche Informationen
KeyStoreProvider	Der Name des Providers für Verschlüsselungsdienste, der den Keystore implementiert.	
DoesAliasMatter	Gibt an, ob der Aliasnamen der Schlüssel für diesen Keystoretyp eindeutig sein muss.	Mögliche Werte sind 'true' und 'false'. Schlüssel müssen über eindeutige Aliasnamen verfügen, wenn nur ein Keystore pro Einheit definiert ist.
SignatureProvider	Der Name des Providers für Verschlüsselungsdienste, der zum Erstellen von Signaturen mit Schlüsseln aus dem Keystore verwendet wird.	
EncryptionProvider	Der Name des Providers für Verschlüsselungsdienste, der zum Entschlüsseln von Informationen mit Schlüsseln aus dem Keystore verwendet wird.	Dieser Parameter wird meistens für RSA-Schlüsseltransportoperationen verwendet.
KeyOnHSM	Gibt an, ob sich der Keystore in einem Hardwaresicherheitsmodul befindet.	

Die Zeichenfolge NULL ist ein zulässiger Wert und wird so interpretiert, als ob kein Provider angegeben worden wäre. Ein Eintrag muss mindestens zwei Werte aufweisen. Wenn ein Eintrag weniger als sechs Werte enthält, dann werden die Werte von links nach rechts dem Keystore-Provider zugeordnet. Dabei spielt es keine Rolle, ob der Aliasname beim Speichern des Schlüssels, des Signaturproviders und des Verschlüsselungsproviders relevant ist und ob der Schlüssel sich in einem Hardwaresicherheitsmodul für den Keystoretyp befindet. Die anderen Elemente werden als Nullen interpretiert und für die Operationen mit Schlüsseln dieses Typs wird kein spezieller Provider angefordert.

Momentan lautet der Standardwert für KeyStoreProviderMap wie folgt:

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

HSM-Schlüssel und zugehörige Schlüsselinformationen verwalten

Sterling B2B Integrator verfügt über verschiedene Java-Scripts zum Verwalten von Schlüsseln in HSMs (Hardwaresicherheitsmodule).

Die Java-Programme werden im Folgenden aufgelistet.

Programm	Zweck
com.sterlingcommerce.db.RemoveSystemCert	Dient zum Auflisten und Löschen von Sterling B2B Integrator-Systemzertifikaten. Während einer Löschoperation versucht das Programm, den Schlüssel aus dem Keystore zu entfernen und das Keystoreobjekt in der Datenbank zu überschreiben.
com.sterlingcommerce.db.CreateCertEx	Generiert ein Schlüsselpaar in einem HSM und ein selbst signiertes Zertifikat, das den öffentlichen Schlüssel des Schlüsselpaares enthält.

Programm	Zweck
com.sterlingcommerce.security.util. CertificateSigningRequest	Generiert ein Schlüsselpaar in einem HSM und erstellt und verwaltet eine zugehörige PKCS10-Zertifikatssignieranforderung. Die PKCS10-Zertifikatssignieranforderung kann an eine Zertifizierungsstelle eingereicht werden, um ein von dieser Zertifizierungstelle signiertes Zertifikat anzufordern. Dieses Programm kann verwendet werden, um dieses Zertifikat anschließend in den Keystore zu laden und es dem entsprechenden Schlüsselpaar zuzuordnen.
com.sterlingcommerce.db.ImportSystemCert	Importiert einen privaten Schlüssel und ein Zertifikat in einem unterstützten Format (PKCS12 oder PEM) in einen Keystore in einem HSM. Importiert Informationen zu einem privaten Schlüssel und Zertifikat in einem HSM in die Sterling B2B Integrator-Datenbank.

JDK-Änderungen für nCipher-HSM-Unterstützung

Damit Sterling B2B Integrator nCipher-Hardwaresicherheitsmodule (HSMs) verwenden kann, müssen Sie die Provider für Java-Verschlüsselungsdienste von nCipher installieren. Zur Installation müssen Sie die folgenden JAR-Dateien in das Unterverzeichnis 'jre/lib/ext' Ihres JDK kopieren. Ändern Sie die Datei 'java.security', sodass die nCipher-Provider geladen werden können.

Die folgenden Dateien werden vom nCipher-Installationsprogramm im Verzeichnis '/opt/nfast/java/classes' gespeichert:

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

Sie sollten die nCipher-Provider nach dem IBM JCE-Provider und vor dem Certicom-Provider angeben. Beispiel:

```
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
```

Auf Solaris-Systemen mit der Sun-JDK sollten Sie die nCipher-Provider nach den Sun-JCA- und -JCE-Providern und vor dem Certicom-Provider platzieren. Beispiel:

```
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
```

Definieren Sie eine TLSProvider-Richtlinie und verwenden Sie dazu das Beispiel in 'security.properties'. Beispiel:

```
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
```

JDK-Änderungen für Eracom-HSM-Unterstützung

Damit Sterling B2B Integrator Eracom-Hardwaresicherheitsmodule (HSMs) verwenden kann, müssen Sie den Provider für Java-Verschlüsselungsdienste von Eracom installieren. Zur Installation müssen Sie die entsprechenden JAR-Dateien im Unterverzeichnis 'jre/lib/ext' Ihres JDK speichern und anschließend 'java.security' so ändern, dass die nCipher-Provider geladen werden können.

Diese Dateien werden vom nCipher-Installationsprogramm im Verzeichnis '/opt/nfast/java/classes' gespeichert:

- jcprov.jar
- jprov.jar

Der Eracom-Provider sollte nach dem Certicom-Provider hinzugefügt werden. Beispiel:

```
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
```

Anmerkung: Eracom verfügt über einen Provider, der für jeden Slot auf der Karte angegeben werden kann. Verwenden Sie für den Provider für Slot 8 folgende Angabe:

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

Änderungen in Linux-Umgebungen für nCipher-HSM-Unterstützung

nCipher empfiehlt Ihnen die Erstellung eines speziellen Benutzerkontos zur Ausführung des nCipher-Hardwareservers.

Das Konto, über das Sterling B2B Integrator ausgeführt wird, muss über gleichwertige Berechtigungen verfügen oder Sie müssen Sterling B2B Integrator über das spezielle nCipher-Konto oder mit der Berechtigung 'root' ausführen. Wenn Sie eine dieser Aktionen ausführen und dabei MySQL verwenden, müssen Sie die MySQL-Berechtigungen ändern oder MySQL über Ihr normales Konto starten, bevor Sie 'run.sh' aufrufen.

Änderungen in Linux-Umgebungen für Eracom-HSM-Unterstützung

Um die Eracom-Einheit zu verwenden, müssen Sie zusätzliche Informationen in Umgebungsvariablen für die Sitzung angeben, über die auf die Einheit zugegriffen wird.

Die folgenden Änderungen an PATH, LD_LIBRARY_PATH und MANPATH werden empfohlen:

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

Zusätzlich müssen Sie, wenn Sie anstelle einer lokalen PCI-Karte eine Netzeinheit verwenden, ET_HSM_NETCLIENT_SERVERLIST wie folgt angeben:

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

Sie müssen diese Variablen in 'tmp.sh' exportieren.

Hardware Security Module (HSM) V5.2.6 oder höher

Hardwaresicherheitsmodul (HSM)

Beim HSM (Hardwaresicherheitsmodul) handelt es sich um eine hardwarebasierte Sicherheitseinheit, die zum Generieren, Speichern und Schützen von Chiffrierschlüsseln dient. Sie können Systemzertifikate mithilfe von Sterling B2B Integrator in einer Datenbank speichern oder ein Hardwaresicherheitsmodul zur Speicherung verwenden.

Sterling B2B Integrator unterstützt die folgenden HSM-Einheiten:

- SafeNet Luna SA
- nCipher nShield Connect

Das Hardwaresicherheitsmodul kann zur Ausführung folgender Tasks verwendet werden:

- Systemzertifikate im HSM erstellen
- Systemzertifikate aus Sterling B2B Integrator importieren
- Systemzertifikate aus Sterling B2B Integrator exportieren
- Systemzertifikate aus dem Hardwaresicherheitsmodul entfernen
- Systemzertifikatdetails für Zertifikate im Hardwaresicherheitsmodul anzeigen

Sterling B2B Integrator-Funktionen für HSM-Unterstützung

Für jedes Schlüsselpaar und jedes Zertifikat wird in der Tabelle CERTS_AND_PRI-_KEY von Sterling B2B Integrator ein Eintrag gespeichert.

Dieser Eintrag enthält Informationen zu folgenden Bereichen:

- Schlüssel und Zertifikate einschließlich ihres Gültigkeitszeitraums, der Seriennummer, der geltenden Nutzungsbeschränkungen, der Angaben zum Aussteller und zum Betreff, der von der Benutzerschnittstelle zur Anzeige für den Benutzer verwendet wird, ohne dass Zugriff auf den Schlüssel oder das Zertifikat bestehen muss.
- Normalisierungen des definierten Namens, die vom System bei Suchvorgängen verwendet werden.
- Änderungen am Datensatz.

- Statusinformationen zum Zertifikatswiderruf.
- Typ des Keystores (Schlüsselspeichers).
- Verweise auf ein binäres Schlüsselspeicherobjekt in DATA_TABLE. Wenn ein Software-Keystore verwendet wird, dann enthält das Referenzobjekt möglicherweise Schlüsseldaten. Im Fall eines HSM (Hardwaresicherheitsmodul) enthält es entweder Referenzinformationen (nCipher) oder einen Platzhalter (Luna).

Parameter für HSM-Systemzertifikat

Die folgende Tabelle enthält die Parameter für die Befehle 'CreateSystemCert', 'ImportSystemCert' und 'ExportSystemCert'.

Parameter	Beschreibung
autogen	Gibt an, ob vom System generierte Informationen für die Steuerung des Zugriffs auf den Schlüssel und den Keystore verwendet werden sollen. Dieser Parameter muss für Schlüssel in HSMs auf den Wert 'false' gesetzt werden.
alias	Der Name des Schlüssels, der im HSM (Hardware Security Module; Hardwaresicherheitsmodul) gespeichert ist. Verwenden Sie nur solche Aliasnamen, die die Zeichen a - z, A - Z, 0 - 9 oder Bindestriche (-) enthalten und deren Gesamtlänge die Länge der GUID (global eindeutige ID) für das System nicht überschreitet.
Certtype	Der Typ des zu importierenden Zertifikats. Das System unterstützt die folgenden vier Zertifikatsdateitypen: pkcs12, pkcs8, pem und keystore. Sterling B2B Integrator unterstützt nur PEM-Schlüssel, die mit DES oder 3DES verschlüsselt wurden. Verwenden Sie 'keystore', um den Keystore aufzulisten oder zu importieren.
certname	Der Name, der dem Zertifikat in der Sterling B2B Integrator-Datenbank zugeordnet wird.
file	Die Keycert- oder PEM-Datei, die importiert werden soll.
keyname	Der Name des Sterling B2B Integrator-Systemschlüssels, der erstellt werden soll.
keypass	Die PIN für das Token, das zum Schutz des SafeNet- oder or nCipher-Hardwaresicherheitsmoduls verwendet wird, in dem der Keystore enthalten ist.
key passphrase	Die Kennphrase für den privaten Schlüssel. Dieser Wert ist in der Befehlszeile optional. Wenn Sie ihn nicht angeben, werden Sie vom System zur Eingabe aufgefordert.
keysize	Die Länge (in Bit) des RSA-Modulus. Zulässige Werte sind 1024, 2048, 3072 und 4096.
keystoretype	Der Typ des zu importierenden Keystores. Zulässige Werte sind 'nCipher.sworld', 'Luna' und 'PKCS11IMPLKS' (ab 5.2.6.2).
keystoreprovider	Der Provider-Typ. Zulässige Werte sind 'nCipherKM', 'LunaProvider' und 'IBMPKCS11Impl' (ab 5.2.6.2).
keytype	Der Algorithmus mit öffentlichem Schlüssel. RSA ist der einzige unterstützte Algorithmus.
ObjectID	Die ID des Systemzertifikats.
pkcs12file	Die zu importierende PKCS12-Datei.
password	Die Speicherkennphrase für die Keycert- oder PEM-Datei.
pkcs12storepass	Die Speicherkennphrase für die PKCS12-Datei.

Parameter	Beschreibung
pkcs12keypass	Die Schlüsselkennphrase, die zur Verschlüsselung des privaten Schlüssels in der PKCS12-Datei verwendet wird.
provider	Der Provider des Keystoretyps. Zulässige Werte sind 'nCipherKM', 'LunaProvider' und 'IBMPKCS11Impl' (ab 5.2.6.2).
rfc1779rdnsequence	Das Feld für die Zeichenfolge des definierten Namens enthält die Felder, die in der Spalte 'Gültige Werte' angegeben sind. Nur das Feld 'CN' ist erforderlich. Trennen Sie die einzelnen Felder durch ein Komma. Folgende Werte sind gültig: • CN = CommonName (allgemeiner Name) • O = Organization (Organisation) • OU = Organization Unit (Organisationseinheit) • L = Location (Position) • ST = State (Staat) • C = Country (Land; geben Sie einen aus zwei Buchstaben bestehenden ISO3166-1 Alpha-2-Code an)
storetype	Der Keystoretyp. Zulässige Werte sind 'nCipher.sworld', 'Luna' und 'PKCS11IMPLKS' (ab 5.2.6.2).
signingbit	Setzt das Bit für die Signierschlüsselverwendung für das selbst signierte Zertifikat. Gültige Werte sind 'true' (wahr) und 'false' (falsch).
serial	Die Seriennummer des Zertifikats.
system passphrase	Die Sterling B2B Integrator-Systemkennphrase. Dieser Wert ist in der Befehlszeile optional.
store passphrase	Die Kennphrase für den Zugriff auf den Keystore. Dieser Wert ist in der Befehlszeile optional. Wenn Sie ihn nicht angeben, werden Sie vom System zur Eingabe aufgefordert.
systempass	Die Sterling B2B Integrator-Systemkennphrase.
storepass	Die PIN für das Token, das zum Schutz des SafeNet- oder or nCipher-Hardwaresicherheitsmoduls verwendet wird, in dem der Keystore enthalten ist.
totrusttable	Gibt an, ob das Zertifikat zur Tabelle der vertrauenswürdigen Zertifikate hinzugefügt wird. Gültige Werte sind 'true' (wahr) und 'false' (falsch).
validityindays	Die Zeitdauer in Tagen, die das Zertifikat gültig ist.

Hardwaresicherheitsmodul verwenden

Systemzertifikate zur Speicherung im Hardwaresicherheitsmodul erstellen

Sie können ein selbst signiertes Systemzertifikat erstellen und es Hardwaresicherheitsmodul (HSM) speichern.

Vorbereitende Schritte

Vorbemerkungen:

- Stoppen Sie Sterling B2B Integrator.
- Vergewissern Sie sich, dass die Sterling B2B Integrator-Datenbank aktiv ist.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um ein selbst signiertes Systemzertifikat zur Speicherung im Hardwaresicherheitsmodul (HSM) zu erstellen:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. Wenn Sie die Kennphrase des Systems, des Speichers und des Schlüssels in der Befehlszeile nicht angegeben haben, dann werden Sie zur Eingabe dieser Daten aufgefordert.

Im HSM gespeicherte Systemzertifikate auflisten

Sie können Informationen zu Systemzertifikaten auflisten, die im HSM (Hardwaresicherheitsmodul) gespeichert sind.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um Informationen zu Systemzertifikaten aufzulisten, die im HSM (Hardwaresicherheitsmodul) gespeichert sind:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Beispiel

Im Folgenden ist ein Beispiel für die Befehlsausgabe aufgeführt:

```
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
```

Anmerkung: Ab Version 5.2.6.2 ist PKCS11IMPLKS der gültige Wert für 'Keystoretype'.

HSM-Systemzertifikat in Sterling B2B Integrator-Datenbank importieren

Verwenden Sie diese Vorgehensweise, wenn ein Schlüssel und ein Zertifikat im HSM (Hardwaresicherheitsmodul) vorhanden sind und unabhängig von Sterling B2B Integrator zum HSM hinzugefügt wurden. Sie müssen die Informationen für ein Systemzertifikat, das in einem HSM gespeichert ist, in die Datenbank importieren, bevor es von Sterling B2B Integrator benutzt werden kann.

Informationen zu diesem Vorgang

Abhängig von der Methode, die Sie zum Hinzufügen des privaten Schlüssels und des Zertifikats zum HSM angewendet haben, werden in der Listenfunktion möglicherweise doppelte Einträge für ein einzelnes Paar aus Schlüssel und Zertifikat angezeigt.

Sie müssen den Alias des Systemzertifikats anfordern, bevor Sie Informationen zu einem Systemzertifikat in die Datenbank importieren können.

Gehen Sie wie folgt vor, um das Systemzertifikat zu importieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

Im HSM gespeicherte Systemzertifikate entfernen

Informationen zu diesem Vorgang

Mit dieser Prozedur wird das Systemzertifikat permanent aus dem HSM (Hardwaresicherheitsmodul) gelöscht. Die Daten zum privaten Schlüssel, die es enthält, können nicht wiederhergestellt werden.

Gehen Sie wie folgt vor, um ein im HSM gespeichertes Systemzertifikat zu entfernen:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./RemoveSystemCert.sh -r` *xxxx*
   Hierbei steht *xxxx* für die Objekt-ID des zu entfernenden Zertifikats.

Systemzertifikate exportieren

Sie können Systemzertifikate aus Sterling B2B Integrator exportieren, sodass sie in das Hardwaresicherheitsmodul importiert werden können.

Informationen zu diesem Vorgang

Systemzertifikate in einem Hardwaresicherheitsmodul können nicht mit 'ExportSystemCert.sh' exportiert werden.

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie Folgendes ein: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Geben Sie Ihre Kennphrase ein.

Beispiel: HSM-Systemzertifikat

Sie können ein Systemzertifikat im Keycert-, PKCS12- oder PEM-Format in das Hardwaresicherheitsmodul (HSM) importieren. Durch den Import eines Systemzertifikats werden der Schlüssel und das Zertifikat zum HSM hinzugefügt und es wird ein entsprechender Eintrag in der Sterling B2B Integrator-Datenbank erstellt.

Wenn Sie ein PEM-Zertifikat und einen entsprechenden Schlüssel importieren, dann müssen Sie sicherstellen, dass der private Schlüssel im DES- oder im Triple DES-Verschlüsselungsformat erstellt wurde.

Im Folgenden ist ein Beispiel für einen privaten PEM-Schlüssel aufgeführt, der im Triple DES-Format erstellt wurde:

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

Dienstprogramme zur Verwaltung von Systemzertifikaten

HSM-Schlüsselpaare und Zertifikatssignieranforderungen

Das Dienstprogramm GenCSR generiert ein Schlüsselpaar in einem HSM (Hardwaresicherheitsmodul) und erstellt eine PKCS10-Zertifikatssignieranforderung (CSR = Certificate Signing Request) mit einem öffentlichen Schlüssel anhand dieses Schlüsselpaars. Sie können dann die CSR an eine Zertifizierungsstelle (CA = Certificate Authority) übergeben.

Wenn Sie ein von einer Zertifizierungsstelle ausgestelltes Zertifikat erhalten, dann können Sie GenCSR verwenden, um das Zertifikat zu aktualisieren. Das Systemzertifikat ist in Sterling B2B Integrator erst dann verfügbar, wenn eine Aktualisierung mit einem von einer Zertifizierungsstelle ausgestellten Zertifikat durchgeführt wurde.

Sie können dieses Dienstprogramm auch verwenden, um eine Liste von CSRs anzuzeigen, Informationen zu einer CSR in eine Datei zu schreiben, eine CSR zu löschen oder um Informationen zu einem von einer Zertifizierungsstelle ausgestellten Zertifikat, das im Hardwaresicherheitsmodul gespeichert ist, in eine Datei zu schreiben. Informationen zu Zertifikatssignieranforderungen werden in der Sterling B2B Integrator-Datenbank verwaltet, während die eigentlichen Schlüssel im HSM gespeichert werden.

Zur Verwendung des Dienstprogramms müssen Sie zuerst feststellen, welche Aktion Sie ausführen möchten. Anschließend können Sie das Dienstprogramm GenCSR verwenden und die Aktion in der Befehlszeile angeben. Für jede Aktion müssen Sie die Argumente, die für die Aktion erforderlich sind, in der Eigenschaftendatei angeben. Ein Beispiel für eine Eigenschaftendatei mit dem Namen 'csr.properties.sample' wird im Verzeichnis '/*installationsverzeichnis*/install/properties' bereitgestellt.

Das Dienstprogramm GenCSR befindet sich im Verzeichnis '/*installationsverzeichnis*/install/bin'.

Die Befehlssyntax lautet wie folgt: `GenCSR.sh -a ACTION -p PROPERTIES`

GenCSR-Parameter

In der folgenden Tabelle sind die Parameter aufgelistet, die bei Verwendung des Scripts GenCSR verwendet werden.

Parameter	Beschreibung	Gültige Werte
-a ACTION	Die auszuführende Aktion.	Die folgenden Aktionen sind zulässig: • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	Die Eigenschaftendatei, die zusätzliche Parameter enthält, die für die Aktionen benötigt werden. Sie müssen den Pfad zu der Eigenschaftendatei angeben.	Der Name einer Eigenschaftendatei. Beispiel: `csr_create.properties`

HSM-Keystore mit von einer Zertifizierungsstelle ausgestellten Zertifikaten aktualisieren

Informationen zu diesem Vorgang

Mit dem Dienstprogramm GenCSR und dem Argument 'update' können Sie Informationen zu einem von einer Zertifizierungsstelle ausgestellten Zertifikat im HSM-Keystore speichern.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'csr_update.properties' korrekt konfiguriert ist.

   In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'csr_update.properties' für das Argument 'update' benötigt werden.

Parameter	Beschreibung	Gültige Werte
provider	Der Name des Keystore-Providers.	'IBMPKCS11IMPL' (ab V5.2.6.2) oder 'nCipherKM' oder 'LunaProvider'
keystoretype	Der Name des verwendeten Keystores.	'PKCS11IMPLKS' (ab V5.2.6.2) oder 'nCipher.sworld' oder 'Luna' **Anmerkung:** Der Wert für 'keystoretype' muss mit dem Wert für 'provider' synchron sein.
certificate.request.Name	Der Name der zu aktualisierenden CSR (Certificate Signing Request; Zertifikatssignieranforderung).	Der Name, der einer CSR zugeordnet ist.
add.trusted	Gibt an, ob die Zertifikatsinformationen zur Tabelle der vertrauenswürdigen Zertifikate hinzugefügt werden sollen.	True | false

Parameter	Beschreibung	Gültige Werte
ca.cert.file	Der Pfad und der Dateiname der Datei, in die die Informationen zu dem von einer Zertifizierungsstelle ausgestellten Zertifikat geschrieben werden sollen.	Der gültige Pfad und Dateiname einer von einer Zertifizierungsstelle ausgestellten Zertifikatsdatei.

2. Aktualisieren Sie den HSM-Keystore.

   Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Zertifikatssignieranforderungen auflisten

Mit dem Dienstprogramm GenCSR können Sie unter Verwendung des Arguments 'list' Zertifikatssignieranforderungen (CSRs = Certificate Signing Requests) in der HSM-Datenbank anzeigen. Für das Argument 'list' ist keine Konfiguration der Eigenschaftendatei erforderlich.

Informationen zu diesem Vorgang

Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a list`

Zertifikatssignieranforderung löschen

Mit dem Dienstprogramm GenCSR können Sie unter Verwendung des Arguments 'delete' eine Zertifikatssignieranforderung (CSR = Certificate Signing Request) löschen. Dieses Dienstprogramm löscht ausschließlich die CSR. Systemzertifikate, die mit einem von der Zertifizierungsstelle ausgestellten Zertifikat aktualisiert werden, werden hingegen nicht gelöscht.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'cacert.properties' korrekt konfiguriert wurde. Sie müssen die Eigenschaftendatei konfigurieren, bevor Sie das Argument 'delete' verwenden. In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'cacert.properties' für das Argument 'delete' benötigt werden.

Parameter	Beschreibung	Gültige Werte
certificate.request.Name	Der Name der zu löschenden CSR.	Name einer CSR
keystoretype	Der Name des verwendeten Keystores.	'PKCS11IMPLKS' (ab V5.2.6.2) oder 'nCipher.sworld' oder 'Luna'
provider	Der Name des Keystore-Providers.	'IBMPKCS11IMPL' (ab V5.2.6.2) oder 'nCipherKM' oder 'LunaProvider' **Anmerkung:** Der Wert für 'keystoretype' muss mit dem Wert für 'provider' synchron sein.

2. Löschen Sie die CSR. Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a delete -p ../properties/cacert.properties`

CSR-Informationen im PKCS10-Format schreiben

Informationen zu diesem Vorgang

Mit dem Dienstprogramm GenCSR und dem Argument 'getpkcs10' können Sie eine CSR (Certificate Signing Request; Zertifikatssignieranforderung) im PKCS10-Format in die angegebene Datei schreiben.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'csr_getpkcs10.properties' korrekt konfiguriert ist.

   In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'csr_getpkcs10.properties' für das Argument 'getpkcs10' benötigt werden. Sie müssen die Eigenschaftendatei konfigurieren, bevor Sie das Argument 'getpkcs10' verwenden.

Parameter	Beschreibung	Gültige Werte
certificate.request.Name	Der Name der CSR.	Der Name, der einer CSR zugeordnet ist.
keystoretype	Der Name des verwendeten Keystores.	'PKCS11IMPLKS' (ab V5.2.6.2) oder 'nCipher.sworld' oder 'Luna'
csr.file	Der vollständig qualifizierte Pfad zu der Datei, in die die Informationen zur CSR geschrieben werden sollen.	Der Pfad und der Dateiname einer Datei, in die die CSR-Informationen geschrieben werden sollen.

2. Schreiben Sie die CSR in eine Datei.

   Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Systemzertifikate in HSM verschieben

Sie können selbst signierte Zertifikate oder von einer Zertifizierungsstelle ausgestellte Zertifikate von der Datenbank in das HSM (Hardwaresicherheitsmodul) verschieben.

Informationen zu diesem Vorgang

Die erneute Generierung von Schlüsseln und Zertifikaten mit 'CreateSystemCert.sh' oder 'GenCSR.sh' ist der sicherere Weg.

Gehen Sie wie folgt vor, um selbst signierte Zertifikate oder von einer Zertifizierungsstelle ausgestellte Zertifikate von der Datenbank in das HSM (Hardwaresicherheitsmodul) zu verschieben:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Stoppen Sie Sterling B2B Integrator.
3. Starten Sie die Datenbank.
4. Exportieren Sie das Systemzertifikat in eine PKCS12-Datei:

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

5. Suchen Sie die Objekt-ID des zu entfernenden Systemzertifikats. Geben Sie Folgendes ein:

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

6. Entfernen Sie das Systemzertifikat aus der Datenbank. Geben Sie Folgendes ein:

   `RemoveSystemCert.sh -r` *xxxx*. Hierbei steht *xxxx* für die Objekt-ID des Zertifikats, das Sie entfernen möchten.

7. Gehen Sie wie folgt vor, um das in das HSM exportierte Systemzertifikat zu importieren und einen entsprechenden Datenbankeintrag zu erstellen:

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

   Anmerkung: Wenn Sie die Zertifikate 'OpsDrv', 'OpsKey' und 'UIKey' in das HSM verschieben, dann verwenden Sie die exakten Namen. Andernfalls ist die ordnungsgemäße Funktionsweise von Sterling B2B Integrator nicht gewährleistet. Bei allen anderen Systemzertifikaten ist der Name nicht kritisch. Wenn Sie andere Systemzertifikate als 'OpsDrv', 'OpsKey' und 'UIKey' verschieben, dann ändert sich die von den Diensten und Adaptern verwendete Objekt-ID. Konfigurieren Sie alle Dienste, die die verschobenen Systemzertifikate verwenden, neu.

Von Zertifizierungsstelle ausgestelltes Zertifikat in Datei schreiben

Informationen zu diesem Vorgang

Mit dem Dienstprogramm GenCSR und dem Argument 'getcacert' können Sie Zertifikate, die von einer Zertifizierungsstelle ausgestellt werden, in eine Datei schreiben.

Vorgehensweise

1. Vergewissern Sie sich, dass die Datei 'getcacert.properties' korrekt konfiguriert wurde.

   In der folgenden Tabelle werden die Parameter beschrieben, die in der Datei 'getcacert.properties' für die Aktion 'getcacert' benötigt werden. Sie müssen die Datei 'getcacert.properties' konfigurieren, bevor Sie das Argument 'getcacert' verwenden.

Parameter	Beschreibung	Gültige Werte
certificate.request.Name	Der Name der CSR (Certificate Signing Request; Zertifikatssignieranforderung).	Zertifikatsname
keystoretype	Der Name des verwendeten Keystores.	'PKCS11IMPLKS' (ab V5.2.6.2) oder 'nCipher.sworld' oder 'Luna'
ca.cert.file	Der vollständig qualifizierte Pfad zu der Datei, in die die Informationen zum CA-Zertifikat geschrieben werden sollen.	Der Name und Pfad der Datei für das CA-Zertifikat.

2. Schreiben Sie das Zertifikat in eine Datei.

   Die Befehlssyntax lautet wie folgt: `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Interne Systemzertifikate (OpsDrv, OpsKey, UIKey) im HSM generieren

Zusammen mit Sterling B2B Integrator werden drei Systemzertifikate installiert, die dazu dienen, die internen Operationen zu sichern. Das Verschieben dieser Zertifikate in das HSM (Hardwaresicherheitsmodul) bietet nur geringe Sicherheitsvorteile. Ihre Sicherheitsrichtlinie schreibt möglicherweise vor, dass alle Zertifikate, die private Schlüssel enthalten, im HSM gespeichert werden müssen.

Informationen zu diesem Vorgang

Wenn Sie die internen Systemzertifikate von Sterling B2B Integrator mit dem Namen 'OpsDrv', 'OpsKey' und 'UIKey' im HSM erstellen, dann verwenden Sie die exakten Namen. Andernfalls ist die ordnungsgemäße Funktionsweise von Sterling B2B Integrator nicht gewährleistet.

Gehen Sie wie folgt vor, um interne Systemzertifikate zu generieren:

Vorgehensweise

1. Navigieren Sie zum Verzeichnis '/*installationsverzeichnis*/install/bin'.
2. Geben Sie `./RemoveSystemCert.sh -l` ein, um Zertifikate in der Datenbank anzuzeigen. Notieren Sie die Objekt-ID für jedes Systemzertifikat.
3. Geben Sie zum Löschen der Systemzertifikate aus der Datenbank für jedes Zertifikat den folgenden Befehl ein: `./RemoveSystemCert.sh -r` *xxxx*. Hierbei steht *xxxx* für die Objekt-ID des Zertifikats, das entfernt werden soll.
4. Geben Sie Folgendes ein, um das Systemzertifikat im HSM für jedes Zertifikat zu generieren:

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

nCipher- und SafeNet Luna-Einheiten konfigurieren

Zuordnung des Keystore-Providers

Sterling B2B Integrator verfügt über den Keystoretyp, der bei den Providern von Verschlüsselungsdiensten eindeutig ist; daher kann das Produkt eine Zuordnung zwischen Keystoretypen und -providern herstellen, die zur Implementierung des Keystoreobjekts selbst, der verwendeten Signaturalgorithmen und des Schlüsseltransportalgorithmus erforderlich sind.

Der Schlüssel und das Abstraktionsobjekt für die Schlüsselinformationen enthalten diese Informationen mit einem Verweis auf com.sterlingcommerce.security.PrivateKeyInfo.

Hierdurch kann Sterling B2B Integrator eine Kombination von Schlüsseln für HSMs (Hardwaresicherheitsmodule) und Softwarespeicher in der Datenbank gleichzeitig verwenden, ohne dass hierzu zusätzliche Konfigurationsmaßnahmen erforderlich sind, die über das einleitende Laden des Schlüssels oder der Schlüsselinformationen in die Datenbank hinausgehen. Für Sterling B2B Integrator sind alle Schlüssel unabhängig von ihrem Speicherort identisch.

Die Zuordnung wird als Eigenschaft mit dem Namen KeyStoreProviderMap in der Datei 'security.properties' implementiert. Sie besteht aus einer Gruppe von Einträgen, die durch Strichpunkte (;) begrenzt ist. Jeder Eintrag verfügt über sechs Elemente, die durch Kommas begrenzt sind. Das Format lautet wie folgt:

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

Die Elemente werden in der folgenden Tabelle beschrieben:

Element	Beschreibung	Zusätzliche Informationen
KeyStoreType	Der Zeichenfolgetyp des Keystores.	
KeyStoreProvider	Der Name des Providers für Verschlüsselungsdienste, der den Keystore implementiert.	
DoesAliasMatter	Gibt an, ob der Aliasnamen der Schlüssel für diesen Keystoretyp eindeutig sein muss.	Mögliche Werte sind 'true' und 'false'. Schlüssel müssen über eindeutige Aliasnamen verfügen, wenn nur ein Keystore pro Einheit definiert ist.
SignatureProvider	Der Name des Providers für Verschlüsselungsdienste, der zum Erstellen von Signaturen mit Schlüsseln aus dem Keystore verwendet wird.	
EncryptionProvider	Der Name des Providers für Verschlüsselungsdienste, der zum Entschlüsseln von Informationen mit Schlüsseln aus dem Keystore verwendet wird.	Dieser Parameter wird meistens für RSA-Schlüsseltransportoperationen verwendet.
KeyOnHSM	Gibt an, ob sich der Keystore in einem Hardwaresicherheitsmodul befindet.	

Die Zeichenfolge NULL ist ein zulässiger Wert und wird so interpretiert, als ob kein Provider angegeben worden wäre. Ein Eintrag muss mindestens zwei Werte aufweisen. Wenn ein Eintrag weniger als sechs Werte enthält, dann werden die Werte von links nach rechts dem Keystore-Provider zugeordnet. Dabei spielt es keine Rolle, ob der Aliasname beim Speichern des Schlüssels, des Signaturproviders und des Verschlüsselungsproviders relevant ist und ob der Schlüssel sich in einem Hardwaresicherheitsmodul für den Keystoretyp befindet. Die anderen Elemente werden als Nullen interpretiert und für die Operationen mit Schlüsseln dieses Typs wird kein spezieller Provider angefordert.

Momentan lautet der Standardwert für KeyStoreProviderMap wie folgt:

```
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.
```

JDK-Änderungen für nCipher-HSM-Unterstützung

Damit Sterling B2B Integrator nCipher-Hardwaresicherheitsmodule (HSMs) verwenden kann, müssen Sie die Provider für Java-Verschlüsselungsdienste von nCipher installieren. Zur Installation müssen Sie die folgenden JAR-Dateien in das Unterverzeichnis 'jre/lib/ext' Ihres JDK kopieren. Ändern Sie die Datei 'java.security', sodass die nCipher-Provider geladen werden können.

Anmerkung:

1. Die folgende Konfiguration ist nicht erforderlich, wenn Sie neue Schlüssel oder Zertifikate mit der PKCS11IMPLKS-Implementierung ab Version 5.2.6.2 erstellen.
2. Führen Sie die folgenden Schritte aus, wenn Die die vorhandenen Schlüssel oder Zertifikate nach einem Upgrade auf Version 5.2.6.2 weiterhin verwenden wollen.

Die folgenden Dateien werden vom nCipher-Installationsprogramm im Verzeichnis '/opt/nfast/java/classes' gespeichert:

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

Sie sollten die nCipher-Provider nach dem IBM JCE-Provider und vor dem Certicom-Provider angeben.

Darüber hinaus müssen Sie IBMJCEFIPS aus der Liste entfernen.

Beispiel:

```
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
```

Verwenden Sie das folgende Beispiel, wenn Sie die vorhandenen Schlüssel oder Zertifikate in einer Version ab 5.2.6.2 unterstützen wollen.

```
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
```

JDK-Änderungen für SafeNet Luna-HSM-Unterstützung

Damit Sterling B2B Integrator SafeNet Luna-Hardwaresicherheitsmodule (HSMs) verwenden kann, müssen Sie den Provider für Java-Verschlüsselungsdienste von SafeNet Luna installieren. Zur Installation müssen Sie die entsprechenden JAR-Dateien im Unterverzeichnis 'jre/lib/ext' des JDK speichern und anschließend 'java.security' so ändern, dass die Luna-Provider geladen werden können.

Anmerkung:

1. Die folgende Konfiguration ist nicht erforderlich, wenn Sie neue Schlüssel oder Zertifikate mit der PKCS11IMPLKS-Implementierung ab Version 5.2.6.2 erstellen.
2. Führen Sie die folgenden Schritte aus, wenn Die die vorhandenen Schlüssel oder Zertifikate nach einem Upgrade auf Version 5.2.6.2 weiterhin verwenden wollen.

Die folgenden Dateien werden vom nCipher-Installationsprogramm im Verzeichnis '/opt/nfast/java/classes' gespeichert:

- libLunaAPI.so
- LunaProvider.jar

Sie sollten den Luna-Provider nach dem IBM JCE-Provider und vor dem Certicom-Provider angeben.

Darüber hinaus müssen Sie IBMJCEFIPS aus der Liste entfernen.

Beispiel:

```
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
```

Verwenden Sie das folgende Beispiel, wenn Sie die vorhandenen Schlüssel oder Zertifikate in einer Version ab 5.2.6.2 unterstützen wollen.

```
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
```

HSM mit IBM PKCS11IMPLKS konfigurieren (ab Version 5.2.6.2)

HSM mit der IBM PKCS11 Implementierung IMPLKS konfigurieren (ab Version 5.2.6.2)

Informationen zu diesem Vorgang

Ab Version 5.2.6.2 unterstützt das System die IBM PKCS11-Implementierung für HSM-Einheiten. HSMs implementieren die Java-JCE-API. Diese Schnittstelle greift auf die Schlüssel in der Einheit zu.

Vorgehensweise

1. Die neue Eigenschaftendatei **hsm.properties.in** wurde hinzugefügt, um PKCS11IMPLKS/IBMPKCS11Impl zu unterstützen.

   In der folgenden Tabelle werden die Eigenschaften aufgelistet, die für die Konfiguration des HSM verwendet werden.

Attribut	Beschreibung
HSM_KEYSTORE_TYPE	Wenn HSM_ENABLED auf *true* gesetzt ist, muss der Attributwert *IBMPKCS11IMPLKS* sein.
HSM_KEYSTORE_PROVIDER	Wenn HSM_ENABLED auf *true* gesetzt ist, muss der Attributwert *IBMPKCS11Impl* sein.
HSM_KEYSTORE_FILE	<Dieses Feld sollte leer gelassen werden>
HSM_ADAPTER_TYPE	ncipher oder safeNetFor ncipher - Führen Sie beim Erstellen oder Aktualisieren von Schlüsseln oder Zertifikaten den folgenden Befehl aus: UNIX: export CKNFAST_OVERRIDE_SECURITY_ASSURANCES= "longterm;tokenkeys" Windows: set CKNFAST_OVERRIDE_SECURITY_ASSURANCES ="longterm;tokenkeys"
HSM_ENABLED	Dieses Attribut muss auf *true* gesetzt werden, damit das HSM nterstützt wird.
HSM_PRNG_ALGORITHM	Wenn HSM_ENABLED auf *true* gesetzt ist, muss der Attributwert *PKCS11DeviceRNG* sein.
HSM_CONFIG_FILE_LOCATION	Wenn HSM_ENABLED auf *true* gesetzt ist, muss der Attributwert auf die Position der Konfigurationsdatei für IBMPKCS11 festgelegt werden.

2. Aktualisieren oder erstellen Sie die Konfigurationsdatei die abhängig vom HSM-Typ für die HSM-Konfiguration erforderlich ist.

   Je nach HSM-Typ finden Sie die Konfigurationsdatei für die Einheit wie im Folgenden angegeben. Sie können sich auch an den IBM Support wenden,um die Konfigurationsdatei anzufordern. Sie können beliebige der Standardeinstellungen aktualisieren, um sie an Ihre Anforderungen anzupassen. Bearbeiten Sie den Wert für *library*, wenn Ihre Position sich von der Standardeinstellung unterscheidet.

```
Für eine SafeNet Luna-Einheit:

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}
```

Für eine nCipher-Einheit:

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

Anmerkung: Bei SafeNet Luna ist das Importieren eines extern erstellten privaten Schlüssels nicht möglich. Sie müssen die Schlüssel in der HSM-Einheit erstellen und speichern.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. IBM stellt dieses Material möglicherweise auch in anderen Sprachen zur Verfügung. Für den Zugriff auf das Material in einer anderen Sprache kann eine Kopie des Produkts oder der Produktversion in der jeweiligen Sprache erforderlich sein.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes 2,
avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

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

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Die angeführten Kundenbeispiele dienen nur zur Illustration. Die tatsächlichen Ergebnisse beim Leistungsverhalten sind abhängig von der jeweiligen Konfiguration und den Betriebsbedingungen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis)

und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

Marken

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter http://www.ibm.com/legal/copytrade.shtml.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

IT Infrastructure Library ist eine eingetragene Marke der Central Computer and Telecommunications Agency. Die Central Computer and Telecommunications Agency ist nunmehr in das Office of Government Commerce eingegliedert worden.

Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

ITIL ist eine eingetragene Marke, eine eingetragene Gemeinschaftsmarke des Office of Government Commerce und eine eingetragene Marke, die beim U.S. Patent and Trademark Office eingetragen ist.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Java™ und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Cell Broadband Engine wird unter Lizenz verwendet und ist eine Marke der Sony Computer Entertainment, Inc. in den USA und/oder anderen Ländern.

Linear Tape-Open, LTO, das LTO-Logo, Ultrium und das Ultrium-Logo sind Marken von HP, der IBM Corporation und von Quantum in den USA und/oder anderen Ländern.

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®, und Sterling Integrator® sind Marken oder eingetragene Marken der Sterling Commerce, Inc., einer IBM Company.

Weitere Unternehmens-, Produkt- und Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

Bedingungen für die Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit

Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. ürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen

Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die hierin gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden. Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.