Seguridad (V5.2.3 o posterior)

Contenido

Seguridad (V5.2.3 o posterior)

Sterling B2B Integrator utiliza diversos mecanismos de seguridad, incluyendo contraseñas de sistema para funciones administrativas, políticas de contraseña basadas en las políticas de seguridad de la empresa y seguridad basada en rol para proporcionar diferentes niveles de acceso a usuarios diferentes de la organización.

Se proporcionan las siguientes características de seguridad con Sterling B2B Integrator:

- La seguridad basada en rol proporciona a los usuarios acceso a archivos, procesos de negocio, plantillas web, servicio y características de producto, de acuerdo con los permisos asociados con la cuenta de usuario.
- Las políticas de contraseñas son conjuntos de decisiones de seguridad que se toman y se aplican a diferentes cuentas de usuario de acuerdo con las políticas de seguridad de la empresa. Estas opciones incluyen elementos tales como el número de días que una contraseña es válida y la longitud máxima y mínima de una contraseña.
- Se puede utilizar la autenticación LDAP para delegar la autenticación de una cuenta de usuario externa en un directorio LDAP y proporcionar autenticación utilizando la misma información de seguridad utilizada para otras aplicaciones de la empresa. Si la empresa ya ha adoptado LDAP, puede utilizar los directorios LDAP existentes con la aplicación.
- Frase de contraseña de instalación de sistema: Durante la instalación se crea una frase de contraseña de sistema para la instalación de Sterling B2B Integrator. La frase de contraseña es una serie muy compleja que tiene más de 16 caracteres. La frase de contraseña de sistema es necesaria para iniciar el sistema y para acceder a la información de sistema protegida.
- Soporte de certificados x.509 para la seguridad de capa de cifrado, firma y transporte.
- Módulo de software certificado por FIPS (Federal Information Processing Standards - Estándar federal de proceso de información) 140-2 y soporte para hardware certificado por FIPS 140-2 de nCipher y Safenet.
- SSL (Secure Socket Layering - Capa de sockets seguros) y TLS (Transport Layer Security - Seguridad de la capa de transporte).

Además, se pueden configurar las características de seguridad siguientes:

- La característica de tiempo de espera de seguridad le ofrece la posibilidad de configurar tiempos de espera de sesiones de usuario.
- La característica Política de contraseñas personalizada le permite añadir reglas de política de contraseña adicionales. Estas reglas de contraseña adicionales pueden ayudarle a evitar que se utilicen contraseñas débiles que se pueden piratear fácilmente y rechazar contraseñas que no cumplen con los estándares.
- La característica Inicio de sesión único (SSO) es un proceso de autenticación que permite a los usuarios acceder a varias aplicaciones y tener que entrar sólo un nombre de usuario y una contraseña.
- La característica Cifrado de documentos permite la configuración de una capa adicional de seguridad además de los permisos de archivo y base de datos tradicionales.

Seguridad basada en roles

Visión general de seguridad basada en rol

La seguridad basada en rol proporciona a los usuarios acceso a determinados archivos, procesos de negocio, plantillas web, servicios y características de producto, de acuerdo con los permisos asociados con la cuenta de usuario.

Para saber cómo administrar la seguridad basada en rol, debe conocer cómo funcionan juntos los grupos, los permisos y las cuentas de usuario.

- Los permisos proporcionan acceso a las páginas de interfaz de usuario y a la funcionalidad proporcionada por la página.
- Los grupos son colecciones de permisos.
- Las cuentas de usuario se asignan a los permisos y las políticas de contraseña.

La gestión de la seguridad basada en rol incluye las tareas siguientes:

- Crear permisos
- Crear grupos
- Crear políticas de contraseña
- Crear cuentas de usuario

Grupos

Los grupos son colecciones de permisos. Los grupos hacen que sea posible mantener los permisos de acceso para varios usuarios desde un solo lugar. Los grupos ayudan a minimizar la cantidad de trabajo destinado al mantenimiento de cuentas, especialmente cuando varios usuarios realizan la misma función de trabajo.

Puede asociar muchos permisos a usuarios diferentes creando grupos para cada función de trabajo en lugar de cada usuario. También puede asignar un grupo como un subgrupo a otro grupo.

Por ejemplo, un departamento de aprovisionamiento tiene cinco especialistas de aprovisionamiento todos cuales realizan los mismos trabajos. En lugar de aplicar permisos a cada cuenta de usuario de especialista de aprovisionamiento individual, puede crear un grupo de aprovisionamiento y mantener los permisos de acceso para todos los especialistas de aprovisionamiento en un grupo. Dentro del grupo de aprovisionamiento, puede asignar subgrupos para refinar adicionalmente los permisos de acceso de acuerdo con el tipo de aprovisionamiento que lleva a cabo el especialista. Puede asignar subgrupos denominados suministros de oficina, maquinaria, equipo general o vehículos al grupo de aprovisionamiento para refinar los permisos de acceso.

Para evitar que se sobrescriba al aplicar actualizaciones o parches, no modifique los grupos que vienen preconfigurados con el sistema.

Las tareas de grupo incluyen:

- Crear un grupo
- Buscar un grupo
- Editar un grupo
- Suprimir un grupo

Grupos preconfigurados

Para asignar permisos a los usuarios, puede asignar los grupos preconfigurados. Los usuarios heredan todos los permisos asociados con los grupos. Es posible que se asigne un grupo predefinido a un usuario cuando se definen Accesibilidad y Tema para la cuenta de usuario.

Debe tener permiso en el módulo de Cuentas para crear grupos.

Convenios de denominación de grupo

La denominación de grupo sigue una serie de convenios.

Utilice los siguientes convenios de denominación para grupos:

- Los ID de grupo deben ser diferentes.
- Los nombres son sensibles a las mayúsculas y minúsculas.
- Dos nombres de grupo con mayúsculas y minúsculas distintas se consideran como nombres diferentes.
- Si un nombre de grupo se ha utilizado, no se puede utilizar como nombre de un grupo nuevo. Se visualizará un mensaje de error.

Buscar grupos

Puede buscar un grupo desde el menú **Administración**.

Acerca de esta tarea

Para buscar un grupo:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Grupos**.
2. Realice una de las acciones siguientes:
   - Bajo Buscar, entre una parte del **Nombre de grupo** o el **Nombre de grupo** entero que está buscando y pulse **Ir** La página Grupos lista todos los grupos que coinciden con los criterios de búsqueda.
   - Bajo Lista, seleccione ALL o la letra por la que empieza el nombre del grupo que está buscando en el campo **Alfabéticamente** y pulse **Ir** La página Grupos lista todos los grupos que coinciden con los criterios de búsqueda.

Crear grupos

Puede crear un grupo desde el menú **Administración**.

Acerca de esta tarea

Antes de empezar, es necesario saber lo siguiente:

- ID de grupo para el grupo que está creando.
- Nombre de grupo para el grupo que está creando.
- Nombre del propietario del grupo.
- Identidad del socio comercial a asociar con el grupo. Sólo se puede asociar un socio comercial con un grupo, pero una cuenta de usuario puede estar asociada con muchos grupos. Este permite asociar una cuenta de usuario con más de un socio comercial. El campo de identidad se utiliza para direccionar mensajes en el buzón.

Para crear un grupo:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Grupos**.
2. Junto a **Crear un nuevo grupo**, pulse **Ir**
3. En la página Nuevo grupo, entre el **ID de grupo**.
4. Entre el **Nombre de grupo**.
5. Entre el **Propietario**.
6. Seleccione la **identidad**.
7. Pulse **Siguiente**.
8. En la página Asignar subgrupos, si desea filtrar grupos por nombre, bajo Filtrar datos en el campo **Por nombre**, entre una parte del nombre o el nombre entero del grupo que desea filtrar y pulse el botón Filtrar.
9. Seleccione los grupos que desea asignar a este grupo. Mueva los grupos del panel Disponible al panel Asignado.
10. Pulse **Siguiente**.
11. En la página Asignar permisos, ¿desea filtrar permisos?
    - Para filtrar por nombre, bajo Filtrar datos en el campo **Por nombre**, entre una parte del nombre o el nombre entero del permiso que desea filtrar y pulse el botón Filtrar a la derecha del campo **Por tipo**.
    - Para filtrar por tipo, bajo Filtrar datos, seleccione el tipo de permiso para el que desea filtrar en la lista Por tipo y pulse el botón Filtrar situado a la derecha del campo **Por tipo**.
12. Seleccione los permisos que desea asignar a este grupo. Mueva los permisos del panel Disponible al panel Asignado. De forma predeterminada, los permisos asociados con los subgrupos asignados a este grupo ya están seleccionados. Los permisos asociados no se visualizan en la columna disponible; pero se visualizan en la página de confirmación.
13. Pulse **Siguiente**.
14. Revise la información de grupo.
15. Pulse **Finalizar**.

Editar grupos

Puede editar un grupo para actualizar los valores, los subgrupos y los permisos.

Acerca de esta tarea

Al editar un grupo, puede actualizar:

- Parámetros
- Subgrupos
- Permisos

No puede cambiar el ID de grupo. Si necesita cambiar el ID de grupo, debe crear un grupo nuevo.

Para editar un grupo:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Grupos**.
2. Busque el grupo que desea editar, utilizando la búsqueda de nombre de grupo o la lista alfabética, y pulse **Ir**
3. Seleccione **editar** para el grupo que desea actualizar.

4. Actualice cualquiera de los valores de grupo y pulse **Siguiente**.
5. Actualice cualquiera de los subgrupos asignados y pulse **Siguiente**.
6. Actualice cualquiera de los permisos asignados y pulse **Siguiente**.
7. Pulse **Siguiente**.
8. Revise la información de grupo.
9. Pulse **Finalizar**.

Suprimir grupos

Puede suprimir grupos desde el menú **Administración**.

Acerca de esta tarea

No puede eliminar el grupo de administradores de Sterling B2B Integrator o el permiso de cuentas de interfaz de usuario de un usuario administrador. Éstos permiten al administrador del sistema administrar el sistema.

Para suprimir un grupo:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Grupos**.
2. En la página Grupos, localice el grupo que desea suprimir utilizando la opción Buscar o Lista.
3. En la página Grupos, junto al grupo que desea suprimir, pulse **suprimir**.

   El sistema suprime el grupo y visualiza el mensaje:

   ```
   La actualización del sistema se ha realizado correctamente.
   ```

Revisar el nombre y el ID de grupo

Puede revisar el nombre y el ID de un grupo desde el menú **Administración**.

Acerca de esta tarea

Para revisar un nombre y un ID de grupo:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuenta** > **Grupo**.
2. En la página Grupo, localice el grupo que desea revisar utilizando las opciones Buscar o Lista.
3. Seleccione el grupo. Se visualizan el nombre y el ID de grupo.

Permisos

Los permisos proporcionan acceso a los diferentes módulos en Sterling B2B Integrator y son la base de la seguridad basada en rol. Los permisos de un usuario consisten en permisos de grupos más los permisos que están asignados individualmente.

Utilice permisos para:

- Gestionar el acceso para varios usuarios desde un único lugar.
- Gestionar las cuentas de usuario con un mínimo esfuerzo, especialmente para varios usuarios que realizan la misma función de trabajo.

Las tareas de permisos incluyen:

- Crear un permiso

- Buscar un permiso
- Editar un nombre de permiso
- Suprimir un permiso

Antes de crear, editar o suprimir un permiso, decida a qué módulos necesitan o no necesitan acceder los usuarios de ese grupo para realizar las funciones asignadas. Se le debe asignar permiso al módulo de Cuentas para crear permisos.

Para evitar que se sobrescriba al aplicar actualizaciones o parches, no modifique los permisos que vienen preconfigurados con el sistema. Cuando se necesiten agrupaciones personalizadas de permisos, cree un grupo nuevo.

Convenios de denominación de permisos

Los nombres de permisos son sensibles a mayúsculas y minúsculas y no se pueden duplicar.

Los convenios de denominación de permisos incluyen:

- Los nombres son sensibles a mayúsculas y minúsculas por lo que dos nombres con diferente uso de mayúsculas y minúsculas se consideran nombres exclusivos. Por ejemplo, "Cualquier documento" y "Cualquier Documento" son dos nombres de permiso distintos.
- Si un nombre se ha utilizado para un permiso existente, no se puede utilizar como nombre de un permiso nuevo. Se visualizará un mensaje de error.

Aunque dos permisos pueden tener el mismo nombre con distinto uso de mayúsculas y minúsculas, no es recomendable.

Permisos heredados de grupos

Estos grupos están preinstalados y los permisos se heredan cuando un grupo de permisos se asigna a una cuenta de usuario. Los mismos permisos se heredan cuando se asigna un grupo como subgrupo.

Cada grupo contiene los permisos para los elementos de menú más el correspondiente permiso de interfaz de usuario (UI) que se utiliza para otorgar acceso a la página. Por ejemplo, EBXML contiene EBXML de UI.

Nombre de grupo	**ID de grupo**	**Permisos heredados del grupo**
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	Todos los permisos del subgrupo BPMONITOR, más 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	Ninguno
Accounts	acctadmin	Todos los permisos del subgrupo ACCOUNTS más UI Groups, UI User Accounts.
Alert Notifications	notifications	Ninguno

Nombre de grupo	ID de grupo	Permisos heredados del grupo
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	Todos los permisos de los subgrupos BPMONITOR y SERVICES, más UI BP Manager, UI Business Process, UI Delete BP.
CD Server Proxy Administrator	cdsp_admin	Todos los permisos de los subgrupos ACCOUNTS, BPMONITOR, CD Server Proxy User, OPERATIONS y SERVICES, más UI Groups, UI Licenses, UI Password Policy, UI SQL Tool, UI User Accounts.
CD Server Proxy User	cdsp_user	Este grupo se asigna de forma predeterminada cuando se crea una cuenta de usuario con accesibilidad CDSP. Todos los permisos de los subgrupos ACCOUNTS, BPMONITOR, OPERATIONS y SERVICES, más 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.
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	Este grupo se asigna de forma predeterminada cuando se crea una cuenta de usuario con la accesibilidad de UI de panel de instrumentos y cualquiera de los siguientes temas de panel de instrumentos: • AFT • Valor predeterminado • Community Management Operator, Participant, Participant Sponsor, o 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

Nombre de grupo	ID de grupo	Permisos heredados del grupo
Deployment	deploymentadmin	Todos los permisos de los subgrupos ADAPTER_UTILITIES, DEPLOYMENT, EBXML, MAILBOX, MAPS, SERVICES, WEB_EXTENSIONS y WEB_SERVICES, más 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	Ninguno
MAILBOX	MAILBOX	Configuration, Messages, Routing Rules, UI Mailbox, VirtualRoots
MAPS	MAPS	ExtendedRuleLibraries, Maps, Standards, UI Maps
Mailbox Administrators	mboxadmins	Todos los permisos de los grupos MAILBOX y Mailbox Browser Interface Users, más 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	Ninguno
SERVICES	SERVICES	Configuration, Installation/Setup, UI Services
SSH	SSH	AuthorizedUserKey, KnownHostKey, RemoteProfiles, UI SSH, UserIdentityKey

Nombre de grupo	ID de grupo	Permisos heredados del grupo
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
Sterling B2B Integrator Admin	super	Todos los permisos de los subgrupos ACCOUNTS, ADAPTER_UTILITIES, ADVANCED_SETUP, BPMONITOR, DEPLOYMENT, EBXML, ENVELOPES, MAILBOX, MAPS, Mailbox Administrators, OPERATIONS, SERVICES, SSH, WEB_EXTENSIONS y WEB_SERVICES, más 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	Todos los permisos del subgrupo OPERATIONS, más 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	Todos los permisos de los subgrupos ADVANCED_SETUP, ENVELOPES, y SSH, más 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

Nombre de grupo	ID de grupo	Permisos heredados del grupo
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
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

Nombre de grupo	ID de grupo	Permisos heredados del grupo
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
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

Permisos necesarios para acceder a los recursos de interfaz de usuario

Éste es el conjunto mínimo de permisos necesarios para acceder a un elemento de menú así como a la página y la funcionalidad asociadas. Es posible que al asignar el conjunto de permisos mínimos también queden disponibles para el usuario algunas funciones adicionales. Si no tiene permiso para un elemento de menú y su funcionalidad asociada, éste no se mostrará.

Desde el Menú de administración > Proceso de negocio, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Proceso de negocio > Gestor	UI BP Manager (BPMANAGE) más UI Business Process (BUSINESS_PROCESS)
Proceso de negocio > Supervisar > Búsqueda avanzada > Proceso de negocio	BusinessProcesses (PLTADM2) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > Correlación SWIFTNET	SWIFTNETCorrelation (GISADM9) más UI BP Monitor (BPMONITOR) y UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
Proceso de negocio > Supervisar > Búsqueda avanzada > Flujos de datos	DataFlows (GISADM1) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > Documentos	Documents (GISADM2) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > Sesiones de comunicación	Communication Sessions (GISADM3) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > Correlación	Correlation (GISADM4) más UI BP Monitor (BPMONITOR)

Desde el Menú de administración > Proceso de negocio, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Proceso de negocio > Supervisar > Búsqueda avanzada > Correlación BPSS	BPSSCorrelations (GISADM5) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > Correlación EBXML	EBXMLCorrelation (GISADM6) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > Correlación EDI	EDICorrelation (GISADM7) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda avanzada > EDIINT	EDIINT (STDSADM6) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Búsqueda central	CentralSearch (GISADM10) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Procesos actuales	CurrentProcesses (PLTADM3) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Documentos actuales	CurrentDocuments (GISADM11) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Supervisar > Actividades actuales	CurrentActivities (PLTADM4) más UI BP Monitor (BPMONITOR)
Proceso de negocio > Estación de trabajo de entrada de mensajes	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

Desde el Menú de administración > Socio comercial, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Socio comercial > Configuración > Básica	UI Basic Trading Profile Setup (BASIC_SETUP)
Socio comercial > Configuración > Avanzada > Identidades	Identities (GISADM12) más UI Advanced Trading Profile Setup (ADVANCED_SETUP) La supresión también requiere el permiso UI Delete Trading Partner (TP_DELETE)
Socio comercial > Configuración > Avanzada > Transportes	Transports (GISADM13) más UI Advanced Trading Profile Setup (ADVANCED_SETUP) La supresión también requiere el permiso UI Delete Trading Partner (TP_DELETE)
Socio comercial > Configuración > Avanzada > Intercambio de documentos	DocumentExchange (GISADM14) más UI Advanced Trading Profile Setup (ADVANCED_SETUP) La supresión también requiere el permiso UI Delete Trading Partner (TP_DELETE)
Socio comercial > Configuración > Avanzada > Canales de entrega	DeliveryChannels (GISADM15) más UI Advanced Trading Profile Setup (ADVANCED_SETUP) La supresión también requiere el permiso UI Delete Trading Partner (TP_DELETE)
Socio comercial > Configuración > Avanzada > Empaquetado	Packaging (GISADM16) más UI Advanced Trading Profile Setup (ADVANCED_SETUP) La supresión también requiere el permiso UI Delete Trading Partner (TP_DELETE)

Desde el Menú de administración > Socio comercial, Recurso de interfaz de usuario	**Nombre de permiso / ID de permiso**
Socio comercial > Configuración > Avanzada > Perfiles	Profiles (GISADM17) más UI Advanced Trading Profile Setup (ADVANCED_SETUP) La supresión también requiere el permiso UI Delete Trading Partner (TP_DELETE)
Socio comercial > Certificados digitales > CA	UI CA Certs (CA_CERTS) más UI System Certs (SYSTEM_CERTS) UI Certificados de sistema añade la opción Sistema.
Socio comercial > Certificados digitales > De confianza	UI Trusted Certs (TRUSTED_CERTS)
Socio comercial > Certificados digitales > Sistema	UI System Certs (SYSTEM_CERTS)
Socio comercial > Sobres de documentos > Sobres	Envelopes (STDSADM1) más UI Envelope (ENVELOPE)
Socio comercial > Sobres de documentos > Números de control	ControlNumbers (STDSADM2) más UI Envelope (ENVELOPE)
Socio comercial > Sobres de documentos > Registro de transacción	TransactionRegister (STDSADM3) más UI Envelope (ENVELOPE)
Socio comercial > Sobres de documentos > Historial de número de control	ControlNumberHistory (STDSADM4) más UI Envelope (ENVELOPE)
Socio comercial > Sobres de documentos > Cola de verificación de secuencia EDI	EDISequenceCheckQueue (STDSADM5) más UI Envelope (ENVELOPE)
Socio comercial > Contratos	UI Contracts (CONTRACTS) más UI Advanced Trading Partner Setup (ADVANCED_SETUP)
Socio comercial > Listas de códigos	UI CodeLists (CODELISTS)
Socio comercial > AS2	UI AS2 Trading Profile Setup (AS2_SETUP)
Socio comercial > SSH > Perfiles remotos	RemoteProfiles (ASSETADM1) más UI SSH
Socio comercial > SSH > Clave de host conocida	KnownHostKey (ASSETADM2) más UI SSH
Socio comercial > SSH > Clave de identidad de usuario	UserIdentityKey (ASSETADM3) más UI SSH
Socio comercial > SSH > Clave de usuario autorizado	AuthorizedUserKey (ASSETADM4) más UI SSH
Socio comercial > AS3	UI AS3 Trading Profile Setup (AS3_SETUP)
Socio comercial > Perfil de socio FTP Odette > Socio físico	OftpPhysicalPartner (ASSETOFTP1) más UI Adapter Utilities (ADAPTER_UTILITIES)
Socio comercial > Perfil de socio FTP Odette > Contrato de socio físico	OftpPhysicalPartnerContract (ASSETOFTP3) más UI Adapter Utilities (ADAPTER_UTILITIES)

Desde el Menú de administración > Socio comercial, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Socio comercial > Perfil de socio FTP Odette > Socio lógico	OftpLogicalPartner (ASSETOFTP2) más UI Adapter Utilities (ADAPTER_UTILITIES)
Socio comercial > Perfil de socio FTP Odette > Contrato de socio lógico	OftpLogicalPartnerContract (ASSETOFTP4)
Socio comercial > PGP > Gestor de servidores	PGP Server Manager (ASSETADM55) más UI PGP Profile Manager (PGP)
Socio comercial > PGP > Gestor de patrocinadores	PGP Sponsor Manager (ASSETADM56) más UI PGP Profile Manager (PGP)
Socio comercial > PGP > Gestor de socios	PGP Partner Manager (ASSETADM57) más UI PGP Profile Manager (PGP)

Desde el Menú de administración > Despliegue, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Despliegue > Servicios > Instalación/Configuración	Installation/Setup (PLTADM9) más UI Services (SERVICES)
Despliegue > Servicios > Configuración	Configuración (PLTADM10) más UI Services (SERVICES), UI BP Manager (BPMANAGE). Al igual que V5.2.4.3 y superior, también se precisa adaptadores UI StartStop.
Despliegue > Planificaciones	UI Scheduler (SCHEDULER)
Despliegue > Mapas	Maps (ASSETADM5) más UI_Maps
Despliegue > Estándares	Standards (STDSADM7) más UI_Maps
Despliegue > Bibliotecas de reglas ampliadas	ExtendedRuleLibraries (ASSETADM6) más UI_Maps
Despliegue > XSLT	UI XSLT (XSLT)
Despliegue > Extensiones web > Recursos web	WebResources (GISADM19) más UI Web Extensions y UI Web Services (WEB_SERVICES) UI Web Services permite al usuario incorporar un nuevo archivo de recurso web
Despliegue > Extensiones web > Utilidades	Utilities (GISADM20) más UI Web Extensions. Sólo está visible en el caso de una actualización de una versión anterior.
Despliegue > Esquemas	UI Schemas (SCHEMAS)
Despliegue > Buzones > Configuración	Configuration (MBXADM1) más UI Mailbox (MAILBOX)
Despliegue > Buzones > Raíces virtuales	VirtualRoots (MBXADM2) más UI Mailbox (MAILBOX)
Despliegue > Buzones > Reglas de direccionamiento	RoutingRules (MBXADM3) más UI Mailbox (MAILBOX)
Despliegue > Buzones > Mensajes	Messages (MBXADM4) más UI Mailbox (MAILBOX)
Despliegue > EBXML > BPSS	BPSS (ASSETADM7) más UI EBXML (EBXML)

Desde el Menú de administración > Despliegue, Recurso de interfaz de usuario	**Nombre de permiso / ID de permiso**
Despliegue > EBXML> Extensión BPSS	BPSSExtension (ASSETADM8) más UI EBXML (EBXML)
Despliegue > EBXML > CPA	CPA (ASSETADM9) más UI EBXM (EBXML)
Despliegue > Gestor de recursos > Etiquetas de recursos	Resource Tags (PLTADM1) más UI Deployment (DEPLOYMENT)
Despliegue > Gestor de recursos > Importar/Exportar	UI Import/Export (IMPORT_EXPORT)
Despliegue > Programas de utilidad de adaptador > Generador de SAP Suite	SAPSuiteBuilder (ASSETADM10) más UI Adapter Utilities
Despliegue > Programas de utilidad de adaptador > Rutas Sap > Rutas Sap	SAPRoutes (ASSETADM11) más UI Adapter Utilities
Despliegue > Programas de utilidad de adaptador > Rutas Sap > SapRouteXRef	SAPRouteXREF (ASSETADM12) más UI Adapter Utilities
Despliegue > Programas de utilidad de adaptador > BEATuxedo	BEATuxedo (ASSETADM13) más UI Adapter Utilities El elemento de menú no se visualiza a menos que se instale el jar BEATuxedo.
Despliegue > Programas de utilidad de adaptador > Regla de direccionamiento SWIFTNet	UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
Despliegue > Programas de utilidad de adaptador > Perfil de servicio SWIFTNet	UI SWIFTNet Service Profile (SWIFTNET_SVC_PROFILE)
Despliegue > Programas de utilidad de adaptador > Perfil de servicio de copia SWIFTNet	UI SWIFTNet Copy Profile (SWIFTNET_COPY_PROFILE)
Despliegue > Programas de utilidad de adaptador > Gestor de políticas de bloqueo	LockoutPolicyManager (ASSETADM50)
Despliegue > Programas de utilidad de adaptador > Mapas de red C:D > Nodo C:D	CDNetmaps (ASSETADM51) más UI Adapter Utilities (ADAPTER_UTILITIES)
Despliegue > Programas de utilidad de adaptador > Mapas de red C:D > Mapas de red C:D	CDNodes (ASSETADM52) más UI Adapter Utilities (ADAPTER_UTILITIES)
Despliegue > Programas de utilidad de adaptador > Mapas de red C:D > Mapa de red C:D X-REF	CDNetmapXref (ASSETADM53) más UI Adapter Utilities (ADAPTER_UTILITIES)
Despliegue > Programas de utilidad de adaptador > Configuración de políticas	Adapter Policies (ASSETADM54)
Despliegue > Programas de utilidad de adaptador > Raíz virtual de sistema de archivos	File System Virtual Root (ASSETADM58)
Despliegue > Clave de identidad de host SSH	UI SSH Local Identity Key (SSH_LCL_ID_KEY) y UI SSH (SSH)
Despliegue > Servicios web > Gestor	WebServicesManager (ASSETADM16) y UI Web Services (WEB_SERVICES)
Despliegue > Servicios web > Correlaciones de esquema	SchemaMappings (ASSETADM17), UI Web Services (WEB_SERVICES) y UI EBXML (EBXML)

Desde el Menú de administración > Despliegue, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Despliegue > Servicios web > Incorporar WSDL	WSDLCheckIn (ASSETADM18) más UI Web Services (WEB_SERVICES)
Despliegue > Servicios web > Token de seguridad	SecurityToken (ASSETADM18) más UI Web Services (WEB_SERVICES)

Desde el Menú de administración > e-Invoicing, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
e-Invoicing > Acuerdos	eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT) La supresión también necesita el permiso DELETE AGREEMENT (EINV_DELETE_AGREEMENT) de eInvoicing.
e-Invoicing > Archivo integrado	eInvoicing Archive (EINVOICING_ARCHIVE) más eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE)
e-Invoicing > Configuración	eInvoicing Configuration (EINVOICING_CONFIGURATION)

Desde el Menú de administración > Operaciones, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Sistema > Solución de problemas	Troubleshooter (PLTADM17) más UI Operations (OPERATIONS)
Sistema > Rendimiento > Ajuste	Tuning (PLTADM18) más UI Operations (OPERATIONS)
Sistema > Rendimiento > Estadísticas	Statistics (PLTADM19) más UI Operations (OPERATIONS)
Sistemas > Rendimiento > Supervisor JVM	Perfdumps (GISADMIN27) más UI Operations (OPERATIONS)
Sistema > Herramientas de soporte > Gestor SQL	UI SQL Tool (SQLMANAGER)
Sistema > Herramientas de soporte > Caso de asistencia	UI Support Case Tool (SUPPORT_CASE)
Sistema > Registros	UI Logs (SYSTEM_LOGS)
Sistema > Licencias	UI Licenses (LICENSES)
Informes	UI Reports (REPORTS)
Supervisor de subproceso	ThreadMonitor (PLTADM24) más UI Operations (OPERATIONS)
Supervisor de JDBC	JDBCMonitor (PLTADM25) más UI Operations (OPERATIONS) y UI SQL Tool (SQLMANAGER)
Gestor de archivos	UI Archive (ARCHIVE-UI) más UI Operations (OPERATIONS), UI BP Manage (BPMANAGE) y UI Business Process (BUSINESS_PROCESS)
Gestor de bloqueos	UI Lock Manager (LOCK_MANAGER)

Desde el Menú de administración > Operaciones, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Supervisor de mensajes	MessageMonitor (GISADM24) más UI Operations (OPERATIONS)
Servicios perimetrales	UI Perimeter Servers (PSERVERS)
Servidores proxy	UI Proxy Servers (PROXYSERVERS) más Sterling B2B Integrator Admin group

Desde el Menú de administración > Cuentas, Recurso de interfaz de usuario	Nombre de permiso / ID de permiso
Grupos	UI Groups (GROUPS) más UI Accounts (ACCOUNTS)
Permisos	Permissions (PLTADM27) más UI Accounts (ACCOUNTS)
Cuentas de usuarios	UI User Accounts (USER_ACCOUNTS) más UI Accounts (ACCOUNTS)
Política de contraseñas	PasswordPolicy (PLTADM29) más UI Accounts (ACCOUNTS)
Noticias de usuario	UserNews (GISADM25) más UI Accounts (ACCOUNTS)
Mi cuenta	MyAccount (PLTADM30)

Permisos preconfigurados

Con el sistema se proporcionan permisos preconfigurados. Igual que los permisos personalizados, proporcionan acceso a los diferentes módulos del sistema.

Buscar nombres de permiso

Puede buscar un permiso desde el menú **Administración**.

Acerca de esta tarea

Para buscar un permiso:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Permisos**.
2. En la página de Permisos, realice una de las acciones siguientes:
   - Bajo Buscar en el campo **Nombre de permiso**, entre una parte del nombre de permiso o el nombre de permiso entero que está buscando y pulse **Ir** La página Permisos lista todos los permisos que coinciden con los criterios de búsqueda.
   - Bajo Lista en el campo **Alfabéticamente**, seleccione **TODOS** o la letra por la que empieza el nombre del permiso que está buscando y pulse **Ir** La página Permisos lista todos los permisos que coinciden con los criterios de búsqueda.

Crear permisos

Si ha actualizado desde una versión anterior del sistema, los permisos existentes se establecen en Otro de forma predeterminada. Podría tener que editar cada permiso para aplicar un nuevo tipo de permiso.

Acerca de esta tarea

Antes de empezar, debe conocer la información siguiente:

Campo	Descripción
ID de permiso	ID de permiso para el permiso que está creando. El ID de permiso es el nombre del proceso de negocio, documento XSLT, plantilla web o recurso para el que está estableciendo el permiso. Incluya la extensión para el recurso después del ID. Campo necesario. ID de permiso: • Deben ser exclusivos. • Son sensibles a las mayúsculas y minúsculas. • El ID de permiso debe coincidir con el nombre del proceso de negocio, documento XSLT, plantilla web o recurso. Si el ID de permiso y el nombre del recurso no coinciden exactamente, puede bloquear el recurso.
Nombre de permiso	Asunto del permiso que está creando. Campo necesario. Un nombre de permiso debe ser exclusivo. Los nombres de permiso son sensibles a las mayúsculas y minúsculas, por ejemplo, "Cualquier documento" y "Cualquier Documento" son dos nombres de permiso distintos.
Tipo de permiso	Tipo de permiso para el permiso que está creando. Campo necesario. Los tipos de permiso incluyen: • UI - Permite el acceso a elementos de menú específicos en la interfaz. • Buzón - Permite el acceso a los buzones específicos del sistema. • Plantilla – Permite el acceso a plantillas web específicas. • BP – Permite el acceso a procesos de negocio específicos. • Seguimiento - Permite el acceso a opciones de seguimiento de documentos específicas. • Comunidad – Permite el acceso a opciones de gestión de comunidad específicas. • Servicio web • Servicio • eInvoicing • Otro – Permite el acceso a recursos no identificados por uno de los tipos anteriores.

Para crear un permiso:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Permisos**.
2. Junto a **Crear un nuevo permiso**, pulse **Ir**!
3. En la página Permisos, entre el**ID de permiso**.
4. Entre el **Nombre de permiso**.
5. Seleccione el **Tipo de permiso**.
6. Pulse **Siguiente**.
7. Revise los valores de permiso.
8. Pulse **Finalizar**.

Editar nombres de permiso

Si necesita cambiar el nombre de un permiso para reflejar el permiso más detenidamente, edite un nombre de permiso. Los nombres de permiso deben ser exclusivos y son sensibles a las mayúsculas y minúsculas. No puede cambiar el ID de permiso. Si necesita editar el ID de permiso, debe crear un nuevo permiso.

Acerca de esta tarea

Para editar un nombre de permiso:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Permisos**.
2. Busque el permiso que desea editar, utilizando la búsqueda de nombre de permiso o la lista alfabética, y pulse **Ir**
3. Junto al permiso que desea editar, pulse **editar**.
4. Entre un nuevo **Nombre de permiso**.
5. Actualice el tipo de permiso, si es necesario, y pulse **Siguiente**.
6. Revise la información de valores de permisos.
7. Pulse **Finalizar**.

Suprimir permisos

Puede suprimir un permiso que esté asociado con una cuenta de usuario. Cuando se suprime un permiso, se elimina del uso para todas las cuentas de usuario.

Acerca de esta tarea

Si el permiso que está suprimiendo es el único permiso que está asociado con una cuenta de usuario, debe editar la cuenta de usuario para asociar otro permiso. Si no asocia al menos un nuevo permiso con la cuenta de usuario, el usuario puede iniciar la sesión, pero no tiene acceso a ningún elemento de menú.

Para suprimir un permiso:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Permisos**.
2. Busque el permiso que desea suprimir, utilizando la búsqueda de nombre de permiso o la lista alfabética y pulse **Ir**
3. En la página Permisos, pulse **Suprimir** para el permiso que desea suprimir.
4. Verifique que la información de permiso coincide con el permiso que desea suprimir y pulse **Suprimir**.

   El sistema suprime el permiso y visualiza el mensaje:

   ```
   La actualización del sistema se ha realizado correctamente.
   ```

Revisar el nombre y el ID de permiso

Puede revisar el nombre y el ID de un permiso desde el menú **Administración**.

Acerca de esta tarea

Para revisar un nombre y un ID de permiso:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Permisos**.

2. Busque el permiso que desea revisar, utilizando la búsqueda de nombre de permiso o la lista alfabética y pulse **Ir**
3. Seleccione el permiso. Se visualizan el nombre y el ID de permiso.

Cuentas de usuarios

Las cuentas de usuario se definen por grupos, permisos y políticas de contraseña para ayudar a proporcionar un entorno seguro. Este tipo de definición de cuenta de usuario se define como un modelo de seguridad basado en rol.

Antes de crear las cuentas de usuario nuevas, necesita determinar qué grupos, permisos y políticas de contraseña necesita el entorno de negocio. La asignación de grupos, permisos y políticas de contraseña es opcional.

Sólo la cuenta con permisos para crear puede crear cuentas de usuario nuevas. Las tareas de las cuentas de usuario incluyen:

- Crear una cuenta de usuario
- Buscar una cuenta de usuario
- Editar una cuenta de usuario
- Suprimir una cuenta de usuario

Permisos de cuenta de usuario predeterminados

Los permisos MyAccount y de aplicación web se asignan automáticamente a las cuentas de usuario.

Los permisos siguientes se asignan automáticamente a las cuentas de usuario:

- MyAccount (ID de permiso PLTADM30) – Permite el acceso a la página Mi cuenta (Cuentas > Mi cuenta).
- Permisos de aplicación web de administración (ID de permiso WebAppAdminPermission) – Se utiliza para acceder a otras aplicaciones web.

No elimine estos permisos de las cuentas de usuario. Si se eliminan accidentalmente, edite la cuenta de usuario y guárdela. Se restaurarán los permisos que faltan.

Autenticación de cuenta de usuario

La autenticación de la cuenta de usuario puede ser local o externa.

La autenticación de la cuenta de usuario puede ser:

- Local – La autenticación se realiza en la base de datos.
- Externa – La autenticación se completa contra un servidor LDAP. La autenticación externo no necesita el adaptador LDAP, que se utiliza con procesos de negocio y permite comunicarse con servidores LDAP locales o remotos utilizando una JNDI (Java Naming Directory Interface). Si no tiene una licencia para un único inicio de sesión o LDAP, todos los usuarios que crea son usuarios locales y se autentican en la base de datos de la aplicación. Para crear una cuenta de usuario externo, debe tener una licencia de aplicación para un único inicio de sesión o LDAP.

Lista de comprobación de creación de cuenta de usuario

Puede crear una cuenta de usuario.

Utilice esta lista de comprobación para crear una cuenta de usuario:

Tarea	Lista de comprobación de seguridad basada en rol	Notas del usuario
1	Crear permisos nuevos o revisar los permisos preconfigurados que vienen preinstalados.	
2	Crear grupos nuevos o revisar los grupos que vienen preinstalados.	
3	Crear una política de contraseña personalizada a asignarla al usuario.	
4	Si está utilizando la autenticación externa, configure el entorno para la autenticación externa.	
5	Crear la cuenta de usuario y asignar los permisos, los grupos y las políticas de contraseña.	

Configurar el entorno para la autenticación de cuenta de usuario externo

Si está creando un usuario externo, puede especificar un método de autenticación alternativo (generalmente LDAP).

Acerca de esta tarea

Antes de crear una cuenta de usuario externo, debe realizar lo siguiente:

Procedimiento

1. Detenga Sterling B2B Integrator.
2. Especifique el método de autenticación alternativo añadiendo o modificando la configuración de autenticación en el archivo authentication_policy.properties.in. Las propiedades deben seguir este formato: authentication_4.*xxx*=*xxx*_value.
3. Entre `setupfiles.sh`.
4. Inicie Sterling B2B Integrator.

Buscar cuentas de usuario

Puede buscar una cuenta de usuario desde el menú **Administración**.

Acerca de esta tarea

Para buscar una cuenta de usuario:

Procedimiento

1. En el menú **Administración**, seleccione **Cuentas** > **Cuentas de usuario**.
2. Realice una de las acciones siguientes:
   - Bajo Buscar en el campo **Nombre de cuenta**, escriba una parte del nombre o el nombre entero de la cuenta de usuario que está buscando y pulse **Ir** La página Cuentas lista todas las cuentas de usuario que coinciden con los criterios de búsqueda.

- Bajo Lista en el campo **Alfabéticamente**, seleccione **TODOS** o la letra por la que empieza el nombre de la cuenta de usuario que está buscando y pulse **Ir** La página Cuentas lista todas las cuentas de usuario que coinciden con los criterios de búsqueda.

Crear cuentas de usuario

Puede crear una nueva cuenta de usuario desde el menú **Administración**.

Acerca de esta tarea

Antes de empezar, debe saber si está utilizando la autenticación local o externa:

- Local – La autenticación se completa en la base de datos de la aplicación. Valor predeterminado.
- Externa – La autenticación se completa contra un servidor LDAP. La autenticación externa no requiere el adaptador LDAP, que se utiliza con procesos empresariales y permite al sistema comunicarse con servidores LDAP locales o remotos mediante JNDI.

Si asigna una o más claves de usuario autorizado a esta cuenta, las claves se deben obtener del socio comercial e incorporar antes de crear la cuenta de usuario.

Nota: Aunque se soportan varios idiomas, una cuenta de usuario no se debe utilizar con más de un idioma específico para evitar problemas de visualización de interfaz de usuario.

También debe conocer la información siguiente:

Campo	Descripción
ID de usuario	ID de usuario de la cuenta de usuario que está creando. El ID de usuario debe tener una longitud mínima de cinco caracteres alfanuméricos. No se pueden utilizar caracteres especiales ni signos de puntuación. Campo necesario. Sólo en el caso de la base de datos MySQL, el inicio de sesión no distingue entre mayúsculas y minúsculas. Debe utilizar siempre ID con grafía exclusiva, de modo que un usuario no utilice accidentalmente el ID de otro usuario.
Contraseña (sólo autenticación local)	Contraseña de la cuenta de usuario que está creando. La contraseña debe tener como mínimo 6 caracteres alfanuméricos. Se permiten caracteres especiales. Obligatorio para usuarios locales. Este campo no se muestra en el caso de los usuarios externos.
Confirmar contraseña (sólo autenticación local)	Escriba la contraseña una segunda vez. Obligatorio para usuarios locales. Este campo no se muestra en el caso de los usuarios externos.
Política (sólo autenticación local)	Política de contraseña que debe asociarse con esta cuenta de usuario. En la lista, seleccione la política que desea asociar. Opcional. Este campo no se muestra en el caso de los usuarios externos. El sistema calcula la fecha de caducidad a partir de la primera fecha que el usuario inicia sesión con esta contraseña.

Campo	Descripción
Host de autenticación (sólo autenticación externa)	El servidor LDAP (Lightweight Directory Access Protocol) en el que se autentica el servidor. El servidor o los servidores listados en este campo se especifican en el archivo authentication_policy.properties.in.
Tiempo de espera de sesión	Cantidad de tiempo en minutos durante la cual puede permanecer inactivo antes de volver a iniciar sesión. El tiempo se expresa en minutos. Campo necesario.
Accesibilidad	Parte de la interfaz de usuario del panel de instrumentos a la que tiene acceso la cuenta de usuario. Campo opcional. Se encuentran disponibles las opciones de accesibilidad siguientes: • IU Admin – Accede al panel Consola de administración del panel de instrumentos solamente. • IU AS2 – Accede a la interfaz AS2 Edition solamente. • IU de panel de instrumentos – Accede a la interfaz del panel de instrumentos. Se perfecciona seleccionando un tema de panel de instrumentos.
Tema del panel de instrumentos	Panel de instrumentos predefinidos al que tiene acceso la cuenta de usuario. Obligatorio si la accesibilidad se establece como IU de panel de instrumentos. Se encuentran disponibles las opciones de tema de panel de instrumentos siguientes: • Predeterminado • Operador • Participante • Patrocinador del participante • Patrocinador • AFT
Nombre de pila	El nombre del usuario. Campo necesario.
Apellido	El primer apellido del usuario. Campo necesario.
Correo electrónico	Dirección de correo electrónico del usuario.
Localizador	Número de localizador del usuario.
Idioma preferido	Establezca el valor en **Usar valores de la aplicación cliente**. **Nota:** Este valor indica a Sterling B2B Integrator que utilice el idioma especificado en el navegador del usuario y/o el entorno local del sistema operativo del cliente. **Nota:** Es el valor predeterminado.
ID de gestor	ID de usuario del gestor del usuario

Campo	Descripción
Identidad	Identidad del socio comercial que debe asociarse con la cuenta de usuario. Sólo se puede asociar un socio comercial con una cuenta de usuario. Una cuenta de usuario puede asociarse con muchos grupos, cada uno con su propia asociación de identidad de socio comercial. Este permite asociar una cuenta de usuario con más de un socio comercial. El campo Identidad se utiliza para direccionar mensajes en el buzón. Seleccione una identidad de socio comercial de la lista. El valor por defecto es la organización Hub.

Para crear una cuenta de usuario:

Procedimiento

1. En el menú **Administración**, seleccione **Cuentas** > **Cuentas de usuario**.
2. Junto a **Crear una nueva cuenta**, pulse **Ir**
3. En la página Nueva cuenta, seleccione el **tipo de autenticación**.
4. Entre el **ID de usuario**.
5. Entre la **Contraseña**.
6. Confirme la contraseña.
7. Seleccione la **política**.
8. Especifique el **tiempo de espera de la sesión**.
9. Seleccione la **accesibilidad**.
10. Seleccione el **tema del panel de instrumentos**.
11. Pulse **Siguiente**.
12. En la página Clave de usuario autorizado SSH, asigne una o más claves públicas. Mueva las claves del panel **Disponible** al panel **Asignado** y pulse **Siguiente**.
13. En la página Grupos, asigne grupos de permisos. Mueva los nombres de grupo desde el panel **Disponibles** al panel **Asignados** y pulse **Siguiente**.
14. En la página Permisos, asigne permisos individuales. Mueva los permisos desde el panel **Disponibles** al panel **Asignados** y pulse **Siguiente**. De forma predeterminada, los permisos asociados con los grupos a los que está asignado este usuario ya están seleccionados. Los permisos necesarios son el permiso de aplicación web de administrador y MyAccount.
15. En la página Información de usuario, especifique el **nombre de pila**.
16. Especifique el **apellido**.
17. Especifique la **dirección de correo electrónico**.
18. Especifique el **número del localizador**.
19. Seleccione el **idioma preferido**. Seleccione el valor **Usar valores de la aplicación cliente**.

    Nota: Este valor indica a Sterling B2B Integrator que utilice el idioma especificado en el navegador del usuario y/o el entorno local del sistema operativo del cliente.
20. Especifique el **ID de gestor**.
21. Seleccione la **identidad**.
22. Pulse **Siguiente**.

23. Revise los valores de la cuenta de usuario.
24. Pulse **Finalizar**. Se crea la cuenta de usuario y se muestra el mensaje siguiente:

    ```
    La actualización del sistema se ha realizado correctamente.
    ```

    Si ha creado un usuario externo, cierre sesión en el sistema y, a continuación, vuelva a iniciar sesión con el ID o la cuenta del usuario externo. El sistema autenticará el ID de usuario externo en el servidor LDAP externo.

Editar cuentas de usuario

Puede editar una cuenta de usuario desde el menú **Administración**.

Acerca de esta tarea

Nota: Aunque se soportan varios idiomas, una cuenta de usuario no se debe utilizar con más de un idioma específico para evitar problemas de visualización de interfaz de usuario.

Para editar una cuenta de usuario:

Procedimiento

1. En el menú **Administración**, seleccione **Cuentas** > **Cuentas de usuario**.
2. Localice la cuenta de usuario que desea editar utilizando las opciones Buscar o Lista.
3. Pulse **editar** para la cuenta de usuario que desea editar.
4. Realice los cambios en el tipo de autenticación para este usuario.

   Si cambia el tipo de autenticación de externa a local, tendrá que crear una contraseña para el usuario. Si cambia el tipo de autenticación de local a externo, no puede cambiar la contraseña del usuario o política de contraseñas.
5. Realice los cambios en la **Nueva contraseña** y confirme la nueva contraseña.
6. Realice los cambios en la **Política**.
7. Realice los cambios en el **Tiempo de espera de sesión** y pulse **Siguiente**.
8. Realice los cambios en **Clave de usuario autorizado SSH** y pulse **Siguiente**.
9. Realice los cambios de grupos y pulse **Siguiente**.
10. Realice los cambios de permisos y pulse **Siguiente**.

    No puede eliminar el permiso de aplicación web de administración o MyAccount.
11. Realice los cambios en la información de usuario y pulse **Siguiente**.

    Nota: Para las cuentas de usuario que se visualizan la interfaz de usuario en otro idioma soportado, verifique el valor de idioma preferido esté establecido en **Usar valores de la aplicación cliente**. Este valor indica a Sterling B2B Integrator que utilice el idioma especificado en el navegador del usuario y/o el entorno local del sistema operativo del cliente.
12. Revise los valores de la cuenta de usuario.
13. Pulse **Finalizar**.

Suprimir cuentas de usuario

Puede suprimir una cuenta de usuario desde el menú **Administración**.

Acerca de esta tarea

Para suprimir una cuenta de usuario:

Procedimiento

1. En el menú **Administración**, seleccione **Cuentas** > **Cuentas de usuario**.
2. Localice la cuenta de usuario que desea suprimir utilizando las opciones Buscar o Lista.
3. Pulse **Suprimir** para la cuenta de usuario que desea suprimir.
4. Pulse **Aceptar**.
5. Revise los valores de la cuenta de usuario.
6. Pulse **Suprimir**. La cuenta de usuario seleccionada se suprime y se visualiza este mensaje:

   ```
   La actualización del sistema se ha realizado correctamente.
   ```

Actualizar la información de Mi cuenta

La información de Mi cuenta está asociada con el nombre de usuario y la contraseña, de modo que al iniciar la sesión se visualiza la información personal en la página Mi cuenta. Puede editar su propia información de cuenta y cambiar la página inicial que aparece al iniciar la sesión en el sistema.

Acerca de esta tarea

Hay muchos casos en los que la información de cuenta personal cambia obligándole a editar la información de cuenta. Además, puede que tenga que cambiar la contraseña por razones de seguridad.

Nota: Aunque se soportan varios idiomas, una cuenta de usuario no se debe utilizar con más de un idioma específico para evitar problemas de visualización de interfaz de usuario.

Para actualizar la información de cuenta:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Mi cuenta**.
2. Si desea actualizar su contraseña de cuenta, en el campo **Contraseña antigua**, entre la contraseña actual y escriba una contraseña nueva en el campo **Nueva contraseña**. Entre la nueva contraseña otra vez en el campo **Confirmar nueva contraseña**.
3. Entre los cambios en los campos **Nombre**, **Apellido**, **Correo electrónico** o **Localizador**.
4. Para cambiar las **Claves de usuario autorizadas SSH** asignadas a esta cuenta, mueva las claves del panel Disponible al panel Asignado.
5. Para cambiar el **Idioma preferido**, seleccione un idioma.

   Nota: Para las cuentas de usuario que visualizan la interfaz de usuario en otro idioma soportado, verifique que el valor esté establecido en **Usar valores de la aplicación cliente**. Este valor indica a Sterling B2B Integrator que utilice el idioma especificado en el navegador del usuario y/o el entorno local del sistema operativo del cliente.
6. Para cambiar la **Página de bienvenida** (inicio de consola de administración) que se visualiza al iniciar la sesión, realice una selección en la lista.

7. Para cambiar el número de procesos visualizados a la vez en la página Procesos actuales, seleccione un nuevo valor para **Tamaño de la página para los procesos actuales**.
8. Para cambiar el número de documentos visualizados a la vez en la página Documentos actuales, seleccione un nuevo valor para **Tamaño de la página para los documentos actuales**.
9. Si desea reutilizar las ventanas de navegador para iniciar atajos, seleccione **Reutilizar ventanas para iniciar atajos**.
10. Si desea que el sistema realice búsquedas automáticamente basándose en series que ha especificado anteriormente, seleccione **Completar automáticamente para búsquedas**.
11. Si desea que el sistema recuerde los valores de búsqueda, seleccione **Recordar buscar por valores**. Esta opción guarda el último valor que escribió en cada uno de los campos de búsqueda.
12. Pulse **Guardar**. La nueva información de cuenta se guarda y se visualiza este mensaje:

    ```
    La actualización se realizó correctamente.
    ```

Salidas de cuenta de usuario para inicio de sesión (V5.2.5 y posterior)

Sterling B2B Integrator proporciona salidas de usuario de sincronización de Active Directory, que puede utilizar para gestionar las cuentas de usuario con Active Directory en lugar de la interfaz de usuario de Sterling B2B Integrator. Estas salidas de usuario las puede configurar IBM Services durante la fidelización de clientes de IBM Services. Para obtener más información, póngase en contacto con el representante de ventas de IBM.

Salida de usuario	Descripción
IUserLoginUserExit_preAuthenticate	Se utiliza para insertar código personalizado antes de la autenticación.
IUserLoginUserExit_postAuthenticateFail	Se utiliza para insertar código personalizado después de una autenticación con éxito.
IUserLoginUserExit_postAuthenticateSuccess	Se utiliza para insertar código personalizados después de una autenticación fallida.

Salidas de usuario de cuenta de usuario para cierre de sesión (V5.2.6 y superior)

Sterling B2B Integrator proporciona salidas de usuario de sincronización de Active Directory, que puede utilizar para gestionar las cuentas de usuario con Active Directory en lugar de la interfaz de usuario de Sterling B2B Integrator. Estas salidas de usuario las puede configurar IBM Services durante la fidelización de clientes de IBM Services. Para obtener más información, póngase en contacto con el representante de ventas de IBM.

Salida de usuario	Descripción
ILogoutUserExit_OnSessionInvalidate	Se utiliza para insertar código personalizado antes de que se invalide la sesión.

Inicio de sesión único

Inicio de sesión único

El inicio de sesión único (SSO) es un proceso de autenticación que permite a los usuarios acceder a varias aplicaciones y tener que entrar sólo un nombre de usuario y una contraseña. Anteriormente, un usuario que se conectaba a cada aplicación y tenía que gestionar varios nombres de usuario y contraseñas.

La autenticación de usuario para SSO no necesita el adaptador LDAP, que se utiliza con los procesos de negocio para comunicarse con los servidores LDAP locales o remotos utilizando JNDI (Java Naming Directory Interface).

Sterling B2B Integrator permite el SSO mediante la integración con Netegrity SiteMinder o a través de clases de implementación personalizadas para plug-ins SSO en otras aplicaciones y servidores de inicio de sesión único.

El inicio de sesión único está limitado a los componentes siguientes:

- Interfaz de administración
- Interfaz de buzón
- Interfaz de panel de instrumentos
- Interfaz de Transferencia avanzada de archivos (AFT)
- Interfaz MyAFT

Clase predeterminada de proveedor de inicio de sesión único

El URL de inicio de sesión SSO para todas las interfaces excepto la del panel de instrumentos es similar al de la interfaz de inicio de sesión normal. El URL de interfaz de panel de instrumentos es http:Host:puerto/dashboard/sso.jsp. La cabecera de solicitud para la interfaz de panel de instrumentos debe tener el valor SM_USER=Nombre de usuario SSO (o el valor se puede configurar en el archivo security.properties bajo SSO_USER_HEADER).

La interfaz SSOProviderDefault permite que el plug-in de inicio de sesión único (SSO) maneje la función de inicio de sesión único para Netegrity SiteMinder.

Puede configurar el SSO para redirigir a una página HTTP externa (en lugar de la página de cierre de sesión de Sterling B2B Integrator) después de que el usuario se haya desconectado de una sesión de SSO. La página externa del servidor SSO puede ser una página de inicio de sesión o cierre de sesión.

El ejemplo siguiente muestra la clase SSOProviderDefault.java:

```
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.*;
/**
 * Implementación de inicio de sesión único predeterminada para
 * ISSOProvider que utilizará
* Cabecera de solicitud para obtener SSO_USER
 *
 * @author nombre de desarrollador
 */
```

```
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();
/**
* Autenticar proceso SSO (inicio de sesión)
*
* @param Request : La solicitud http.
*
* @return String : El ID de usuario SSO si se pasa la autenticación
*                : nulo si se rechaza la autenticación
* << No se genera ninguna excepción para el proveedor SSO predeterminado
* - Tiene valor o es nulo >>
*/
public String authenticate(HttpServletRequest request)
                        throws SSOAuthenticationException, SSOException
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (AUTHLOG.debug) {
          AUTHLOG.logDebug(CLASS_NAME + " Código de usuario autenticado : " +
              SecurityManager.getInstance().getSSOAuthenticationHeader() +
              " value : " + sso_user);
    }
    return sso_user;
}
/**
 * Proceso de SSO de AuthenticatePage  (Página)
 *
 * @param Request : La solicitud http.
*
 * @return boolean : Verdadero (True) si se pasa la autenticación SSO en la página
 *                   o no se necesita
 *                   autenticación de página porque no se ha habilitado o no es
 *                   usuario SSO.
 *                 : Falso (False) si se rechaza la autenticación
 *                   (Debe generar SSOException si se devuelve false)
 */
public boolean authenticatePage(HttpServletRequest request)
                           throws SSOAuthenticationException, SSOException
{
    return true; // Pasar siempre la validación de página para SSOProviderDefault
    /*****  Eliminar signo de comentario si se desea realizar comprobación de
    SSO_USER_HEADER (SM_USER) en página
    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;   ******/
}
/**
 * Cuando el usuario cierra la sesión, se llama esto para realizar acciones
 * adicionales
*
 * @param Response : La respuesta http
 * @param Request : La solicitud http.
 * @param int reason : ID para indicar desde dónde se ha realizado la llamada
* @param String: La serie identifica el tipo de sesión: WS, DASHBOARD, MAILBOX,
 *            AFT, MYAFT o nulo si no se conoce
*
 * @return boolean : Verdadero (True) si se ejecuta satisfactoriamente,
```

```
 *           Falso (False) si no es así y se debe utilizar lógica de cierre de
 *           sesión predeterminada
 *
 */
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 {  // Otras razones : enviar todo a 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 {
           // Tiempo de espera de panel de instrumentos - Utilizar JSP para
           salir de 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; // Establecido en falso, es necesario manejar
                            redirección en JSP
           } else {
              response.sendRedirect(response.encodeRedirectURL(forwardUrl));
           }
       } catch (Exception e) {
           return false;
       }
       return true;
   }
   return false;   // Utilizar lógica predeterminada (es decir: Página de
                      cierre de sesión/inicio de sesión de GIS)
}
}
```

Componentes de plug-in de inicio de sesión único

Sterling B2B Integrator permite una clase de implementación personalizada para plug-ins de inicio de sesión único (SSO) en otros servidores y aplicaciones de inicio de sesión único. Debe añadir una clase de implementación SSO_AUTHENTICATION_CLASS.<n>=<Nueva entrada de clase> en el archivo security.properties para implementar un plug-in SSO.

Puede escribir clases de implementación personalizadas para los plug-ins SSO basándose en la siguiente clase de interfaz ISSOProvider.java.

Clase de interfaz SSOProvider.java

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

SSOException class

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

SSOAuthenticationException class

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

Método de autenticación de usuario

El método de autenticación se inicializa durante el inicio de sesión. El método de autenticación devuelve el ID de usuario después de una autenticación satisfactoria. Se genera una excepción SSOAuthenticationException para una autenticación no satisfactoria. La excepción debe contener un código de razón apropiado y una página de redirección a manejar si existen cabeceras SSO. Si no hay cabeceras SSO, se devuelve el control a la pantalla de inicio de sesión del sistema.

Método de autenticación de página

Se inicializará el método authenticatePage en cada página. En este método se maneja cualquier validación adicional durante la transición de página desde el servidor SSO. Por ejemplo, puede ejecutar ping en el servidor SSO para comprobar si la sesión SSO ha excedido el tiempo de espera. En el caso de una autenticación no satisfactoria, se generará una excepción, que deberá contener un código de razón apropiado y una página de redirección.

Solicitudes SSO que no son válidas

El método de invalidación se inicializa cuando el usuario finaliza la sesión, no puede autenticar el inicio de sesión o una página o cuando caduca la sesión. Se debe ejecutar el método de redirección HTTP para invalidar solicitudes SSO. En el caso de una autenticación no satisfactoria, se inicializan los métodos siguientes:

- Si la autenticación de servidor SSO es satisfactoria y la autenticación de Sterling B2B Integrator no es satisfactoria, se inicializa el método REASON_GIS_AUTHENTICATION_FAILURE con el código de razón.
- Sola autenticación de servidor SSO no es satisfactoria, se inicializa el método REASON_SSO_AUTHENTICATION_FAILURE con el código de razón.

- Si el usuario finaliza la sesión, se inicializa el método REASON_LOGOUT con el código de razón.
- Si la sesión HTTP caduca, se inicializa el método REASON_HTTP_SESSION_EXPIRED con el código de razón.
- Si la sesión SSO del usuario caduca, se inicializa el método REASON_SSO_SESSION_EXPIRED con el código de razón.

Inicio de sesión único con lista de comprobación de Netegrity SiteMinder

Para poder configurar el Inicio de sesión único (SSO), debe conocer SSO y Netegrity SiteMinder.

Utilice esta lista de comprobación para configurar SSO con Netegrity SiteMinder:

Tarea	Inicio de sesión único con lista de comprobación de Netegrity SiteMinder	Notas
1	Instalar Netegrity SiteMinder y configurarlo con un servidor proxy inverso.	
2	Configurar los archivos de propiedades para utilizarlos con Netegrity SiteMinder.	
3	Configurar el servidor proxy seguro de Netegrity.	
4	Crear reinos seguros de servidor de Netegrity.	

Para la implementación personalizada de los plug-ins SSO para otras aplicaciones y servidores de inicio de sesión único, consulte Componentes de plug-in de inicio de sesión único.

Inicio de sesión único con IBM Global High Availability Mailbox (V5.2.6 o posterior)

Los usuarios de Sterling B2B Integrator con los permisos adecuados pueden acceder directamente a la herramienta de gestión de IBM® Global High Availability Mailbox mediante el inicio de sesión único desde Sterling B2B Integrator para gestionar Global Mailbox.

Antes de empezar

Los usuarios de Sterling B2B Integrator deben pertenecer a uno de los grupos siguientes para acceder directamente a la herramienta de gestión de Global Mailbox desde Sterling B2B Integrator:

- *MAILBOX*
- *El despliegue*
- *Mailbox Administrators*
- *Sterling B2B Integrator Admin*

Acerca de esta tarea

Cuando elige acceder a la herramienta de gestión de Global Mailbox mediante inicio de sesión único, la nueva sesión de Global Mailbox se abre en una ficha de navegador web, mientras la sesión de Sterling B2B Integrator permanece disponible.

Puede acceder a Global Mailbox mediante un inicio de sesión único únicamente desde Sterling B2B Integrator. Si cierra la sesión de la herramienta de gestión de Global Mailbox, no ha cerrado la sesión de Sterling B2B Integrator.

Si desea cambiar la contraseña de administrador de Global Mailbox, debe iniciar la sesión directamente en la herramienta de gestión de Global Mailbox.

Restricción: Si inicia la sesión en la herramienta de gestión de Global Mailbox, no puede cambiar la contraseña de administrador de Global Mailbox, y **Cambiar contraseña**, en el menú **Administrador**; no está disponible.

Para acceder a la herramienta de gestión de Global Mailbox mediante inicio de sesión único:

Procedimiento

1. En la página Consola de administración, expanda **Despliegue** en el Menú de administración.
2. Expanda **Global Mailbox**.
3. Seleccione **Administración de buzones**.
4. Pulse el hiperenlace **Iniciar herramienta de gestión de Global Mailbox** para abrir una nueva sesión en la herramienta de gestión de Global Mailbox.

   Recuerde: Cuando pulsa el hiperenlace **Iniciar herramienta de gestión de Global Mailbox**, se abre una nueva sesión de Global Mailbox en una ficha de navegador web nueva.

Configurar archivos de propiedades para el inicio de sesión único con Netegrity SiteMinder

Puede configurar archivos de propiedades para el inicio de sesión único con Netegrity SiteMinder.

Acerca de esta tarea

Para editar los archivos neo-ui.properties y security.properties:

Procedimiento

1. Detenga Sterling B2B Integrator.
2. Vaya a */dir_instalación*/install/properties.
3. Abra el archivo neo-ui.properties.
4. Añada la entrada SSO asociada para cada interfaz. El siguiente ejemplo de código muestra la entrada asociada a los mismos sitios HTTP:

```
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. Guarde y cierre el archivo neo-ui.properties.
6. Abra el archivo */dir_instalación*/install/properties/security.properties en un editor de texto.
7. En security.properties, localice los parámetros de configuración de autenticación ## SSO, como se muestra en el siguiente ejemplo de código:

```
## Configuración de autenticación SSO
## habilitar autenticación sso  (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true
## habilitar autenticación sso en cada página (true, false) default=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false
## variable de cabecera http que contiene el id de usuario autenticado externamente
SSO_USER_HEADER=SM_USER
## Lista de clases SSOProvider proporcionadas para utilizarse - Si la autenticación SSO es
## habilitar, debe tener como mínimo una clase, lo siguiente es el valor predeterminado que
## se proporciona.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Intentará utilizar ésta primero
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Intentará utilizar ésta si la primera
## ha fallado
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Intentará utilizar ésta si la segunda
## también ha fallado
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Intentará utilizar ésta si todas
## las primeras clases –1 han fallado
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS OProviderDefault
## Página externa para SSO cuando finaliza la sesión (Especificar la página externa de servidor SSO
## para cada uno de los casos)
## Ejemplo: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## Después de la finalización de sesión de usuario SSO del Buzón, en lugar de visualizar la pantalla
## de inicio de sesión de buzón se visualiza la página web de IBM.
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=
## Manejo predeterminado para LOGOUT si no conoce el origen
SSO_FORWARD_URL.LOGOUT=
## Página externa para SSO cuando se excede el tiempo de espera (Especificar la página externa de
## servidor SSO para cada ## del caso)
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=
## Manejo predeterminado para TIMEOUT si no conoce el origen
SSO_FORWARD_URL.GIS_TIMEOUT=
## Página externa para SSO en anomalía de validación/autenticación (la validación de usuario SSO
## ha fallado - En inicio de sesión o la validación de página)
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=
##Manejo predeterminado para VALIDATION FAILED si no conoce el origen
SSO_FORWARD_URL.VALIDATION_FAILED=
```

8. Bajo la entrada de configuración de autenticación ##SSO, realice los cambios siguientes en los parámetros SSO:

Parámetro	Descripción	Valor enviado	Valor nuevo
SSO_AUTHENTICATION_ENABLED	Habilita o inhabilita el uso de SSO.	False (falso)	True (verdadero)
SSO_USER_HEADER	Nombre de cabecera de usuario de Netegrity SiteMinder o configuración de aplicación SSO.	SM_USER Es el valor en Netegrity SiteMinder.	Debe coincidir con la entrada en Netegrity SiteMinder o la aplicación SSO.

Parámetro	Descripción	Valor enviado	Valor nuevo
SSO_PAGE_ AUTHENTICATION_ ENABLED	Habilita o inhabilita la autenticación SSO en cada página	False (falso)	True (verdadero) – Para autenticar SSO en cada página. Cámbielo sólo si se proporciona la clase de proveedor SSO personalizada.
SSO_AUTHENTICATION_ CLASS.n	Clase de implementación para proporcionar soporte de autenticación.	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	Seleccionar en la lista de clases SSOProvider proporcionadas.
SSO_FORWARD_ URL URL	Visualiza la página de URL proporcionada después de finalizar la sesión de buzón. De lo contrario, visualiza el valor predeterminado.	Comentado Visualiza la página predeterminada.	Proporcionar el URL.

9. Guarde y cierre el archivo security.properties.
10. Inicie Sterling B2B Integrator.

Configurar el servidor proxy seguro de Netegrity

Puede configurar el servidor de proxy seguro de Netegrity añadiendo reglas de reenvío al archivo proxyrules.xml.

Acerca de esta tarea

Antes de configurar el servidor proxy seguro de Netegrity, debe:

- Instalar Sterling B2B Integrator en un servidor como acme.si.com.
- Conocer el número de puerto en el que está instalada la MBI (Interfaz de navegador de buzón). Debe utilizar esta información en las reglas de reenvío adecuadas.
- Conocer el número de puerto en el que está instalada la interfaz de usuario de panel de instrumentos de Sterling B2B Integrator. Debe utilizar esta información en las reglas de reenvío adecuadas.

Para configurar el servidor proxy seguro de Netegrity:

Procedimiento

1. Añada las reglas de reenvío necesarias para Sterling B2B Integrator al archivo /opt/netegrity/proxy-engine/conf/proxyrules.xml.

   El ejemplo siguiente muestra qué aspecto debe tener el archivo proxyrules.xml completado después de añadir las reglas de reenvío para acceder a los componentes de Sterling B2B Integrator:

```
<?xml version="1.0"?>
<?cocoon-process type="xslt"?>
<!DOCTYPE nete:proxyrules SYSTEM "file:////home/netegrity/proxy-engine/conf/dtd/proxyrules.dtd">
<!-- Reglas de proxy -->
<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. Añada lo siguiente a las líneas en el archivo proxyrules.xml para desactivar la comprobación de scripts de servidor cruzados en el servidor proxy seguro, puesto que Sterling B2B Integrator no soporta la imposición de política de scripts de servidor cruzados de Netegrity.

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

3. Guarde y cierre el archivo proxyrules.xml.

Crear reinos seguro de servidor de políticas de Netegrity

El administrador de servidor de políticas de Netegrity debe crear dominios seguros alrededor de cada uno de los patrones de URL que el servidor proxy seguro reenvía. Estos reinos de seguridad deben tener las reglas necesarias asignadas para la autenticación y autorización.

Acerca de esta tarea

Además, el agente web del servidor proxy seguro debe estar configurado para comunicarse con el servidor de políticas.

Cree un reino seguro para cada patrón de URL listado:

Patrón de URL	Permite acceder a:
/mbi/*	Interfaz de buzón de aplicación
/dashboard/*	Interfaz de panel de instrumentos de aplicación, utilizando el formato http://host:puerto/panel de instrumentos
/datastore/*	Componentes de almacén de datos
/portlets/*	Componentes de portlet de aplicación en la interfaz de panel de instrumentos
/help/*	Componentes de ayuda según contexto
/webxtools/*	Programas de utilidad de Extensiones web
/gbm/*	Componentes de Modelador de procesos gráficos

Contraseñas

Políticas de contraseñas

Las políticas de contraseñas son conjuntos de decisiones de seguridad que se toman y se aplican a diferentes cuentas de usuario de acuerdo con las políticas de seguridad de la empresa. Estas opciones incluyen elementos tales como el número de días que una contraseña es válida y la longitud máxima y mínima de una contraseña.

Puede utilizar políticas de contraseñas para agilizar las operaciones de seguridad cuando se añaden nuevos usuarios. En lugar de tener que añadir políticas individuales para cada usuario individual, puede crear una política de contraseñas y aplicarla a todos los usuarios que necesitan el mismo acceso.

Después de crear una política de contraseñas, puede aplicarla sólo a las cuentas de usuario internas. Esto le proporciona la mayor flexibilidad en el mantenimiento de las políticas de seguridad. Si está utilizando LDAP, no puede aplicar políticas de contraseñas para las cuentas externas.

Los valores predeterminados para la política de contraseñas son:

Parámetro	Valor predeterminado
ID de política	default_user
Nombre de política	Política de usuario predeterminada
Número de días de validez	60
Longitud mínima	6
Longitud máxima	28
Número de contraseñas conservadas en el historial	5
Contraseña necesaria para contener caracteres especiales	Seleccionado
Cambio de contraseña necesario en el primer intento de inicio de sesión	Seleccionado

Las tareas de políticas de contraseñas incluyen:

- Crear una política de contraseñas
- Buscar una política de contraseñas

- Editar una política de contraseñas
- Suprimir una política de contraseñas
- Editar el parámetro de bloqueo
- Editar el mensaje de caducidad de contraseña

Política de contraseñas personalizada

La política de contraseñas personalizada de Sterling B2B Integrator es una característica de seguridad que añade más reglas de políticas de contraseña. Estas reglas de contraseña adicionales pueden ayudarle a evitar que se utilicen contraseñas débiles que se pueden piratear fácilmente y rechazar contraseñas que no cumplen con los estándares.

Para habilitar esta funcionalidad, necesita:

- Implementar un código Java personalizado a través de un punto de conexión. Una vez habilitado, el punto de conexión se utiliza para todos los usuarios del sistema asociado a una política de contraseña (este es un valor global).
- Añadir la propiedad passwordPolicyExtensionImpl al archivo customer_overrides.properties.
- Aplicar la política de contraseñas personalizada a las cuentas de usuario.

La extensión de política de contraseñas predeterminada se aplica antes que la política de contraseñas predeterminada. Si una contraseña viola más de un requisito de política (impuesto por la clase de extensión y otro impuesto por la implementación predeterminada), sólo se visualiza al usuario el mensaje de error devuelto desde la clase de extensión.

Ejemplo de política de contraseñas

Este ejemplo muestra una posible configuración de la política de contraseña.

Por ejemplo, una política de contraseñas denominada Test puede tener los valores siguientes para un contraseña:

- Válida durante 10 días
- Longitud mínima de 10 caracteres
- Longitud máxima de 20 caracteres
- Debe tener al menos dos caracteres especiales
- El usuario debe cambiar la contraseña predeterminada durante el inicio de sesión inicial
- Número de contraseñas a conservar en el historial

Utilizando el ejemplo anterior, el administrador del sistema asigna al usuario un nombre de usuario y una contraseña. El usuario inicia la sesión utilizando el nombre de usuario y la contraseña proporcionados y se le solicita que cambie la contraseña. Si el usuario no proporciona una contraseña con un mínimo de 10 caracteres, con más de 20 caracteres o sin dos caracteres especiales como mínimo, el sistema solicita al usuario que realice correcciones. Una vez que el usuario ha cumplido todas las condiciones establecidas en la política de contraseña cambiando la contraseña, el sistema guarda la nueva contraseña y permite el acceso al usuario. Cada cuenta de usuario sólo puede tener una política de contraseña asociada, pero se puede aplicar una política de contraseña a varias cuentas de usuario.

Además de los cambios de política de contraseña en la interfaz, puede cambiar el número de veces que un usuario puede fallar el intento de inicio de sesión correcto antes de que se bloquee la cuenta del usuario que está intentando iniciar la sesión.

Por ejemplo, si el número de intentos de inicio de sesión consecutivos antes de fallar se ha establecido en tres y escribe una contraseña incorrecta tres veces, no podrá iniciar la sesión utilizando ese sistema específico. Puede iniciar la sesión utilizando cualquier otro sistema que tenga acceso al sistema.

Contraseña o frase de contraseña de instalación

Durante la instalación, se crea una frase de contraseña de sistema para la instalación de Sterling B2B Integrator. La frase de contraseña es una serie muy compleja que tiene más de 16 caracteres. La frase de contraseña de sistema es necesaria para iniciar el sistema y para acceder a la información de sistema protegida.

La única persona que puede actualizar o cambiar la frase de contraseña es la persona que ha creado/instalado el software. Si pierde u olvida la contraseña, no podrá iniciar el sistema. El único usuario que puede actualizar la frase de contraseña de sistema es el usuario que ha realizado la instalación.

El sistema no almacena la frase de contraseña de sistema, excepto en instalaciones Windows, donde se almacena de una forma enmascarada en security.properties para facilitar que el sistema se ejecute como un servicio no interactivo. Se puede almacenar sin peligro en otras plataformas en security.properties, de modo que no tiene que entrarla en la línea de mandatos al iniciar el sistema. Sin embargo, la frase de contraseña de sistema sólo está protegida por el control de accesos de archivo de sistema operativo.

Lista de comprobación de contraseña de política personalizada

Puede implementar una contraseña de política personalizada.

Utilice la lista de comprobación siguiente para implementar una política de contraseña personalizada:

Tarea	**Lista de comprobación de contraseña de política personalizada**
1	Cree una estructura de directorios en <Dir_instalación_SI> para prueba, política y extensión.
2	Cree la clase java en el directorio de extensión.
3	Especificar la clase Java que implementa la política de contraseña (propiedad passwordPolicyExtensionImpl) en el archivo customer_overrides.properties.
4	Añadir el archivo jar de clase de implementación a la vía de acceso de clases.
5	Definir mensaje de error.

Ejemplo - Contraseña de política personalizada

Este ejemplo muestra una extensión de contraseña de política personalizada.

Aquí se muestra un ejemplo de extensión de contraseña de política personalizada.

La interfaz com.sterlingcommerce.woodstock.security.PasswordPolicyExtension se ha añadido al sistema de la manera siguiente:

```
public interface IPasswordPolicyExtension {
    /**
     * Implementa la validación ampliada en las contraseñas y
devuelve nulo si la validación de contraseña
     * es satisfactoria. Si la validación falla,
se deberá
     * devolver una clave de mensaje de error que se puede
buscar en Login_*.properties*.
     * @param password - La serie de contraseña a validar
     * @param policyId - PWD_POLICY.POLICY_NAME de
la política asociada con el usuario, en caso de que la extensión
la necesite.
     * @return String Devolver nulo si la validación de contraseña
ha sido satisfactoria, la clave de mensaje de error si falla la validación de contraseña
     */
    public String validateNewPassword (String password,
String policyName);
}
```

La devolución de nulo desde el método indica que se ha aceptado la contraseña. La devolución de cualquier otra cosa significa que la contraseña no era válida.

Ejemplo de implementación

```
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) {
           // Comprobaciones de validación de contraseña adicionales
                  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";
      }

}
```

Buscar políticas de contraseñas

Puede buscar una política de contraseñas desde el menú **Administración**.

Acerca de esta tarea

Para buscar una política de contraseñas:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Política de contraseñas**.
2. En la página Política de contraseñas, realice una de las acciones siguientes:
   - Bajo Buscar en el campo **Nombre de política de contraseña**, entre una parte del nombre o el nombre completo de la política de contraseñas que está buscando y pulse **Ir** La página Política de contraseñas lista todos los permisos que coinciden con los criterios de búsqueda.

- Bajo Lista en el campo **Alfabéticamente**, seleccione **TODOS** o la letra por la que empieza el nombre de la política de contraseñas que está buscando y pulse **Ir** La página Política de contraseñas lista todos los permisos que coinciden con los criterios de búsqueda.

Crear políticas de contraseña

Puede crear una política de contraseña para asignar la política a las cuentas de usuario. No es necesario que asocie una política de contraseña con una cuenta de usuario, pero esto ayuda a gestionar la seguridad.

Acerca de esta tarea

Antes de empezar, debe tener la información siguiente:

Campo	Descripción
ID de política	ID que identifica la política de contraseñas en la base de datos.
Nombre de política	Nombre de política que se muestra en la interfaz de usuario cuando se hace cualquier referencia a la política de contraseña.
Número de días de validez	Número de días que una contraseña de usuario es válida. El valor predeterminado es 0, lo que significa que la contraseña no caduca nunca. Si proporciona un valor entre 1 y 999, se solicita al usuario que cambie la contraseña cuando caduque dicho periodo de tiempo. La cuenta atrás de la caducidad se inicia la primera vez que un usuario inicia la sesión después de que se asigne una contraseña a la cuenta de usuario.
Longitud mínima	Longitud mínima que debe tener la contraseña. Campo necesario. Cualquier número es un valor válido. Este número debe estar establecido en el número 6 como mínimo. El valor predeterminado es 6. Si no se aplica ninguna política, el sistema impone una longitud mínima de 6.
Longitud máxima	Longitud máximo que puede tener la contraseña. Campo necesario. Cualquier número es un valor válido. Este número se debe establecer, como mínimo, en el mismo número que la longitud mínima. El valor predeterminado es 28.
Número de contraseñas conservadas en el historial	Número de contraseñas a conservar en la tabla PWD_HISTORY de la base de datos para un usuario. Cuando se supera este número de contraseñas, la contraseña más antigua se elimina de la tabla y el usuario la puede volver a utilizar. El valor predeterminado es 0.
Contraseña necesaria para contener caracteres especiales	Especifica que la contraseña debe contener como mínimo un carácter especial. Los valores válidos son números, letras en mayúsculas, !, @, #, $, %, ^, & o *.
Cambio de contraseña necesario en el primer intento de inicio de sesión	Especifica que el usuario debe cambiar la contraseña predeterminada después del inicio de sesión inicial. Se solicita al usuario que cambie la contraseña después de iniciar la sesión por primera vez.

Para crear una política de contraseñas:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Política de contraseñas**.
2. Junto a **Crear una nueva política de contraseña**, pulse **Ir**
3. En la página Política de contraseñas, entre **ID de política**.
4. Entre el **Nombre de política**.
5. Entre el **Número de días de validez**.
6. Entre la **Longitud mínima**.
7. Entre la **Longitud máxima**.
8. Entre el **Número de contraseñas conservadas en el historial**.
9. Si es necesario que la contraseña contenga caracteres especiales, seleccione el recuadro de selección.
10. Si es necesario que el usuario cambie la contraseña en el primer intento de inicio de sesión, seleccione el recuadro de selección.
11. Pulse **Siguiente**.
12. Revise los valores de política de contraseñas.
13. Pulse **Finalizar**.

Editar políticas de contraseñas

Puede editar la política de contraseñas desde el menú **Administración**.

Acerca de esta tarea

Para editar la política de contraseñas:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Política de contraseñas.**
2. Localice la política de contraseñas que desea editar utilizando las opciones Buscar o Lista.
3. Pulse **editar** para la política de contraseñas que desea editar.
4. En la página Valores de política de contraseñas, realice los cambios adecuados y pulse **Siguiente**.
5. Revise los valores de política de contraseñas.
6. Pulse **Finalizar**.

   Se visualiza el mensaje siguiente:

   ```
   La actualización del sistema se ha realizado correctamente.
   ```

Suprimir políticas de contraseña

Si suprime una política de contraseñas, las cuentas de usuario que están asociadas con dicha política de contraseña específica aún pueden iniciar la sesión, pero el usuario no se ve obligado a cambiar la contraseña. Si el usuario cambia la contraseña, no se realiza ninguna validación en la nueva contraseña.

Acerca de esta tarea

Para suprimir una política de contraseñas:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Política de contraseñas**.

2. Localice la política de contraseñas que desea suprimir utilizando las opciones Buscar o Lista.
3. Pulse **suprimir** para la política de contraseñas que desea suprimir.
4. En la página Confirmar, pulse **Suprimir**.

   Se visualiza el mensaje siguiente:

   ```
   La actualización del sistema se ha realizado correctamente.
   ```

Cambiar el número de días de la caducidad de contraseña de usuario

El sistema le avisa de una inminente caducidad de contraseña poniendo un mensaje en la sección de alertas del sistema de la página de inicio de la consola de administración. Los administradores del sistema pueden cambiar el número de días antes de la caducidad que se notificará a los usuarios.

Acerca de esta tarea

El mensaje indica que la contraseña caducará al cabo de un número específico de días. Cada día, el número se reduce en uno, hasta el día en que caduca la contraseña, momento en que se le solicita que cambie la contraseña.

Los administradores del sistema pueden cambiar el número de días antes de la caducidad en el archivo ui.properties.in. Debe realizar todos los cambios en el archivo ui.properties.in y no en el archivo ui.properties. Si realiza los cambios en el archivo ui.properties y reinicia el sistema, el archivo ui.properties.in sobrescribirá los cambios realizados en el archivo ui.properties.

Para cambiar el número de días para la caducidad de contraseña:

Procedimiento

1. Detenga Sterling B2B Integrator.
2. Vaya a */dir_instalación*/install/properties.
3. Abra el archivo ui.properties.in.
4. Localice la entrada MsgPwdExpires= 15.
5. Cambie el 15 por el nuevo número de días para la caducidad de contraseña de usuario.
6. Guarde el archivo.
7. Vaya a */dir_instalación*/install/bin.
8. Entre **setupfiles.sh**.
9. Reinicie Sterling B2B Integrator. Los cambios realizados en el archivo ui.properties.in se aplican al archivo ui.properties y entran en vigor para todas las cuentas de usuario.

Restablecer su propia contraseña después de bloqueo

Si ha quedado bloqueado, puede iniciar la sesión utilizando otro sistema, esperar 30 minutos a que finalice el bloqueo o ponerse en contacto con el administrador del sistema para que elimine el bloqueo.

Acerca de esta tarea

Si está bloqueado:

- Inicie la sesión utilizando cualquier otro sistema que tenga acceso al sistema.

- Espere 30 minutos segundos y el bloqueo caducará permitiéndole intentar iniciar la sesión utilizando de nuevo el sistema bloqueado.
- Póngase en contacto con el administrador del sistema para que elimine el bloqueo a través de la página Gestor de bloqueos. Esto le permite intentar iniciar la sesión utilizando de nuevo el sistema bloqueado.

Definir mensaje de error para la política de contraseñas personalizada

Puede definir el mensaje de error para una extensión de política de contraseña personalizada.

Acerca de esta tarea

Los mensajes de error informan al usuario de las reglas de contraseña y listan las razones de los cambios de contraseña rechazados. Los mensajes de error de contraseña personalizados se definen en los archivos Login_*dir_idioma*.properties_*ID_exclusivo*_ext. Si no se proporciona texto específico personalizado, se devuelve al usuario el mensaje de error predeterminado. El archivo Login_*id_idioma*.properties_*ID_exclusivo*_ext no forma parte del código de sistema predeterminado. Se debe crear después de la instalación de sistema inicial y llenar para que coincida con el entorno.

Para definir el mensaje de error para una extensión de política de contraseña personalizada:

Procedimiento

1. Vaya al directorio */dir_instalación*/install/properties/lang/*dir_idioma*. Donde *dir_idioma* es el idioma establecido para el entorno local del cliente (por ejemplo en, ja, fr).
2. Edite el archivo Login_*dir_idioma*.properties_*ID_exclusivo*_ext. Donde dir_idioma es el idioma establecido para el entorno local del cliente y <nombre_archivo> es el identificador exclusivo para la nueva extensión de contraseña personalizada. Por ejemplo: Login_en.properties_custompasswd_ext.
3. Añada una entrada al archivo para la condición de error establecida en el archivo de extensión personalizado y defina la serie descriptiva que se debe devolver al usuario. Por ejemplo, nogood = La contraseña debe contener un mínimo de un carácter en minúsculas, un carácter en mayúsculas y un dígito o carácter especial.
4. Guarde y cierre el archivo.

Especificar la extensión de política de contraseñas personalizada en el archivo customer_overrides.property

Puede especificar la clase Java que implementa la extensión de política de contraseñas.

Acerca de esta tarea

Para incorporar la implementación personalizada, es necesario especificar el nombre de clase Java en la propiedad passwordPolicyExtensionImpl del archivo customer_overrides.properties.

Para especificar la clase Java que implementa la extensión de política de contraseñas:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio de propiedades.
3. Edite el archivo customer_overrides.properties.
4. Añada la propiedad passwordPolicyExtensionImpl al final del archivo y entre el nombre de la clase Java que implementa la validación ampliada de las contraseñas. Por ejemplo security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl.
5. Guarde y cierre el archivo.

Añadir el archivo JAR de clase de implementación a la vía de acceso de clases para la política de contraseñas personalizada

Para una política de contraseñas personalizada, debe añadir el archivo JAR de clase de implementación a la vía de acceso de clases.

Acerca de esta tarea

La clase de implementación de extensión se debe compilar y ejecutar con jar de la manera siguiente:

Procedimiento

1. Vaya a *Dir_Intalación_SI*.
2. Entre el mandato siguiente para compilar el archivo de clase personalizada:
   `javac -cp /Dir_Instalación_SI/jar/platform_ifcbase/1_3/platform_ifcbase.jar test/policy/extension/*.java`
3. Cree el archivo jar ejecutando el mandato siguiente desde *Dir_Instalación_SI* :
   `jar cf cualquier_nombre_archivo.jar vía_acceso_absoluta_a_archivo_clase_personalizada.class` donde `cualquier_nombre_archivo.jar` es el nombre del nuevo archivo jar que se creará y donde `vía_acceso_absoluta_a_archivo_clase_personalizada.class` es el nombre del archivo de clase Java de implementación personalizada. Por ejemplo: `jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class`
4. Vaya al directorio *Dir_Intalación_SI*.
5. Entre el mandato siguiente para añadir el archivo jar recién creado a la vía de acceso de clase:
   `./install3rdParty.sh userExit 1_0 -j vía_acceso_a_jar_que_se_creó_en_paso3`
   por ejemplo, `./install3rdParty.sh userExit 1_0 -j Dir_instalación_SI/userExit.jar`

Autenticación LDAP

LDAP (Lightweight Directory Access Protocol) es una herramienta de autenticación para Sterling B2B Integrator

LDAP (Lightweight Directory Access Protocol) es un conjunto de protocolos que se utilizan para acceder a la información almacenada en un directorio de información, que es un directorio LDAP.

Un directorio LDAP es una base de datos, pero no una base de datos relacional, que se utiliza para gestionar la información que se reparte entre varios servidores de una red y que se ha optimizado para el rendimiento de lectura.

Puede utilizar LDAP para delegar la autenticación de una cuenta de usuario externa a un directorio LDAP y para proporcionar autenticación utilizando la misma información de seguridad que se utiliza para otras aplicaciones de la empresa. Si la empresa ya ha adoptado LDAP, puede utilizar los directorios LDAP existentes.

La autenticación de cuenta de usuario no necesita el adaptador LDAP, que se utiliza con procesos de negocio para comunicarse con servidores LDAP locales o remotos utilizando una JNDI (Java Naming Directory Interface).

Si el servidor LDAP no funciona, los usuarios que tienen cuentas internas conservan el acceso; sin embargo, los usuarios que tienen cuentas externas no tienen acceso hasta que el servidor LDAP está funcionando.

Antes de poder configurar LDAP con Sterling B2B Integrator, debe:

- Tener conocimientos de LDAP
- Tener acceso a un servidor LDAP instalado y configurado que contiene información de usuario
- Tener la ubicación del servidor LDAP
- (Para SSL) Tener los certificados de seguridad instalados en el almacén de claves y el almacén de confianza
- Haber creado las cuentas de usuario externas para cada usuario que se autenticará a través del servidor LDAP
- (Para SSL) Tener la ubicación del almacén de claves y el almacén de confianza

Ejemplo: Parámetros de configuración de autenticación LDAP

Este ejemplo muestra los parámetros de configuración de autenticación LDAP.

El ejemplo siguiente muestra los parámetros de configuración de autenticación LDAP:

```
## Configuración de autenticación GIS/LDAP
## propiedades de sistema java ssl opcionales (jsse) para localizar y utilizar
## el almacén de confianza y el almacén de claves
## un conjunto de propiedades de almacén de claves y almacén de confianza para
## toda la configuración LDAP.
# LDAP_SECURITY_TRUSTSTORE=/home/applications/properties/cacerts
# LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# LDAP_SECURITY_KEYSTORE=/home/applications/properties/keystore
# LDAP_SECURITY_KEYSTORE_PASSWORD=password
#########################################################################
#
# Configuración de autenticación GIS
#
#########################################################################
authentication_0.className=com.sterlingcommerce.woodstock.security
.GISAuthentication
authentication_0.display_name=GIS Authentication
#########################################################################
#
# Para la Configuración de autenticación de servidor LDAP adicional,
# copie y pegue el siguiente conjunto de propiedades y elimine el signo de
# comentario de todas las propiedades
# que empiezan por "authentication_<número>". Sustituya la etiqueta <número>
# por el número adicional para el método de autenticación. Por ejemplo:
```

```
# si el último método de autenticación es "authentication_0", debe
# sustituir la etiqueta <número> por "1" para el siguiente método
# de autenticación de LDAP nuevo.
# A continuación, tiene que cambiar cada propiedad con la información
# de servidor LDAP correcta.
#
# Puede comentar o dejar en blanco la propiedad "authentication_<número>
# .security_protocol"
# si no va a utilizar SSL para el protocolo de seguridad.
#
# Las propiedades de autenticación LDAP authentication_1 se deben sustituir si
# el cliente ya ha utilizado la autenticación LDAP como configurada en security
# .properties.
#
#########################################################################
#########################################################################
#
# Configuración de autenticación de <número> de servidor LDAP
#
#########################################################################
# authentication_<número>.className=com.sterlingcommerce.woodstock.security
# .LDAPAuthentication
# authentication_<número>.display_name=LDAP Serveragrona <número>
## enable ldap authentication  (true, false) default=false
# authentication_<número>.enabled=true
## parámetros jndi para conexiones ldap
# authentication_<número>.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
# authentication_<número>.server=acme.inc.com
# authentication_<número>.port=636
# authentication_<número>.security_type=simple
# authentication_<número>.principle=cn=Manager,dc=acme,dc=inc,dc=com
# authentication_<número>.credentials=SecretPassword
## comente o déjelo en blanco en esta propiedad si el servidor no
## va a utilizar SSL para el protocolo de seguridad.
# authentication_<número>.security_protocol=ssl
## parámetros de búsqueda para contraseña de usuario
# authentication_<número>.password_attribute=userPassword
# authentication_<número>.search_root=dc=acme,dc=inc,dc=com
# authentication_<número>.search_filter=(uid=<userid>)
# authentication_<número>.with_user_bind=falseBelow the ##LDAP Authentication
```

Lista de comprobación de configuración de autenticación LDAP

Puede configurar LDAP con Sterling B2B Integrator.

Utilice esta lista de comprobación para configurar LDAP con Sterling B2B Integrator:

Tareas	Lista de comprobación de configuración de LDAP
1	Configurar LDAP en una de las modalidades siguientes: • Modalidad de comparación de contraseña • Modalidad binaria de contraseña
2	Configurar LDAP con Sterling B2B Integrator
3	Verificar configuración de LDAP
4	Opcional. Cifrar contraseñas de LDAP.

Configurar LDAP en modalidad de enlace de contraseña

Puede configurar LDAP en modalidad de enlace de contraseña entrando su **ID de usuario** y **contraseña** desde su cuenta externa.

Acerca de esta tarea

Para configurar LDAP en modalidad de enlace de contraseña:

Procedimiento

Entre el **ID de usuario** y la **contraseña** de la cuenta de usuario externo. El sistema:

- Intenta enlazarse al repositorio LDAP con credenciales que permitan la ejecución de las consultas necesarias.
- Busca el usuario en el directorio LDAP con el ID de usuario apropiado.
- Recupera el nombre distinguido (DN) del usuario del directorio LDAP.
- Intenta enlazarse al repositorio LDAP utilizando el DN y la contraseña del usuario.
- Éxito – El sistema se enlaza al repositorio LDAP como un usuario.
- Error – El sistema no se puede enlazar al repositorio LDAP como un usuario.

Configurar LDAP en modalidad de comparación de contraseña

Puede configurar LDAP en una modalidad de comparación de contraseña.

Acerca de esta tarea

Para configurar LDAP en una modalidad de comparación de contraseña:

Procedimiento

1. Entre el **ID de usuario** y la **contraseña** de la cuenta de usuario externo.
2. El sistema intenta enlazarse al repositorio LDAP con credenciales que permiten la ejecución de las consultas necesarias.
3. El sistema busca el usuario en el directorio LDAP con el ID de usuario correcto.
4. El sistema recupera la contraseña de usuario del directorio LDAP.
5. El sistema compara la contraseña proporcionada por el usuario con la contraseña recuperada del directorio LDAP. Si las contraseñas coinciden, está autenticado y tiene permiso para acceder al sistema. Si las contraseñas no coinciden, no está autenticado y no se le permite el acceso.

Configurar LDAP con Sterling B2B Integrator

Si desea configurar Sterling B2B Integrator para utilizar LDAP, debe editar el archivo authentication_policy.properties.in. También puede utilizar el archivo customer_overrides.properties para establecer valores de propiedad que una instalación de parche no pueda sobrescribir.

Acerca de esta tarea

Para configurar la autenticación LDAP:

Procedimiento

1. Detenga Sterling B2B Integrator.
2. Vaya al directorio de instalación.
3. Vaya al directorio de propiedades.
4. Abra el archivo authentication_policy.properties.in.
5. En authentication_policy.properties.in, localice la entrada de configuración de autenticación de ## GIS/LDAP.

6. Bajo la entrada de configuración de autenticación de ##GIS/LDAP, realice los cambios siguientes en los parámetros LDAP:

Parámetro	Descripción	Valor enviado	Cambiar por
#LDAP_SECURITY_ TRUSTSTORE	Vía de acceso al almacén de confianza local. Debe tener los certificados LDAP necesarios almacenados en el almacén de confianza. No puede utilizar certificados de un socio comercial. Opcional. Sólo se debe usar si se utiliza SSL.	Vía de acceso inactiva	Vía de acceso completa al almacén de confianza local.
#LDAP_SECURITY_ TRUSTSTORE_ PASSWORD	Contraseña que permite el acceso al almacén de confianza local. Opcional. Sólo se debe usar si se utiliza SSL.	changeit	Contraseña que permita el acceso al almacén local.
#LDAP_SECURITY_ KEYSTORE	Vía de acceso al almacén de claves local. Debe tener los certificados LDAP necesarios almacenados en el almacén de claves. No puede utilizar certificados de un socio comercial. Opcional. Sólo se debe usar si se utiliza SSL.	Vía de acceso inactiva	Vía de acceso completa al almacén de claves local.
#LDAP_SECURITY_ KEYSTORE_ PASSWORD	Contraseña que permite el acceso al almacén de claves. keystore.Optional. Opcional. Sólo se debe usar si se utiliza SSL.	password	Contraseña que permita el acceso al almacén de claves local.
#authentication_ <número>. enabled	Habilita o inhabilita el uso de LDAP. False: Todos los usuarios que se crean desde este host de autenticación se inhabilitarán (no podrán iniciar la sesión). True: Se puede acceder a cada usuario interna o externamente, pero no de ambas formas, ya que cada ID de usuario es exclusivo. Este valor no se comprueba cuando es para la autenticación interna.	False (falso)	True (verdadero)
#authentication_<número> .jndi_factory	Nombre de la clase de fábrica que crea el contexto inicial para el proveedor de servicios LDAP. Ésta es la fábrica de contexto estándar que se suministra con el JDK.	com.sun. jndi.ldap. LdapCtx Factory	Ningún cambio

Parámetro	Descripción	Valor enviado	Cambiar por
#authentication_ <número>.server	URL que especifica el nombre de host del servidor LDAP.	Vía de acceso inactiva	URL de host LDAP local.
#authentication_ <número>.port	Número de puerto del servidor LDAP.		
#authentication_ <número>. tipo de seguridad	Método de autenticación que el proveedor debe utilizar. El sistema sólo soporta la autenticación simple.	simple	Ningún cambio
#authentication_ <número>. principio	Identidad del principio que se debe autenticar, que permite al sistema realizar consultas. Este parámetro es el componente de nombre en una solicitud de enlace ASN.1 de LDAP.	cn=Manager, dc=amr, dc=stercomm, dc=com	Información de denominación local.
#authentication_ <número>. credenciales	Contraseña configurada en el repositorio LDAP para el principio LDAP, que permite al sistema para realizar consultas.	SecretPassword	Contraseña local que va con el principio local.
#authentication_ <número>. protocolo_seguridad	Objeto que especifica el protocolo de seguridad que el proveedor debe utilizar.	SSL	Ningún cambio. Este parámetro no está visible si ha elegido no utilizar SSL.
#authentication_ <número>. atributo_contraseña	Nombre del atributo LDAP que contiene la contraseña de usuario. Este parámetro sólo se utiliza si #LDAP_ AUTHENTICATE_ WITH_USER_BIND está establecido en false.	userPassword	Atributo local que contiene la contraseña.
#authentication_ <número>. raíz_búsqueda	Objeto que especifica la raíz en la que se basa la consulta de usuario.	dc=amr, dc=stercomm, dc=com	Vía de acceso de búsqueda local.
#authentication_ <número>.search_filter	Objeto que especifica la plantilla a utilizar en la búsqueda. El valor <id_usuario> se sustituye dinámicamente en tiempo de solicitud con el ID del usuario que solicita la autenticación.	(uid=<id_usuario>)	Un servidor Windows Active Directory puede utilizar una entrada como (sAMAccount Name=<id_usuario>)

Parámetro	Descripción	Valor enviado	Cambiar por
#authentication_ <número>. with_user_bind	Especifica si se debe autenticar un usuario de acuerdo con un enlace satisfactorio. Falso - El sistema extrae el valor de la contraseña de usuario del servidor LDAP y realiza una comparación con las credenciales de usuario proporcionadas. Verdadero - El sistema se enlaza con el servidor LDAP utilizando el nombre distinguido del usuario y las credenciales proporcionadas. Un enlace satisfactorio significa una autenticación satisfactoria.	false	Cámbielo a true si desea autenticar con el enlace de usuario.

7. Guarde el archivo authentication_policy.properties.in.
8. Entre */dir_instalación*/install/bin/setupfiles.sh (UNIX) o *dir_instalación*\ install\bin\setupfiles.cmd (Windows) para actualizar las entradas LDAP en el archivo authentication_policy.properties desde el archivo authentication_policy.properties.in.
9. Inicie Sterling B2B Integrator.

   Los cambios efectuados en el archivo authentication_policy.properties se aplican y ahora puede empezar a utilizar el servidor LDAP para autenticar a los usuarios.

   Tras el arranque, el sistema identifica los servidores LDAP desde el archivo authentication_policy.properties. El sistema autentica a los usuarios externos cuando los usuarios inician la sesión.

Verificar la configuración de LDAP

Para verificar que ha configurado LDAP correctamente con Sterling B2B Integrator, revise el archivo Authentication.log archivo bajo Autenticación de usuario para asegurarse de que el sistema ha aceptado la configuración de LDAP.

Acerca de esta tarea

Si hay problemas al conectarse al directorio LDAP o falla la autenticación de LDAP, compruebe las sentencias de registro DEBUG en el archivo Authentication.log para solucionar el problema. El archivo Authentication.log registra todos los intentos de inicio de sesión, tanto si son satisfactorios como si no lo son.

Cifrar contraseñas LDAP

Puede ocultar las contraseñas relacionadas con LDAP en los archivos de propiedades cifrándolas en el archivo customer_overrides.property.

Acerca de esta tarea

Se pueden utilizar los parámetros (propiedades) siguientes para cifrar las contraseñas LDAP en el archivo customer_overrides.properties:

Parámetro/propiedad	Descripción
authentication_policy.authentication _1.credentials	Este parámetro o propiedad controla la contraseña principal necesaria para acceder a una instancia de LDAP. Debe estar protegida porque ninguna contraseña que controle la seguridad y el acceso debe mostrarse en texto plano.
authentication_policy. LDAP_SECURITY_ TRUSTSTORE_PASSWORD	Este parámetro o propiedad controla la contraseña para el almacén de confianza (formato JKS) utilizado para asegurar las conexiones LDAP. Se debe proporcionar la frase de contraseña para este JKS para que se pueda acceder al almacén de confianza dado que se trata de un archivo cifrado.
authentication_policy. LDAP_SECURITY_KEYSTORE_PASSWORD	Este parámetro o propiedad controla la contraseña si la autenticación SSL basada en cliente se utiliza para proteger las conexiones con una determinado instancia LDAP.

Para cifrar contraseñas de LDAP:

Procedimiento

1. Vaya al directorio bin.
2. Utilice encrypt_string.[sh/cmd] para determinar el valor real de la propiedad/los parámetros que desea cifrar.
3. Actualice los parámetros/las propiedades en el archivo customer_overrides.properties para tener las entradas siguientes. Sustituya todos los <ENCVAL> por el valor cifrado de la serie no cifrada comentada para esa propiedad utilizando bin/encrypt_string.sh (o .cmd). Por ejemplo:

```
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
```

Noticias de usuario

Noticias de usuario

La característica Noticias de usuario permite publicar mensajes a las páginas de inicio de consola de administración. Noticias de usuario permite informar a los usuarios sobre los cambios realizados en los sucesos y las tareas importantes o recordarles dichos cambios.

Se pueden publicar mensajes:

- Para todos los usuarios
- Para un usuario específico
- Varios usuarios

El elemento de noticias se visualiza basándose en una fecha efectiva y una fecha de caducidad. También puede configurar el mensaje como:

Tipo de mensaje	Símbolo	Descripción
Aviso		Proporciona información de anuncio de prioridad general o baja.
Alerta		Información de anuncio proporcionada de alta prioridad.

Debe tener permisos de grabación para Cuentas si desea crear mensajes de noticias de usuario. La supresión de los mensajes antiguos reduce los requisitos de almacenamiento y la cantidad de esfuerzo necesario para recuperar mensajes específicos.

Las tareas de Noticias de usuario incluyen:

- Crear un mensaje de noticias de usuario para usuarios específicos
- Crear un mensaje de noticias de usuario para todos los usuarios
- Buscar un mensaje de noticias de usuario
- Editar un mensaje de noticias de usuario
- Suprimir un mensaje de noticias de usuario

Crear mensajes de noticias de usuario para todos los usuarios

Puede crear mensajes de noticias de usuario para todos los usuarios desde el menú **Administración**.

Acerca de esta tarea

Antes de empezar, debe conocer la información siguiente:

Campo	Descripción
Tipo	Tipo de mensaje que está creando. Los valores válidos son Notice (Aviso) y Alert (Alerta).

Campo	Descripción
Asunto	Asunto del mensaje que está creando.
Mensaje	Cuerpo del mensaje que está creando.

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Noticias de usuario**.
2. Junto a **Nuevo mensaje**, pulse **Ir**
3. Entre el **Tipo**.
4. Entre el **Asunto**.
5. Entre el **Mensaje**.
6. Pulse **Siguiente**.
7. Seleccione **TODOS los usuarios** y pulse **Siguiente**.
8. Entre la **Fecha de vigencia** del mensaje (aaaa-mm-dd).
9. Entre la **Fecha de caducidad** del mensaje (aaaa-mm-dd).
10. Pulse **Siguiente**.
11. Revise los valores de mensajes de noticias.
12. Pulse **Finalizar**.

Crear mensajes de noticias de usuario para usuarios específicos

Puede crear mensajes de noticias de usuario para usuarios específicos desde el menú **Administración**.

Acerca de esta tarea

Antes de empezar, debe conocer la información siguiente:

Campo	Descripción
Tipo	Tipo de mensaje que está creando. Los valores válidos son Notice (Aviso) y Alert (Alerta).
Asunto	Asunto del mensaje que está creando.
Mensaje	Cuerpo del mensaje que está creando.

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Noticias de usuario**.
2. Junto a **Nuevo mensaje**, pulse **Ir**
3. Entre el **Tipo**.
4. Entre el **Asunto**.
5. Entre el **Mensaje**.
6. Pulse **Siguiente**.
7. Seleccione **Usuarios seleccionados**.
8. Seleccione el nombre de cada usuario que desea que reciba este mensaje.
9. Pulse **Siguiente**.
10. Entre la **Fecha de vigencia** del mensaje (aaaa-mm-dd).
11. Entre la **Fecha de caducidad** del mensaje (aaaa-mm-dd).
12. Pulse **Siguiente**.

13. Revise los valores de mensajes de noticias.
14. Pulse **Finalizar**.

Buscar mensajes de noticias de usuario

Puede buscar un mensaje de noticias de usuario desde el menú **Administración**.

Acerca de esta tarea

Para buscar un mensaje de noticias de usuario:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Noticias de usuario**.
2. Utilice una de las siguientes opciones de búsqueda:

Opciones de búsqueda de noticias de usuario	**Acción**
Por ID de usuario	Seleccione TODOS o el usuario específico en la lista.
Por tema	Entre una parte del texto de mensaje.
Por rango de fechas de vigencia	Entre el rango de fechas (mm/dd/aaaa).

3. Pulse **Ir** La página Noticias de usuario lista todos los mensajes que coinciden con los criterios de búsqueda.

Editar mensajes de noticias de usuario

Puede editar un mensaje de noticias de usuario desde el menú **Administración**.

Acerca de esta tarea

Para editar un mensaje de noticias de usuario:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Noticias de usuario**.
2. Busque el mensaje de noticias de usuario que desea editar.
3. Pulse Editar para el mensaje de noticias de usuario que desea editar.
4. Actualice el tipo de mensaje, el asunto o el mensaje, si es necesario.
5. Pulse **Siguiente**.
6. Actualice los usuarios que recibirán este mensaje, si es necesario y pulse **Siguiente**.
7. Actualice la **Fecha de vigencia** del mensaje (aaaa-mm-dd), si es necesario.
8. Actualice la **Fecha de caducidad** del mensaje (aaaa-mm-dd), si es necesario.
9. Pulse **Siguiente**.
10. Revise los valores de mensajes de noticias.
11. Pulse **Finalizar**.

Suprimir mensajes de noticias de usuario

Puede suprimir un mensaje de noticias de usuario desde el menú **Administración**.

Acerca de esta tarea

Para suprimir un mensaje de noticias de usuario:

Procedimiento

1. En el **Menú de administración**, seleccione **Cuentas** > **Noticias de usuario**.
2. Busque el mensaje de noticias de usuario que desea suprimir.
3. Pulse **suprimir** para el mensaje de noticias que desea eliminar.
4. Revise los valores de mensajes de noticias.
5. Pulse **Suprimir**. Se visualiza el mensaje siguiente:
   `La actualización del sistema se ha realizado correctamente.`

Cifrado de documentos

Visión general de la característica de cifrado de documentos

El cifrado de documentos es una característica que se proporciona con Sterling B2B Integrator y que configura una capa adicional de seguridad además de los permisos de archivo y base de datos tradicionales. Si integra Sterling File Gateway con Sterling B2B Integrator, se utiliza la misma característica de cifrado de documentos para proteger los datos en reposo.

Sterling File Gateway es una aplicación para la transferencia segura de archivos entre socios que utilizan diferentes protocolos, convenios de denominación de archivos y formatos de archivo.

La característica de cifrado de documentos está diseñada para evitar que se puedan fisgonear los datos en reposo. La característica le permite cifrar los datos de carga útil almacenados en la base de datos y/o en el sistema de archivos. También se ha diseñado para impedir que alguien fuera del sistema vea los datos de carga útil accediendo directamente a la base de datos o al sistema de archivos.

Aspectos importantes del cifrado de documentos:

- La configuración predeterminada en la instalación es sin cifrado. Si desea que se cifren los documentos, tendrá que activar esta característica.
- Puede activar esta característica en cualquier momento, pero sólo se cifran los documentos recibidos después de que se active el cifrado.
- Una vez activada esta función, el cifrado es para todas las cargas útiles a través del sistema entero.
- Sólo se cifran los datos de carga útil de documento, **no** los metadatos.
- Se utiliza la misma clave de cifrado para cifrar y descifrar.
- El sistema utiliza un certificado predefinido (doccrypto) para cifrar documentos. Puede crear un certificado de sistema diferente. Si lo hace, debe actualizar el valor de CERT_NAME en el archivo customer_overrides.properties.

Mientras que el rendimiento queda afectado cuando se habilita el cifrado, cada cliente verá impactos de rendimiento diferentes dependiendo del hardware, del número y tamaño de los documentos que se están procesando y de la cantidad relativa de tiempo de proceso empleado por un determinado servidor que realiza la permanencia y recuperación de documentos en otras actividades.

Clave de cifrado para el cifrado de documentos

Se utiliza la misma clave de cifrado para cifrar y descifrar documentos de base de datos o de sistema de archivos. El certificado digital se utiliza para generar y cifrar las claves y la frase de contraseña de sistema se utiliza para cifrar los certificados digitales.

El cifrado de documento crea una clave por documento y esta clave se almacenan junto con el documento como parte de los metadatos. Los certificados digitales se almacenan como cualquier otro certificado de sistema.

El sistema utiliza un certificado predefinido (doccrypto) para generar y cifrar las claves que se utilizan para cifrar los documentos. Puede crear un certificado de sistema diferente. Si lo hace, debe actualizar el valor de CERT_NAME en el archivo customer_overrides.properties.

Asignar un certificado diferente para el cifrado de documentos

El sistema utiliza un certificado predefinido (doccrypto) para cifrar documentos. Puede crear un certificado de sistema diferente para utilizar para cifrado de documentos, por ejemplo, si el certificado anterior caduca. Si lo hace, debe actualizar el valor de CERT_NAME en el archivo customer_overrides.properties.

Acerca de esta tarea

PRECAUCIÓN: No suprima o renombre el certificado del sistema anterior. Necesita el certificado anterior para descifrar documentos que se cifraron anteriormente. El nuevo certificado del sistema no puede descifrar estos documentos, puesto que nunca se utilizó para descifrarlos.

Antes de realizar este procedimiento, necesita:

- Generar el nuevo certificado
- Conocer el nombre del certificado

Para actualizar el valor de CERT_NAME:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio de propiedades.
3. Abra el archivo customer_overrides.properties.
4. Añada la línea siguiente al archivo:
   ```
   security.CERT_NAME=nombre_de_certificado_sistema_nuevo
   ```
5. Guarde y cierre el archivo customer_overrides.properties.
6. Detenga y reinicie Sterling B2B Integrator.

Habilitar cifrado para documentos de sistema de archivos y de base de datos

Puede cifrar documentos de sistema de archivos y de base de datos desde el directorio de propiedades.

Acerca de esta tarea

Para cifrar documentos de sistema de archivos y de base de datos:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio de propiedades.
3. Abra el archivo customer_overrides.properties.
4. Añada la línea siguiente al archivo.
   `security.ENC_DECR_DOCS=ENC_ALL`
5. Guarde y cierre el archivo customer_overrides.properties.
6. Detenga y reinicie Sterling B2B Integrator.

Habilitar cifrado para documentos de base de documentos

Puede cifrar documentos de base de datos desde el directorio de instalación.

Acerca de esta tarea

Para cifrar documentos de base de datos:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio de propiedades.
3. Abra el archivo customer_overrides.properties.
4. Añada la línea siguiente al archivo.
   `security.ENC_DECR_DOCS=ENC_DB`
5. Guarde y cierre el archivo customer_overrides.properties.
6. Detenga y reinicie Sterling B2B Integrator.

Habilitar cifrado para documentos de sistema de archivos

Puede cifrar documentos de sistema de archivos desde el directorio de instalación.

Acerca de esta tarea

Para cifrar documentos de sistema de archivos:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio de propiedades.
3. Abra el archivo customer_overrides.properties.
4. Añada la línea siguiente al archivo.
   `security.ENC_DECR_DOCS=ENC_FS`
5. Guarde y cierre el archivo customer_overrides.properties.
6. Detenga y reinicie Sterling B2B Integrator.

Inhabilitar el cifrado de documentos

Puede inhabilitar el cifrado de documentos desde el directorio de propiedades.

Acerca de esta tarea

La configuración predeterminada en la instalación es sin cifrado.

Para inhabilitar el cifrado de documentos:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio de propiedades.
3. Abra el archivo customer_overrides.properties.
4. Actualice el valor de ENC_DECR_DOCS a NONE. Por ejemplo:
   `security.ENC_DECR_DOCS=NONE`
5. Guarde y cierre el archivo customer_overrides.properties.
6. Detenga y reinicie Sterling B2B Integrator.

Certificados

Certificados digitales

Utilice IBM Key Management Utility (iKeyman) para ayudar a gestionar los certificados digitales.

El sistema utiliza los siguientes tipos de certificados digitales:

- Certificados CA y de confianza: Certificados digitales para los que el sistema no tiene las claves privadas. Estos certificados se almacenan en formato DER estándar.
- Certificados de sistema: Un certificado digital para el que se mantiene la clave privada en el sistema. Estos certificados se almacenan con la clave privada en un formato seguro.

A continuación se proporciona información básica sobre cómo utilizar certificados digitales:

- Cada organización que intercambia documentos seguros debe tener un certificado. Utilice iKeyman para generar el certificado o se puede generar externamente. Para obtener información sobre iKeyman, consulte "IBM Key Management Utility (iKeyman)" en la página 63.
- Cada perfil comercial para un socio comercial con el que intercambia documentos firmados y cifrados debe tener un certificado.
- Una organización o un perfil comercial sólo puede tener un certificado activo a la vez. En el caso de certificados dobles, una organización puede tener un par de certificados activo; uno para la firma y otro para el cifrado.
- Una organización o un perfil comercial debe tener un certificado activo para intercambiar satisfactoriamente los documentos firmados y cifrados.
- Una organización o un perfil comercial puede tener varios certificados válidos.
- Los certificados se pueden utilizar para firmar documentos que se transmiten mediante todos los métodos de transporte.
- La longitud de clave para un certificado no tiene que ser igual que la de un certificado de socio comercial.
- Antes de establecer el periodo de validez para el certificado, se recomienda leer y aplicar las recomendaciones de mejor práctica de la publicación de Microsoft PKI Quick Guide. Para obtener más información sobre las recomendaciones sobre mejores prácticas a la hora de utilizar certificados, consulte http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

Certificados digitales soportados

Sterling B2B Integrator soporta la versión 3 X.509 de los certificados digitales. Los certificados digitales pueden ser de firma personal o firmados por CA (entidad emisora de certificados).

- Un certificado de firma personal es un certificado digital que se ha firmado con la clave privada que corresponde a la clave pública del certificado, demostrando que el emisor tiene la clave privada que corresponde a la clave pública del certificado.
- Una certificado firmado por CA es un certificado digital que se ha firmado utilizando claves mantenidas por entidades emisoras de certificados. Normalmente, antes de emitir un certificado, la entidad emisora de certificados evalúa el solicitante de certificado para determinar que dicho solicitante es de hecho el titular de certificado al que se hace referencia en el certificado.

Certificados CA

Un certificado CA es un certificado digital emitido por una entidad emisora de certificados (CA). La CA verifica las raíces de confianza en los certificados de confianza. Las raíces de confianza son la base sobre la que se crean cadenas de confianza en los certificados.

Confiar en una raíz de CA (entidad emisora de certificados) significa confiar en todos los certificados emitidos por esa CA. Si elige no confiar en una raíz de CA, Sterling B2B Integrator no confía en ningún certificado emitido por esa CA.

Los certificados CA contienen una clave pública que corresponde a una clave privada. La CA es propietaria de la clave privada y la utiliza para firmar los certificados que emite. Para validar un certificado de confianza, primero debe incorporar un certificado CA.

Los certificados raíz de las CA comunes están contenidos en un almacén de claves Java (JKS) de la JVM que se entrega con Sterling B2B Integrator. Esto permite a los usuarios establecer algunas relaciones de confianza basadas en entidad emisora más fácilmente que si tuvieran que buscar y obtener los certificados de un sitio web de CA.

Los certificados CA se almacenan independientemente de los certificados de confianza en el producto.

Desde la interfaz de usuario, puede incorporar certificados raíz de CA que se originen en cualquiera de los orígenes siguientes:

- Certificados raíz de CA comunes enviados con Sterling B2B Integrator en el almacén de claves JKS.
- Sólo se reconocen los certificados y los certificados fiables. Los certificados y las claves privadas no están visibles en la interfaz de usuarios.
- Certificados SSL importados de socios comerciales.
- Otros certificados obtenidos externamente.

Basándose en las políticas de seguridad del sitio, los certificados CA del almacén de claves JKS también se pueden incorporar a través de la consola. Aunque los certificados CA son documentos públicos, debe ser cuidadoso respecto a quienes tienen derecho de añadirlos. Alguien podría añadir maliciosamente un certificado CA falso con el fin de verificar certificados de usuario final falsos.

Nombres de certificado CA

El nombre de certificado CA no forma parte del contenido del certificado. Se crea a partir del Nombre distinguido relativo (RDN) del emisor y el número de serie del certificado. No obstante, los certificados del almacén de claves JKS se denominan con una serie arbitraria.

Puesto que el nombre de certificado se almacena en la base de datos del sistema y se utiliza como alias para hacer referencia al certificado de la GUI, es aconsejable renombrar los certificados CA con nombres más cortos o más descriptivos basándose en los convenios de denominación de archivos. Los certificados se pueden renombrar al incorporarse o editarse.

Ventajas de los certificados digitales de firma personal y firmados por CA

En función de sus necesidades, encontrará ventaja e inconvenientes en los certificados de firma personal en contraposición a los certificados firmados por CA.

Cuando el usuario y sus socios comerciales deciden si deben generar un certificado de firma personal o comprar un certificado firmado a una entidad emisora de certificados, tenga en cuenta lo siguiente:

- Puede crear fácilmente certificados de firma personal utilizando Sterling B2B Integrator. Sin embargo, estos certificados de firma personal no los verifica un tercero de confianza.
- La ventaja principal de utilizar certificados de una CA (entidad emisora de certificados) es que la identidad del titular del certificado se verifica mediante un tercero de confianza. Las desventajas incluyen coste adicional y esfuerzo administrativo. Si decide utilizar un certificado de terceros, obténgalo de una CA.
- Una CA proporciona un origen centralizado para publicar y obtener información acerca de los certificados, incluida la información sobre los certificados revocados.

De forma predeterminada, el sistema confía en todos los certificados de CA y los certificados de firma personal generados por la aplicación. Sin embargo, puede especificar si todos o algunos certificados emitidos por una CA determinada deben ser de confianza. Además, puede no confiar explícitamente en un certificado de firma personal de un socio comercial.

Fechas de caducidad de certificados

Si se utilizan un adaptador y un servlet para las comunicaciones de entrada, debe supervisar las fechas de caducidad de los certificados de sistema para asegurarse de que los certificados son válidos. Antes de que los certificados caduquen, se deben sustituir por certificados válidos.

Definiciones de parámetros de certificados de sistema

Si se utilizan un adaptador y un servlet para las comunicaciones de entrada, debe supervisar las fechas de caducidad de los certificados de sistema para asegurarse de que los certificados son válidos. Antes de que los certificados caduquen, se deben sustituir por certificados válidos.

Parámetro	Descripción
alias	Nombre de clave almacenado en el HSM. Utilice sólo nombres de alias que contengan los caracteres a-z, A-Z, 0-9 o un guión (-) y cuya longitud total no sea mayor que la longitud de GUID de sistema.
certname	Nombre a asignar al certificado de sistema en la base de datos.
Certtype	Tipo de certificado a importar. Se soportan cuatro tipos de archivos de certificado: pkcs12, pkcs8, pem y keystore. Sterling B2B Integrator sólo soporta las claves pem cifradas con DES o 3DES. Utilice keystore para listar o importar el almacén de claves.
file	Nombre del archivo a importar.
keypass	PIN para la ranura en el dispositivo Eracom.
keystoretype	Tipo de almacén de claves a importar. El valor válido es CRYPTOKI.
keystoreprovider	Tipo de proveedor. Eracom es el único tipo de proveedor HSM soportado. Los valores válidos son: • ERACOM • ERACOM.n (si está importando certificados a una ranura distinta de la primera posición)
password	Frase de contraseña de almacén para el archivo de certificado.
pkcs12file	Nombre del archivo PKCS12 a importar.
pkcs12storepass	Frase de contraseña de almacén utilizada para la generación del archivo PKCS12.
pkcs12keypass	Frase de contraseña válida para el archivo PKCS12.
storepass	PIN de la ranura del dispositivo Eracom donde reside el almacén de claves.
systempass	Frase de contraseña de sistema.

IBM Key Management Utility (iKeyman)

IBM Key Management Utility (iKeyman) es un componente del SDK de IBM que genera claves, solicitudes de certificación y certificados firmado automáticamente.

Puede utilizar iKeyman parar crear certificados para proteger comunicaciones y para cifrar y descifrar datos. En una transferencia segura mediante SSL, los certificados proporcionando un nivel añadido de seguridad.

En Sterling B2B Integrator, puede utilizar iKeyman para crear:

- Solicitudes de firma de certificado (CSR): Un archivo que se debe enviar por correo electrónico a una entidad emisora de certificados para solicitar un certificado X.509.
- Certificados de clave– Una combinación de un certificado codificado en ASCII y una clave privada cifrada PKCS12 codificada en ASCII. Si genera certificados de clave utilizando el formato estándar (valor predeterminado) con determinados cifrados, el certificado de salida producirá un error al importarse a Sterling B2B Integrator. PKCS12 es el formato recomendado para certificados de claves.

Para obtener más información sobre cómo configurar y utilizar iKeyman, consulte Visión general de iKeyman para IBM SDK, Java Technology Edition 7.0.0

Tareas de certificado

Crear un certificado de firma personal

Puede crear un certificado de firma personal desde el menú **Administración**.

Acerca de esta tarea

Para crear un certificado de firma personal:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Junto a **Crear certificado de firma personal**, pulse **Ir**
3. Especifique el **Nombre** del certificado de firma personal.
4. Entre el nombre de la **Organización** de origen.
5. Seleccione el **país** o el origen del certificado de firma personal.
6. Especifique una **dirección de correo electrónico** de contacto de la persona responsable de los certificados en el organización y, a continuación, pulse **Siguiente**.
7. Especifique el **número de serie** del certificado. El número de serie es el número que desea asignar al certificado de firma personal.
8. Entre el número de días (**Duración**) durante los cuales el certificado de firma personal es válido.

   Nota: En V5.2.6.2 o posteriores, la fecha de caducidad máxima es *1 de enero de 2080*. Cualquier duración especificada que finalizará más allá del 1 de enero de 2080 tomaría el valor predeterminado *1 de enero de 2080*. En anteriores releases no existía ningún límite superior.
9. Especifique las **direcciones IP** de las interfaces de red que desea asociar con el certificado como el campo SubjectAltName.
10. Especifique los **nombres DNS** de las interfaces de red que desea asociar con el certificado como el campo SubjectAltName.
11. Seleccione la **longitud de clave**. Seleccione una de las longitudes de clave siguientes:
    - 512
    - 1024
    - 2048

    Nota: La longitud de clave 1024 ofrece un buen equilibrio entre seguridad, interoperabilidad y eficiencia. La longitud de clave 2048 es la más segura, aunque también la más lenta, y es posible que no funcione con algunas aplicaciones.

    Nota: Si selecciona la longitud de clave 512, también debe utilizar JDK 7 SR5. JDK 7 SR7 FP1 no da soporte a longitudes de clave por debajo de 1024.
12. Seleccione el **algoritmo de firma**.
13. Seleccione la opción **Validar cuando se utiliza**. Las opciones de validación son:

- Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
- Cadena de autenticación – Construye una cadena de confianza para los certificados no de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.

14. Establezca el **Bit de firma de certificado** seleccionando el recuadro de selección.
15. Pulse **Siguiente**.
16. Revise la información sobre el certificado de firma personal.
17. Pulse **Finalizar**.

Obtener automáticamente el certificado de confianza de los socios comerciales

La Utilidad de captura de certificados automatiza el proceso de obtención de un certificado SSL de un socio comercial. Este método de obtención de información de certificado permite que un socio se conecte y guarde fácilmente un certificado.

Acerca de esta tarea

Si lo desea, se puede realizar entonces una comprobación de seguridad fuera de banda antes de que se incorpore el certificado en el sistema como un certificado CA o de confianza.

Antes de empezar:

- Verifique que el sistema host del socio está habilitado para SSL.
- Obtenga información de host y puerto del servidor del socio comercial.
- Si se va a utilizar la modalidad FTPS, determine si la modalidad será explícita o implícita.
- Configure la instancia de servicio SSLCertGrabberAdapter predeterminada para utilizar el servidor perimetral y (sólo HTTPS) el servidor proxy apropiados. Consulte la documentación de adaptador para obtener detalles.

Para obtener el certificado SSL automáticamente de un socio comercial:

Procedimiento

1. En el **Menú de administración**, seleccione **Socio comercial > Certificados digitales > Utilidad de captura de certificados**.
2. Junto a **Capturar certificado de socio**, pulse **Ir**
3. Seleccione el tipo de conexión para el servidor y pulse **Siguiente**.
   - FTPS
   - HTTPS
4. Entre el **Nombre de host** o la **Dirección IP**.
5. Entre el número de **Puerto**.
6. Seleccione la modalidad de conexión para FTPS (si está utilizando HTTPS, sáltese este paso):
   - Explícita - Se produce la negociación SSL después de que se establezca la conexión FTP. Valor predeterminado.
   - Implícita – Se produce la negociación SSL antes de que se establezca la conexión FTP.

7. Pulse **Siguiente**. El sistema intenta conectarse y recuperar certificados.
8. Cuando la captura haya finalizado, revise la información de resumen y decida qué certificados desea guardar.
9. Seleccione un método de codificación para cada certificado y pulse **Guardar**. Los formatos de codificación son:
   - BASE64 – Utiliza la codificación BASE64 en el certificado DER estándar. Valor predeterminado.
   - DER – Formato estándar para certificados digitales, aceptado por la mayoría de aplicaciones.
10. Pulse **Guardar** y vaya a la ubicación donde desea guardar el archivo.
11. Acepte el nombre de archivo predeterminado o edítelo según los convenios de denominación de archivos y pulse **Guardar**.
12. Después de guardar, los certificados se pueden incorporar al sistema. Si decide incorporar un certificado al sistema:
    a. Verifique que cada certificado es válido y de confianza.
    b. Incorpore el certificado como un certificado CA o de confianza, dependiendo de la función. La confianza basada en entidad emisora de certificados, es posible que tenga que incorporar la cadena de certificados, excluyendo el certificado de usuario final. Para obtener la confianza directa, incorpore el certificado de usuario final.

Configurar información de estado en resúmenes de certificado

De forma predeterminada, la información de estado de certificado se proporciona al final de la ventana emergente de resumen cuando se selecciona un nombre de certificado con hiperenlace. Puede incluir o excluir la información de estado. Dado que la información de estado se compila en tiempo real, quizá no desee incluirla.

Acerca de esta tarea

La propiedad VerificationOnPopupInfo controla si la información de estado se visualiza en el resumen de certificado. Esta propiedad está en el archivo ui.properties. Los valores para la propiedad VerificationOnPopupInfo son:

- true - incluir información de validación (valor predeterminado)
- false - no compilar o visualizar información de validación en la ventana emergente
- (cualquier otro valor) - incluir información de validación

Para impedir la compilación y la visualización de la información de estado:

Procedimiento

1. Abra el archivo ui.properties.
2. Actualice el valor de VerificationOnPopupInfo para que sea false. Por ejemplo:
   ```
   VerificationOnPopupInfo=false
   ```
3. Guarde y cierre el archivo.
4. Reinicie Sterling B2B Integrator.

Configurar visualizaciones de certificado de huella

Además del hash SHA1 calculado previamente, se pueden incluir certificados de huella adicionales en las pantallas de visualización, confirmación y resumen de certificado. Los cálculos hash se realizan a petición cuando se genera una pantalla.

Acerca de esta tarea

Se visualizan certificados de huella adicionales en las pantallas de GUI, pero no tienen ningún efecto sobre el manejo de mensajes o la comunicación del sistema.

Para configurar el sistema de forma que calcule y visualice certificados de huella adicionales:

Procedimiento

1. En el archivo ui.properties, modifique esta línea:

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   Para visualizar más de un hash adicional, separe los valores con comas. Por ejemplo:

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

Parámetro	Descripción
hash_algorithm	Nombre de un algoritmo de hash que se debe aplicar al certificado de huella. Los valores válidos son: • SHA-256 • SHA-384 • SHA-512

2. Guarde y cierre el archivo ui.properties.
3. Reinicie Sterling B2B Integrator.

Buscar certificados CA

Puede buscar un certificado CA desde el menú **Administración**.

Acerca de esta tarea

Para buscar un certificado CA:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, en el **Menú de administración**, seleccione **Socio comercial > Certificados digitales > CA**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Realice una de las acciones siguientes y, a continuación, pulse **Ir**
   - Bajo Buscar en el campo **Por nombre de certificado**, entre una parte del nombre o el nombre de certificado CA entero que está buscando. La página Certificados digitales CA lista todos los certificados CA que coinciden con los criterios de búsqueda.
   - Bajo Lista en el campo **Alfabéticamente**, seleccione **TODOS** o la letra por la que empieza el nombre del certificado CA que está buscando. Si se selecciona TODOS, se listan todos los certificados CA. La página Certificados digitales CA lista todos los certificados CA que coinciden con los criterios de búsqueda.

Ver información de resumen de certificados CA

Cuando se visualiza una lista de certificados, puede pulsar el nombre de certificado para ver información de resumen acerca de ese certificado. Puede configurar el nombre del sistema, el certificado de huella y el estado.

Acerca de esta tarea

Los campos siguientes son configurables en el sistema.

Campo de resumen de certificado	Descripción
Nombre de sistema	El Nombre de certificado es la etiqueta de base de datos. Se utiliza para hacer referencia a este certificado en la GUI y almacena este nombre en la base de datos. El nombre predeterminado para un certificado del almacén de claves JKS es una serie arbitraria. Los nombres de otros certificados se crean a partir del nombre distinguido relativo (RDN) del emisor y del número de serie del certificado. Puede cambiar un nombre de certificado por un nombre más corto o más fácilmente reconocible al incorporar o editar el certificado.
Certificado de huella	La información para el hash SHA1 se incluye de forma predeterminada. Para configurar el cálculo y la visualización de la información de certificado de huella para otros hashes, edite el archivo ui.properties.
Estado	Comprobación en tiempo real del estado actual, indicando si las fechas de certificado son válidas y si el certificado se ha verificado. Para configurar si esta información se calcula en el momento de la visualización, edite el archivo ui.properties.

Aunque esta información se aplica a la información de resumen para un certificado CA, aparecen campos similares en pantallas de resumen y confirmación para otros tipos de certificados.

Incorporar certificados CA de la interfaz de usuario

Puede incorporar un certificado CA desde la interfaz de usuario, bajo el menú **Administración**.

Acerca de esta tarea

Basándose en las políticas de seguridad del sitio, los certificados CA del almacén de claves JKS también se pueden incorporar a través de la consola.

Antes de empezar, guarde en un archivo local los certificados CA que ha obtenido externamente.

Para incorporar un certificado de entidad emisora de certificados:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, en el **Menú de administración**, seleccione **Socio comercial > Certificados digitales > CA**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.

2. Junto a **Incorporar certificado nuevo**, pulse **Ir**
3. Seleccione un método para importar certificados:

Método de importación	Pasos siguientes
Importar desde máquina virtual Java – Importa desde el almacén de claves JKS	1. Pulse **Importar** desde **JVM**. 2. Acepte la contraseña predeterminada que aparece en el campo de contraseña y pulse **Siguiente**. Sun Microsystems proporciona la contraseña de almacén de claves predeterminada. Si el campo de contraseña está vacío, el sistema seguirá utilizando la contraseña por defecto.
Importar desde archivo – Importa certificados guardados como archivo en una unidad local	1. Pulse **Importar** desde **Archivo**. 2. Entre el nombre de archivo o pulse **Examinar** para seleccionar un archivo de certificado CA. Pulse Siguiente. Puede ignorar la contraseña que aparece en el campo de contraseña. No es necesario borrar la entrada.

   Los certificados disponibles se muestran con un resumen de la información de identificación. Todos los certificados se seleccionan por defecto.
4. Pulse los recuadros de selección a la izquierda de cada entrada para seleccionar o de seleccionar los certificados a importar.
5. Para cada certificado seleccionado, acepte el nombre de certificado sugerido o edítelo según las convenciones de nomenclatura de archivo.
6. Seleccione la opción **Validar cuando se utiliza** y pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Intenta construir una cadena de confianza hasta la raíz para los certificados que no son de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
7. Si recibe un mensaje que indica que el certificado duplica un certificado que ya se encuentra en la base de datos, entre Y (Sí) o N (No) para indicar si se debe importar el duplicado.

   Esta indicación sólo se especifica en los certificados individuales. No se especifica al incorporar uno o varios certificados desde un archivo.

   Los certificados se identifican mediante el hash SHA1 con el fin de determinar duplicados. Puede haber más de una copia de un certificado en la base de datos, puesto que cada uno llena una fila diferente y tiene un ID de objeto distinto. El certificado existente no se sobrescribirá.
8. Revise la información del certificado de la entidad emisora de certificados.
9. Pulse **Finalizar**.

Incorporar certificados CA de la consola

Una vez guardados todos los certificados CA en un archivo local, puede incorporar el certificado CA en la consola desde el directorio de instalación.

Acerca de esta tarea

Los certificados CA comunes están contenidos en un almacén de claves JKS que forma parte de la JVM que se envía con Sterling B2B Integrator. El almacén de claves JKS está ubicado en /dir_instalación/jdk/jre/lib/security/cacerts. también puede obtener certificados de forma externa.

Para importar certificados al repositorio de confianza de Sterling B2B Integrator, modifique el mandato en /dir_instalación/install/bin/ImportCACerts.sh (UNIX) o \dir_instalación\install\bin\ImportCACerts.cmd (Windows).

Antes de empezar, guarde en un archivo local los certificados CA obtenidos externamente.

Para incorporar un certificado CA en la consola:

Procedimiento

1. Vaya al directorio de instalación.
2. Vaya al directorio bin.
3. Entre este mandato:

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   Se listan todos los certificados del archivo, uno por uno, con estas excepciones:
   - Las entradas que contienen claves simétricas o privadas no se procesan o no se listan.
   - Sólo se procesa y se lista el primer certificado de un archivo de formato DER.
4. Tras las solicitudes, entre Y (no es sensible a las mayúsculas y minúsculas) para cualquier certificado que desee importar.
5. Para cada certificado aceptado, acepte el nombre de certificado sugerido o edítelo basándose en los convenios de denominación de archivo.
6. Si la etiqueta de certificado es un duplicado de una etiqueta que ya está en la base de datos, entre `Y` o `N` (no es sensible a las mayúsculas y minúsculas) para indicar si desea cambiar la etiqueta. Aunque generalmente los certificados no se identifican por la etiqueta y la base de datos permite duplicados de etiqueta, algunos servicios buscan los certificados por la etiqueta. Procure no utilizar etiquetas duplicadas para evitar la posibilidad de un comportamiento inesperado.
7. Si el certificado duplica un certificado que ya está en la base de datos (como indica en el hash SHA1 del certificado, especifique con Y o N si desea importar el duplicado.

   Los certificados se identifican mediante el hash SHA1 con el fin de determinar duplicados. Puede haber más de una copia de un certificado en la base de datos, puesto que cada uno llena una fila diferente y tiene un ID de objeto distinto. El certificado existente no se sobrescribirá.

Editar certificados CA

Puede editar un certificado CA desde el menú **Administración**.

Acerca de esta tarea

Para editar un certificado CA:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, en el **Menú de administración**, seleccione **Socio comercial > Certificados digitales > CA**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Utilizando Buscar o Lista, localice el certificado CA que desea editar y pulse **Ir**
3. Junto al **Certificado CA** que desea editar, pulse **Editar**.
4. Entre el Nombre de certificado.
5. Seleccione la opción **Validar cuando se utiliza** y pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Construye una cadena de confianza para los certificados no de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
6. Revise la información del certificado de la entidad emisora de certificados.
7. Pulse **Finalizar**.

Suprimir certificados CA

Puede suprimir un certificado CA desde el menú **Administración**.

Acerca de esta tarea

Para suprimir un certificado CA:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, en el **Menú de administración**, seleccione **Socio comercial > Certificados digitales > CA**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Junto a **Alfabéticamente**, pulse **Ir**
3. Junto al certificado CA que desea suprimir, pulse **Suprimir**.

Buscar certificados de sistema

Puede buscar un certificado de sistema desde el menú **Administración**.

Acerca de esta tarea

Para buscar un certificado de sistema:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**

2. En los certificados de sistema, realice una de las acciones siguientes y, a continuación, pulse **Ir**:
   - Bajo Buscar, en el campo **Por nombre de certificado**, entre una parte del nombre o el nombre de certificado de sistema entero que está buscando. La página Certificados de sistema lista todos los certificados de sistema que contienen el nombre completo o parcial que ha escrito.
   - Bajo **Lista**, en el campo **Alfabéticamente**, seleccione **TODOS** o la letra por la que empieza el nombre del certificado CA que está buscando. Si se selecciona TODOS, se listan todos los certificados de sistema. La página Certificados de sistema lista todos los certificados de sistema que coinciden con los criterios de búsqueda.

Editar certificados de sistema

Puede editar un certificado de sistema desde el menú **Administración**.

Acerca de esta tarea

Para editar un certificado de sistema:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Utilizando Buscar o Lista, localice el **certificado de sistema** que desea editar y pulse **Ir**
3. Junto al certificado de sistema que desea editar, pulse **Editar**.
4. Especifique el **nombre de certificado**.
5. Seleccione la opción **Validar cuando se utiliza** y pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Construye una cadena de confianza para los certificados no de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
6. Revise la información del certificado de sistema.
7. Pulse **Finalizar**.

Identificar certificados de sistema en Sterling B2B Integrator

Puede identificar un certificado de sistema desde el menú **Administración**.

Acerca de esta tarea

Para identificar un certificado de sistema:

Procedimiento

1. En el **Menú de administración**, seleccione **Despliegue > Servicios > Configuración**.

2. En la sección Lista, seleccione el tipo de servicio o adaptador aplicable en la lista **por tipo de servicio** y pulse **Ir**
3. En la lista de configuraciones, seleccione la configuración.
4. Pulse el **nombre de servicio** para ver información de configuración.
5. Revise la información de resumen de certificado.

Comprobar la fecha de caducidad de un certificado de sistema

Si se utilizan un adaptador y un servlet para las comunicaciones de entrada, debe supervisar las fechas de caducidad de los certificados de sistema para asegurarse de que los certificados son válidos.

Acerca de esta tarea

Para comprobar la fecha de caducidad de certificado de sistema:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Para ver todos los certificados de sistema, seleccione **Todos** en la lista desplegable alfabética y pulse **Ir**
3. Seleccione le nombre de certificado de sistema que desea ver. Se visualiza el Resumen de certificado.
4. En la sección **Descripción** del Resumen de certificado, revise la información proporcionada en el campo **Fechas válidas**.
5. Revise la información proporcionada en la sección **Estado** para ver si las fechas son válidas y el certificado se ha verificado.

Exportar certificados de sistema en Sterling B2B Integrator

Este mandato de exportación sólo es aplicable a los certificados de sistema de Sterling B2B Integrator. No puede utilizar este mandato para exportar certificados de sistema en el HSM.

Acerca de esta tarea

Para exportar un certificado de sistema, entre el siguiente mandato, con los parámetros adecuados:

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

Parámetro	Descripción
keyname	Nombre de la clave de sistema que se debe exportar.
pkcs12filename	Nombre del archivo que contiene la información exportada.
pkcs12storepass	Contraseña de almacén que protege el almacén.
pkcs12keypass	Contraseña de clave que protege la clave.

Suprimir certificados de sistema en Sterling B2B Integrator

Puede exportar una copia del certificado de sistema al disco local antes de suprimirlo. OpsDrv, OpsKey y UIKeys son certificados de sistema que no se pueden suprimir.

Acerca de esta tarea

Para suprimir un certificado de sistema:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados.**
2. Junto a **Alfabéticamente**, pulse **Ir**
3. Junto al certificado de sistema que desea suprimir, pulse **Suprimir**.
4. Pulse **Suprimir** en la página Confirmar.

Extraer certificados de sistema

Para exportar un certificado de sistema, debe extraer el certificado. Este procedimiento sólo exporta el certificado público, no la clave privada, y le proporciona un certificado público para enviar a un socio comercial.

Acerca de esta tarea

Para extraer un certificado de sistema:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. Utilizando Buscar o Lista, localice el certificado de sistema que desea extraer.
3. Junto al certificado de sistema que desea extraer, pulse **Extraer**.
4. En el recuadro de diálogo **Extraer certificado de sistema**, seleccione el formato de certificado y, a continuación, pulse **Ir**:
   - PKCS12 - Esta opción formatea el certificado digital como un archivo PKCS12. También tiene la opción de entrar una contraseña de clave privada y una contraseña de almacén de claves.
   - BASE64 - Esta opción utiliza la codificación BASE64 en el certificado DER estándar.
   - DER - La mayoría de aplicaciones aceptan este formato estándar para certificados digitales.
5. En el recuadro de diálogo **Descarga de archivos**, pulse **Guardar**.
6. En el recuadro de diálogo **Guardar como**, seleccione la ubicación donde desea guardar el certificado y, a continuación, pulse **Guardar**. No se soporta la opción para abrir el certificado. Debe abrir el certificado dentro del sistema operativo. Si recibe el mensaje de error que indica que éste es un archivo de certificado de seguridad no válido, abra el archivo en un editor de texto y suprima todas las líneas en blanco antes de -----BEGIN CERTIFICATE-----. Guarde el archivo editado y, a continuación, intente abrir el archivo.
7. Pulse **Cerrar** en el recuadro de diálogo Extraer certificado de sistema. Se visualiza la página Certificado de sistema.

Buscar certificados de confianza

Puede buscar un certificado de confianza desde el menú **Administración**.

Acerca de esta tarea

Para buscar un certificado de confianza:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>De confianza**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. En la página Certificados digitales de confianza, realice una de las acciones siguientes y, a continuación, pulse **Ir**:
   - Bajo Buscar en el campo **Por nombre de certificado**, entre una parte del nombre o el nombre de certificado de confianza entero que está buscando. La página Certificados digitales de confianza lista todos los certificados de confianza que coinciden con los criterios de búsqueda.
   - Bajo Lista en el campo **Alfabéticamente**, seleccione **TODOS** o la letra por la que empieza el nombre del certificado de confianza que está buscando. La página Certificados digitales de confianza lista todos los certificados de confianza que coinciden con los criterios de búsqueda.

Incorporar certificados de sistema de confianza

Puede incorporar certificados de confianza, como por ejemplo, certificados SSL importados de socios comerciales u otros certificados externos.

Acerca de esta tarea

Los certificados de confianza podrían proceder de los orígenes siguientes:

- Certificados SSL importados de socios comerciales
- Otros certificados obtenidos externamente

Antes de empezar, guarde el certificado de sistema de confianza en un archivo en el ordenador local.

Para incorporar un certificado de sistema de confianza:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>De confianza**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. Junto a **Incorporar certificado nuevo**, pulse **Ir**
3. Especifique el **nombre de archivo** o pulse **Examinar** para seleccionar el nombre de archivo del certificado de confianza y, a continuación, pulse **Siguiente**.
4. Especifique el **nombre de certificado**.
5. Verifique el nombre del certificado de confianza que está incorporando. Para cada certificado que seleccione, el campo Nombre de certificado muestra una

sugerencia de nombre, seguida por un resumen de la información de identificación en el certificado. Puede cambiar el nombre según la nomenclatura de denominación de archivos.

6. Si tiene más de un certificado de confianza contenido en el archivo que ha seleccionado, seleccione el recuadro de selección a la izquierda de cada certificado para incorporar cada certificado.
7. Seleccione la opción **Validar cuando se utiliza** y pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Intenta construir una cadena de confianza hasta la raíz para los certificados que no son de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
   - Memoria caché de lista de revocación de certificados – Controla si se consulta la memoria caché de lista de revocación de certificados cada vez que se utiliza el certificado de sistema.
8. Revise la información del certificado de confianza.
9. Pulse **Finalizar**.

Editar certificados de confianza

Puede editar un certificado de confianza desde el menú **Administración**.

Acerca de esta tarea

Para editar un certificado de confianza:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>De confianza**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. Utilizando Buscar o Lista, localice el certificado de confianza que desea editar y pulse **Ir**
3. Pulse **editar** junto al certificado de confianza que desea editar.
4. Especifique el **nombre de certificado**.
5. Seleccione la opción **Validar cuando se utiliza** y pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Intenta construir una cadena de confianza hasta la raíz para los certificados que no son de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
   - Memoria caché de lista de revocación de certificados – Controla si se consulta la memoria caché de lista de revocación de certificados cada vez que se utiliza el certificado de sistema.
6. Revise la información del certificado.

7. Pulse **Finalizar**.

Suprimir certificados de sistema de confianza

Puede suprimir un certificado de sistema de confianza desde el menú **Administración**.

Acerca de esta tarea

Para suprimir un certificado de sistema de confianza:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>De confianza**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. Junto a **Alfabéticamente**, pulse **Ir**
3. Junto al certificado de confianza que desea suprimir, pulse **suprimir**.

Importar certificados de sistema PKCS12

Puede importar un certificado de sistema PKCS12.

Acerca de esta tarea

Para importar un certificado de sistema PKCS12:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba:

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

Incorporar certificados de sistema PKCS12

Una vez haya guardado el certificado de sistema PKCS12 en un archivo del sistema local, podrá incorporar el certificado de sistema PKCS12 desde el menú **Administración**.

Acerca de esta tarea

Antes de empezar, es necesario guardar el certificado de sistema PKCS12 en un archivo del sistema local.

Para incorporar un certificado de sistema PKCS12:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. En la página Certificados de sistema, bajo Incorporar, junto a **Certificado PKCS12**, pulse **Ir**

3. Entre el **Nombre de certificado** PKCS12.
4. Entre la **Contraseña de clave privada**. Es la contraseña utilizada para cifrar el certificado PKCS12.
5. Entre la **Contraseña de almacén de claves**. Es la contraseña para el objeto PKCS12. Puede ser la misma que la contraseña de clave privada.
6. Entre el **Nombre de archivo** o pulse **Examinar** para seleccionar el nombre de archivo del certificado PKCS12 y, a continuación, pulse **Siguiente**.
7. Seleccione la opción **Validar cuando se utiliza** y, a continuación, pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Construye una cadena de confianza para los certificados no de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
8. Revise la información de certificado de sistema PKCS12.
9. Pulse **Finalizar**.

Importar certificados de sistema Pem

Puede importar un certificado de sistema pem cifrado con DES o 3DES.

Acerca de esta tarea

Sólo se soportan las claves pem cifradas con DES o 3DES.

Para importar un certificado de sistema pem:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba:

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

Importar certificados de sistema de claves

Puede importar un certificado de sistema de claves.

Acerca de esta tarea

Para importar un certificado de sistema de claves

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba:

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

Importar certificados de sistema de almacén de claves

Puede generar un certificado de sistema de almacén de claves en un HSM.

Acerca de esta tarea

Para generar un certificado de sistema de almacén de claves en un HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba:

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

Incorporar certificados de sistema de claves

Una vez haya guardado el certificado de sistema de claves en un archivo del sistema local, podrá incorporar el certificado de sistema de claves desde el menú **Administración**.

Acerca de esta tarea

Antes de empezar, guarde el certificado del sistema de claves en un archivo del ordenador local.

Para incorporar un certificado de sistema de claves:

Procedimiento

1. Elija una de estas opciones:
   - Si utiliza Sterling B2B Integrator, desde el menú **Administración**, seleccione **Socio comercial >Certificados digitales>Sistema**.
   - Si utiliza AS2 Edition, en el menú **Administración de AS2**, seleccione **Certificados**.
2. Junto a **Certificado de claves**, pulse **Ir**
3. Especifique el **nombre de certificado**.
4. Especifique la **contraseña de clave privada.** Ésta es la contraseña utilizada para cifrar la clave privada.
5. Especifique el **nombre de archivo** o pulse **Examinar** para seleccionar el nombre de archivo del certificado de claves y pulse **Siguiente**.
6. Seleccione la opción **Validar cuando se utiliza** y pulse **Siguiente**. Las opciones de validación son:
   - Validez – Verifica que las fechas del periodo de validez del certificado siguen estando vigentes. Si no lo están, no se utilizará el certificado.
   - Cadena de autenticación – Construye una cadena de confianza para los certificados no de firma personal. Si no se puede crear una cadena de confianza mediante certificados válidos, no se utilizará el certificado. Si el certificado es de firma personal, esta opción sólo verifica la firma del certificado.
7. Revise la información del certificado de claves.
8. Pulse **Finalizar**.

OCSP (Online Certificate Status Protocol)

Soporte de OCSP (Online Certificate Status Protocol) en Sterling B2B Integrator

El OCSP (Online Certificate Status Protocol - Protocolo de estado de certificado en línea) es un conjunto de estructuras de datos definidas por ASN.1 para solicitar y recibir información acerca del estado de revocación de certificados. En principio, estas estructuras de datos se pueden enviar y recibir por medio de muchos protocolos de transporte. En la práctica, se utiliza HTTP.

Un cliente OCSP envía preguntas y procesa respuestas. Un respondedor OCSP responde a preguntas y genera respuestas.

Funcionalidad de cliente OCSP

Una implementación de cliente OCSP consta de estructuras de datos para la gestión de la información relativa a respondedores OCSP, funcionalidad para generar solicitudes OCSP, funcionalidad para procesar respuestas OCSP y funcionalidad para transmitir solicitudes OCSP y recibir respuestas OCSP.

Una implementación de cliente OCSP consta de:

- Estructuras de datos para gestionar información sobre los respondedores OCSP
- Funcionalidad para generar solicitudes OCSP
- Funcionalidad para procesar respuestas OCSP
- Funcionalidad para transmitir solicitudes OCSP y recibir respuestas OCSP

Cómo realiza Sterling B2B Integrator una comprobación de OCSP

Una comprobación de OCSP para un certificado en Sterling B2B Integrator se determina cuando se implementa la comprobación de OCSP en Sterling B2B Integrator como una parte de las API de sistema internas utilizadas por los servicios para obtener certificados y claves de la base de datos.

Acerca de esta tarea

Sterling B2B Integrator realiza comprobaciones de OCSP cuando se llama a los métodos para que obtengan certificados y claves de los objetos que los encapsulan en la base de datos.

Los pasos siguientes describen cómo se implementa la comprobación de OCSP en Sterling B2B Integrator:

Procedimiento

1. El sistema examina el objeto que encapsula el certificado para determinar si la comprobación de OCSP está habilitada. Esto permite que el sistema decida sin ninguna llamadas de base de datos adicional si se debe intentar una comprobación de OCSP.
2. Si la comprobación de OCSP está habilitada, el sistema obtiene el nombre de emisor codificado de un certificado.
3. El sistema realiza hash en el nombre de emisor codificado con SHA1.
4. El sistema intenta encontrar una entidad emisora configurada en el sistema que tenga un nombre cuyo hash coincida con el del certificado.
5. Si no se encuentra ninguna entidad emisora, no se realiza ninguna comprobación.
6. Si se encuentra una entidad emisora, el sistema comprueba la política OCSP para la entidad emisora. Si la política permite o requiere comprobaciones de OCSP, consulte la tabla CERT_AUTHORITY para obtener más información. El sistema intenta encontrar un respondedor OCSP para la entidad emisora.
7. Si no se encuentra ningún respondedor OCSP para la entidad emisora, se produce una de las situaciones siguiente :
   - Si la política de entidad emisora está establecida en comprobar siempre, se genera una excepción y la comprobación falla.
   - Si la política de entidad emisora es realizar la comprobación sólo cuando se ha configurado un respondedor, no se lleva a cabo ninguna comprobación.

- Si se encuentra un respondedor OCSP para la entidad emisora, se intenta una comprobación de OCSP.

Tablas de base de datos

Se han añadido CERT_AUTHORITY y OCSP_RESPONDER para gestionar la información relacionada con OCSP.

Se han añadido dos tablas de base de datos nuevas para gestionar la información relacionada con OCSP:

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

La tabla CERT_AUTHORITY mantiene la información acerca de las entidades emisoras de certificados.

Columna	Tipo	Descripción
OBJECT_ID	VARCHAR (255)	Se trata de un GUID que constituye un ID exclusivo para un registro. Es la clave primaria. No puede ser nulo.
NAME	VARCHAR (255)	Un nombre para un registro. Se permite nulo.
CREATE_DATE	DATETIME	Una fecha de creación para un registro.
MODIFIED_DATE	DATETIME	La fecha en la que un registro se ha modificado por última vez.
MODIFIED_BY	VARCHAR(255)	Información sobre quién ha modificado un registro.
ISSUER_NAME	BLOB	El nombre distinguido relativo (RDN) de la entidad emisora tomada del certificado.
HASH_ALG	VARCHAR(128)	El algoritmo hash utilizado para calcular los hashes de nombre y clave. Sólo se soporta SHA1.
RDN_HASH	VARCHAR(255)	Hash SHA1 codificado en BASE64 el nombre distinguido relativo (RDN) de emisor codificado DER tomado del certificado de la entidad emisora. Esta columna está indexada.
KEY_HASH	VARCHAR(255)	Hash SHA1 codificado en BASE64 de la clave pública codificada del certificado del emisor
CERT_OID	VARCHAR(255)	OBJECT_ID del certificado de la entidad emisora en la tabla CA_CERT_INFO. Cada entidad emisora debe tener un certificado CA en la base de datos. No se permiten nulos.

Columna	Tipo	Descripción
OCSP_POLICY	VARCHAR(128)	La política OCSP para la entidad emisora. Consta de dos valores separados por coma. Los valores describen cuándo hay que utilizar OCSP y qué se debe comprobar. Los valores posibles son: **OCSP_When** • never – no utilizar nunca OCSP • resp – sólo utilizar OCSP si se ha configurado un respondedor cuando se realiza una solicitud • always – utilizar siempre OCSP cuando se realiza una solicitud. Esto requiere que esté configurado un respondedor y, si no se ha configurado ninguno, hará que falle una comprobación de certificado **OCSP_What** • none – no comprobar nunca los certificados • end-user - comprobar sólo los certificados de usuario final • both – comprobar los certificados de usuario final e intermedios. Actualmente no se soporta • Nulo no está permitido en esta columna
CRL_POLICY	VARCHAR(128)	Actualmente no se utiliza.

OCSP_RESPONDER

La tabla OCSP_RESPONDER mantiene la información acerca de los respondedores OCSP.

Columna	Tipo	Descripción
OBJECT_ID	VARCHAR (255)	Se trata de un GUID que constituye un ID exclusivo para un registro. Es la clave primaria. No puede ser nulo.
NAME	VARCHAR (255)	Un nombre para un registro. Se permite nulo.
CREATE_DATE	DATETIME	Una fecha de creación para un registro.
MODIFIED_DATE	DATETIME	La fecha en la que un registro se ha modificado por última vez.
MODIFIED_BY	VARCHAR(255)	Información sobre quién ha modificado un registro.
ISSUER_NAME	BLOB	El nombre distinguido relativo (RDN) de la entidad emisora tomada del certificado.
HASH_ALG	VARCHAR(128)	El algoritmo hash utilizado para calcular los hashes de nombre y clave. Sólo se soporta SHA1.

Columna	Tipo	Descripción
RDN_HASH	VARCHAR(255)	Hash SHA1 codificado en BASE64 el nombre distinguido relativo (RDN) de emisor codificado DER tomado del certificado de la entidad emisora. Esta columna está indexada.
KEY_HASH	VARCHAR(255)	Hash SHA1 codificado en BASE64 de la clave pública codificada del certificado del emisor
CERT_OID	VARCHAR(255)	OBJECT_ID del certificado de la entidad emisora en la tabla CA_CERT_INFO. Cada entidad emisora debe tener un certificado CA en la base de datos. No se permiten nulos.
CACHE_TTL	VARCHAR(64)	El tiempo en segundos que se permite que las respuestas OCSP vivan en la memoria caché de respuesta interna Si la columna es NULL, las respuestas OCSP sólo se almacenarán en la memoria caché durante 1 segundo, lo que en la práctica significa nada.
TRANS_PROF_OID	VARCHAR(255)	OBJECT_ID de un perfil en la base de datos GIS. Tiene que crear un perfil para el respondedor OCSP que incluya el URL correcto para el respondedor.
COMM_BP	VARCHAR(255)	Nombre de un proceso de negocio a utilizar para comunicarse con el respondedor OCSP. Éste tiene que ser un proceso de negocio que realice comunicaciones HTTP. Los servicios del proceso de negocio tienen que estar configurados para no requerir o presentar cabeceras HTTP al enviar y recibir, respectivamente. Se puede utilizar y se recomienda el proceso HTTPClientSend que viene con el sistema
COMM_WAIT	VARCHAR(24)	El número de segundos a esperar a que se produzca la comunicación con el respondedor OCSP antes de deducir que algo no es correcto.

Configuración OCSP

Puede crear autorizaciones y respondedores sin límite cuando configure el sistema para utilizar OCSP.

Acerca de esta tarea

Al configurar el sistema, puede crear tantas autorizaciones y respondedores como desee.

Si desea configurar el sistema para utilizar OCSP:

Procedimiento

1. Compruebe el certificado para la entidad emisora de certificados que emite los certificados que desea incorporar con OCSP en Sterling B2B Integrator para verificar que es un certificado de la entidad emisora de certificados.
2. Liste los certificados CA del sistema y obtenga el ID de objeto para el certificado que acaba de instalar.
3. Si el certificado para firmas de respuesta OCSP de la entidad emisora es diferente del certificado de emisión de certificados de la entidad emisora, incorpore el certificado de firmas de respuesta OCSP de la entidad emisora en Sterling B2B Integrator como un certificado de confianza.

   Nota: Con la versión 5.2.4.2 y superiores, puede incorporar el certificado raíz que ha emitido el certificado de respondedor como CA en lugar del certificado de respondedor como un Certificado de confianza. Puesto que el certificado de respondedor cambia con frecuencia, en función de la CA, puede hacer que OCSP falle hasta que el certificado sea sustituido por otro que sea válido. En adelante, debería incorporar siempre un certificado raíz como práctica habitual, ya que raramente cambian. No obstante, ambos tipos siguen estando permitidos.
4. Si ha incorporado un certificado para firmas OCSP adicional, liste los certificados CA del sistema y obtenga el ID de objeto para el certificado que acaba de instalar.
5. Vaya al directorio bin de la instalación de Sterling B2B Integrator.
6. Inicie la base de datos si es necesario.
7. Inicie el shell bash o el shell Bourne.
8. Busque el origen del archivo tmp.sh
9. Cree una entidad emisora utilizando el programa de utilidad en la clase com.sterlingcommerce.security.ocsp.SCICertAuthority.
10. Cree un respondedor OCSP utilizando el programa de utilidad de la clase com.sterlingcommerce.security.ocsp.SCIOCSPResponder
11. Actualice los certificados de la entidad emisora o los certificados individuales para habilitar OCSP. El programa de utilidad com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo configurará todos los certificados de confianza y de sistema para una entidad emisora. El programa de utilidad com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo configurarán 1 certificado de sistema. El programa de utilidad com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo configurará 1 certificado de confianza.

Scripts de configuración OCSP

Se han incluido los scripts siguientes con la revisión de OCSP para ejecutar los programas de utilidad de configuración de OCSP. Existe una versión UNIX/Linux y Windows de cada script. Los scripts toman los mismos argumentos de línea de mandatos que el programa de utilidad que invocan. Los scripts se encuentran en el directorio bin de la instalación de producto. La información sobre los argumentos de línea de mandatos sólo se repite esencialmente en esta sección que describe los scripts.

ManageCertAuthority.sh y ManageCertAuthority.cmd

Argumento	Descripción

-a, -r, -d	Operación a realizar: -a añadir -l listar -d suprimir La opción –l no toma argumentos adicionales. La opción -d toma un solo argumento: el ID de objeto del registro a suprimir
Nombre	Nombre de la entidad emisora. Es necesario con -a.
Modified_by	Usuario que ha modificado o creado la identidad. Es necesario con -a.
Hash_alg	Algoritmo hash para la entidad emisora. Sólo se soporta el valor “SHA1”. Es necesario con -a.
Certificate_id	ID de objeto del certificado CA asociado con la entidad emisora. Es necesario con -a.
OCSP_policy	Serie de política OCSP para la entidad emisora. Es una serie delimitada por comas como se describe en el apartado que trata sobre la tabla CERT_AUTHORITY. Es necesario con -a. Para el primer elemento de la serie, se permite lo siguiente: • never – no utilizar nunca OCSP • resp – sólo utilizar OCSP si se ha configurado un respondedor cuando se realiza una solicitud • always – utilizar siempre OCSP cuando se realiza una solicitud. Esto requiere que esté configurado un respondedor y, si no se ha configurado ninguno, hará que falle una comprobación de certificado Para el segundo elemento de la serie, se permite lo siguiente: **OCSP What** • none – no comprobar nunca los certificados • end-user - comprobar sólo los certificados de usuario final • both – comprobar los certificados de usuario final e intermedios. Actualmente no se soporta. Ejemplos: • never,none • always,end-user

Crl_policy	Serie de política CRL para la entidad emisora. Es necesario con -a. Se necesita un valor para este argumento, pero actualmente no se utiliza. “None” es aceptable.
Object_ID	ID de objeto a utilizar al crear este registro. Opcional con -a.

ManageOCSPResponder.sh y ManageOCSPResponder.cmd

Argumento	Descripción
-l	Obtiene una lista de los respondedores OCSP configurados actualmente. Esta opción no toma argumentos adicionales.
-d	Suprime el respondedor OCSP configurado con el ID de objeto proporcionado para los datos de configuración de respondedores. Esta opción toma object_id como un argumento adicional.
-u2	Actualiza los registros existentes en la base de datos con la información correcta sobre la clave pública del certificado de entidad emisora y el DN de asunto del certificado de entidad emisora. Es necesario que se ejecute en todos los registros existentes para la entidad emisora de certificados y los respondedores OCSP o deberá suprimir y volver a crear los registros para poner la información correcta en la base de datos. Esta opción toma object_id como un argumento adicional.
-a	Añade datos de configuración para un nuevo respondedor OCSP que se utilizará para comprobar el estado de los certificados emitidos por la entidad emisora proporciona. Los argumentos adicionales son 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 y object_id.
name	(Necesario con -a) Nombre de la entidad emisora.
modified_by	(Necesario con -a) Usuario que ha modificado o creado la identidad.
hash_alg	(Necesario con -a) Algoritmo hash para la entidad emisora. Sólo se soporta el valor “SHA1”.

authority_cert_oid	(Necesario con -a) ID de objeto del certificado CA asociado con la entidad emisora.
response_signing_cert_oid	(Necesario con -a) ID de objeto del certificado que el proveedor de los servicios OCSP ha utilizado para firmar la respuesta que proporciona el estado de los certificados. Este certificado debe añadirse al almacén de certificados digitales CA o al almacén de certificados digitales de confianza. Es el ID de certificado de sistema para el certificado tal como aparece en el almacén.
resp_signing_cert_in_ca_store	(Necesario con -a) Distintivo que indica si el valor anterior del argumento response_signing_cert_oid se encuentra en el almacén de certificados digitales CA en Sterling B2B Integrator.
cache_ttl	(Necesario con -a) Tiempo de vida en segundos para las respuestas de OCSP en la memoria caché interna.
trans_prof_oid	(Necesario con -a) ID de objeto de un transporte configurado para comunicarse con el respondedor OCSP.
comm_bp	(Necesario con -a) Nombre del proceso de negocio a utilizar para comunicarse con el respondedor OCSP. Éste tiene que ser un proceso de negocio que realice comunicaciones HTTP. Los servicios del proceso de negocio tienen que estar configurados para no requerir o presentar cabeceras HTTP al enviar y recibir, respectivamente. Se puede utilizar y se recomienda el proceso HTTPClientSend que viene con el sistema.
comm_wait	(Necesario con -a) Número de segundos a esperar a que se produzca la comunicación con el respondedor antes de deducir que se ha producido un error.
send_nonce	(Necesario con -a) Indica si se enviará un valor NONCE al servicio OCSP. El valor NONCE se utiliza para evitar ataques de reproducción por parte de algunos proveedores de OCSP.
require_nonce	(Necesario con -a) Indica si el servidor debe requerir que el servicio OCSP proporcione un valor NONCE en la respuesta.
object_id	(Opcional con -a) ID de objeto a utilizar al crear este registro.

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

Este programa de utilidad establecerá la información de OCSP en la base de datos para un único certificado de sistema

Argumento	**Descripción**

Este programa de utilidad establecerá la información de OCSP en la base de datos para un único certificado de sistema

-o, -n	Cómo interpretar el segundo argumento: -o object_ID -n name
Object_ID/Name	ID o nombre de objeto de la entidad emisora como se determina en el argumento 1.

SetSystemCertOCSPInfo.sh y SetTrustedCertOCSPInfo.cmd

Este programa de utilidad establecerá la información de OCSP en la base de datos para un único certificado de sistema

Argumento	Descripción
-o, -n	Cómo interpretar el segundo argumento: -o object_ID -n name
Object_ID/Name	ID o nombre de objeto de la entidad emisora como se determina en el argumento 1.

Ejecutar un script OCSP

El ejemplo siguiente muestra cómo ejecutar los scripts de configuración OCSP. Estos scripts presuponen que ya ha incorporado los certificados CA para la entidad emisora, ha iniciado la base de datos, se encuentra en el directorio bin de la instalación de Sterling B2B Integrator y tiene el origen del archivo tmp.sh en el directorio bin.

Acerca de esta tarea

Después de obtener de la entidad emisora el ID de objeto del certificado CA, en Sterling B2B Integrator desde el **Menú de administración**, seleccione **Socios comerciales > Certificados digitales CA**. Seleccione un certificado. El recuadro de diálogo Resumen de certificado aparece con la información de certificado, incluida el ID de objeto.

Realice los pasos siguientes para ejecutar un script OCSP. Para obtener una lista de los mandatos de script OCSP, consulte “Scripts de configuración OCSP” en la página 84.

Procedimiento

1. Ejecute un mandato similar al siguiente para crear una entidad emisora en el sistema:

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

2. Después de crear una entidad emisora y de crear un perfil para comunicarse con un respondedor OCSP, ejecute un mandato similar al siguiente para crear un respondedor OCSP en el sistema:

   ```
   ./ManageOCSPResponder.sh -a CertAuth_TestOCSP admin SHA1
   "kenny:node1:13727b3f8e4:29762" "kenny:node1:13727275fd9:40698" false (utilice
   true si el certificado de firma incorporado
   ```

```
es el mismo certificado que el del respondedor, es decir, incorporado en
la entidad emisora de certificados en el paso 3) "2400" "14ffd4a0:1371823040d:-
77c8"
HTTPClientSend 3600 false false
```

3. Ejecute un mandato similar al siguiente para listar todas las entidades emisoras del sistema:

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

   Se visualiza salida de retorno para cada entidad emisora:

   ```
   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. Utilice un mandato similar al siguiente para habilitar OCSP para todos los certificados de sistema y de confianza emitidos por la entidad emisora:

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

Lógica de comprobación de OCSP

Los pasos siguientes describen la lógica de comprobación de OCSP en Sterling B2B Integrator. Si el estado de certificado es correcto, la comprobación de OCSP se realiza satisfactoriamente. De lo contrario, falla.

Procedimiento

1. Si se encuentra una respuesta existente cuyo tiempo de vida no ha caducado, se utiliza esa respuesta como respuesta OCSP.
2. Si no se encuentra ninguna respuesta existente en la memoria caché o el tiempo de vida ha caducado para una respuesta en la memoria caché, se crea una solicitud OCSP.
3. Si el sistema crea una solicitud OCSP, inicia el proceso de negocio configurado para que el respondedor OCSP envíe la solicitud y obtenga la respuesta. Las solicitudes incluirán un valor nonce si el respondedor se ha configurado para que se envíe uno.
4. Si el proceso de negocio se completa satisfactoriamente, el sistema intenta analizar el documento principal como una respuesta OCSP. El proceso de negocio utilizado para enviar solicitudes OCSP y recibir respuestas OCSP quita las cabeceras HTTP de la respuesta.
5. Si el documento primario se puede analizar como una respuesta OCSP, el sistema comprueba el estado de la respuesta.
6. Si el estado de la respuesta indica que la solicitud ha generado una respuesta válida, el sistema intenta verificar la firma en la respuesta OCSP utilizando el certificado configurado para el respondedor OCSP.
7. Si se ha verificado la firma y el respondedor se ha configurado para que necesite nonce, el sistema intenta obtener y comprobar el nonce de la respuesta.

8. Si todas las demás verificaciones han pasado, el sistema busca la información de estado del certificado para el que se ha construido y enviado la solicitud.
9. Si se encuentra la información de estado, el sistema ha actualizado la memoria caché interna para una respuesta OCSP existente para el certificado.

FIPS (Federal Information Processing Standards)

FIPS (Federal Information Processing Standards) 140-2

Para ajustarse a los requisitos de seguridad de FIPS 200, las aplicaciones deben utilizar módulos criptográficos certificados por el Cryptographic Module Validation Program (Programa de validación de módulo criptográfico) y compatibles con FIPS 140-1 o 140-2.

Los requisitos mínimos para el uso de la criptografía validada por parte de las aplicaciones son:

- Todas las operaciones criptográficas, incluida la generación de claves, deben ser realizadas por módulos criptográficos validados.
- Sólo se permiten funciones de seguridad aprobadas.
- Sólo se permiten técnicas de establecimiento de clave apropiadas.

FIPS 140-2 con Sterling B2B Integrator

GSE (Government Service Edition) de Certicom es un módulo criptográfico certificado FIPS 140-2 de nivel 1 que se distribuye con Sterling B2B Integrator. GSE es un kit de herramientas criptográficas de bajo nivel escrito en Java que implementa diversas funciones de seguridad, incluidas las funciones de seguridad no aprobadas.

Cuando se está en modalidad FIPS, realiza las tareas siguientes:

- Habilita la máquina de estado FIPS GSE e invoca autopruebas de encendido.
- Dirige las llamadas de función criptográficas del sistema de núcleo a GSE.

Habilitar FIPS durante la instalación

Durante una instalación nueva, cuando se le solicite si desea ejecutar en modalidad FIPS, seleccione TRUE.

Habilitar la modalidad FIPS manualmente

Puede habilitar la modalidad FIPS manualmente después de instalar Sterling B2B Integrator. Antes de empezar, verifique que tiene una licencia para operar en modalidad FIPS antes de que se habilite. El sistema comprueba la licencia durante el arranque y no se inicia si la modalidad FIPS está habilitada pero no tiene licencia.

Acerca de esta tarea

Para habilitar manualmente la modalidad FIPS:

Procedimiento

1. Vaya a */dir_instalación*/properties/.
2. Localice el archivo security.properties.
3. Abra el archivo security.properties en un editor de texto. Si realiza cambios en el archivo security.properties, asegúrese de hacer los mismos cambios en el

archivo security.properties.in. Esto impedirá que se sobrescriban los valores personalizados. Debe utilizar el archivo de propiedades de seguridad para personalizar FIPS en lugar de editar directamente los archivos de propiedades.

4. Especifique las configuraciones siguientes: FIPSMode=true
5. Guarde y cierre el archivo security.properties.
6. Reinicie Sterling B2B Integrator. Esto es necesario para que se reconozcan los cambios en el sistema.

Inhabilitar la modalidad FIPS

Puede inhabilitar manualmente la modalidad FIPS.

Acerca de esta tarea

Para inhabilitar manualmente la modalidad FIPS:

Procedimiento

1. Vaya a */dir_instalación*/properties/.
2. Localice el archivo security.properties.
3. Abra el archivo security.properties en un editor de texto.
4. Especifique las configuraciones siguientes: FIPSMode=false
5. Guarde y cierre el archivo security.properties.
6. Reinicie Sterling B2B Integrator. Esto es necesario para que se reconozcan los cambios en el sistema.

Servidores proxy

Servidores proxy

Los servidores proxy amplían la seguridad del sistema.

Configurar servidor proxy HTTP

Puede configurar un servidor proxy HTTP desde el menú **Administración**.

Acerca de esta tarea

Para configurar un servidor proxy HTTP:

Procedimiento

1. En el **Menú de administración**, seleccione **Operaciones** > **Servidores proxy**.
2. Pulse **añadir**.
3. Entre el **Nombre** del servidor proxy.
4. Seleccione **HTTP** como **Tipo**.
5. Entre el nombre de **Host**. Las direcciones IPV6 se deben escribir entre corchetes.
6. Entre el número de **Puerto**.
7. Entre el **Número de reintentos**.
8. Pulse **Siguiente**.
9. Si desea solicitar autenticación básica para el usuario:
   - Seleccione **Sí** y pulse **Siguiente**.
   - Si selecciona No (valor predeterminado), pulse **Siguiente** y vaya al Paso 13.

10. Entre el **ID de usuario de autenticación**.
11. Entre la **Contraseña de autenticación**.
12. Pulse **Siguiente**.
13. Revise los valores de servidor proxy.
14. Pulse **Finalizar**.

Configurar servidor proxy SSP

Puede configurar un servidor proxy SSP desde el menú **Administración**.

Acerca de esta tarea

Para configurar un servidor proxy SSP:

Procedimiento

1. En el **Menú de administración**, seleccione **Operaciones** > **Servidores proxy**.
2. Pulse **añadir**.
3. Entre el **Nombre** del servidor proxy.
4. Seleccione **SSP** como **Tipo**.
5. Entre el nombre de **Host**. Las direcciones IPV6 se deben escribir entre corchetes.
6. Entre el número de **Puerto**.
7. Entre el **Número de reintentos**.
8. Pulse **Siguiente**.
9. Si es necesaria la autenticación básica para el usuario, seleccione Sí o, de lo contrario, seleccione No.
10. Si es necesario SSL, seleccione Sí o, de lo contrario, seleccione No.
11. Pulse **Siguiente**.
12. Si ha seleccionado la autorización básica para este usuario, debe entrar el **ID de usuario de autenticación** y la **Contraseña de autenticación** y pulsar **Siguiente**. Si no necesita esta autorización, esta página no se visualizará.
13. Si selecciona que Sí es necesario SSL, debe seleccionar la **Intensidad del cifrado**, **Certificados CA**y **Certificados de clave** y pulsar **Siguiente**. Si selecciona que SSL no es necesario, esta página no se visualizará.
14. Pulse **Siguiente**.
15. Revise los valores de servidor proxy.
16. Pulse **Finalizar**.

Configurar un servidor proxy para SSL

Puede utilizar SSL con su configuración de servidor proxy SSP creando o importando un certificado SSL y estableciendo el campo **Usar SSL** en la configuración de adaptador apropiada en **Debe**.

Acerca de esta tarea

Si decide utilizar SSL con la configuración de servidor proxy SSP, debe:

Procedimiento

1. Crear un certificado SSL o importar el certificado de la entidad emisora de certificados a Sterling B2B Integrator.

2. Establezca el campo **Usar SSL** en la configuración de adaptador apropiada en **Debe**.

Editar servidores proxy

Puede editar un servidor proxy desde el menú **Administración**.

Acerca de esta tarea

Para editar una configuración de servidor proxy:

Procedimiento

1. En el **Menú de administración**, seleccione **Operaciones** > **Servidores proxy**.
2. Pulse **Editar** para el servidor proxy que desea editar.
3. Actualice los campos, según sea necesario.
4. Pulse **Siguiente**.
5. Revise los valores de servidor proxy.
6. Pulse **Finalizar**.

Suprimir servidores proxy

Acerca de esta tarea

Al suprimir una configuración de servidor proxy se pueden producir errores en algunas características de Sterling B2B Integrator. Es posible que tenga que volver a configurar adaptadores y servicios específicos para que funcionar correctamente sin una configuración de servidor proxy específica.

Para editar una configuración de servidor proxy:

Procedimiento

1. En el **Menú de administración**, seleccione **Operaciones** > **Servidores proxy**.
2. Pulse **suprimir** para el servidor proxy que desea editar.
3. Revise los valores de servidor proxy.
4. Pulse **Suprimir**.

SSL

Sobre la implementación de SSL en Sterling B2B Integrator

Secure Sockets Layer (SSL) proporciona comunicaciones seguras a través de Internet. Utiliza criptografía simétrica y asimétrica.

El protocolo SSL proporciona autenticación de servidor y autenticación de cliente en Sterling B2B Integrator:

- La autenticación de servidor se lleva a cabo cuando un cliente se conecte al servidor. Después del reconocimiento inicial, el servidor envía el certificado digital al cliente. El cliente valida el certificado de servidor o la cadena de certificados.
- Se realiza la autenticación de cliente cuando un servidor envía una solicitud de certificado a un cliente durante el reconocimiento. Si se verifica el certificado de cliente o la cadena y se verifica el mensaje de verificación de certificado, el reconocimiento continúa.

- Se realiza una autenticación opcional adicional comparando el nombre común en el certificado con el nombre de dominio totalmente calificado del servidor desde una búsqueda DNS (Servidor de nombres de dominio) inversa donde se puede obtener el nombre de dominio totalmente calificado del servidor.

Tipos de confianza

Se da soporte a dos tipos de confianza para certificados SSL en Sterling B2B Integrator:

- Confianza de CA – Confianza jerárquica basada en un certificado raíz utilizado para emitir otros certificados. Éste es el modelo de confianza de certificado SSL estándar.
- Confianza directa: Confianza directa de certificados de firma personal que se supone que se distribuirán a través de mecanismos seguro fuera de banda seguros. La confianza directa y los certificados de firma personal no forman parte de los estándares SSL, pero se utilizan frecuentemente en determinadas comunidades comerciales.

Certificados SSL

Para comunicarse utilizando SSL, configure los sistemas implicados para dar soporte a la autenticación de servidor o la autenticación de cliente/servidor. Para realizar la autenticación en un servidor, necesita un Certificado de entidad emisora de certificados (CA) raíz y el conjunto de certificados intermedios en la cadena o, si el servidor utiliza un certificado de firma personal, una copia del certificado de firma personal.

Para permitir la autenticación de cliente/servidor, necesita un certificado CA o de firma personal y un certificado de sistema.

Puede obtener un certificado SSL de una entidad emisora de certificados de confianza proporcionando una Solicitud de firma de certificado (CSR) a la entidad emisora de certificados. El certificado SSL enlaza la clave pública y el servidor o cliente SSL.

Si piensa utilizar la autenticación de cliente/servidor, configure un certificado de sistema. Puede crear certificados de sistema de las maneras siguientes:

- Incorporar un archivo PKCS12 o un archivo de certificado de claves existente
- Generar un certificado de sistema de firma personal
- Utilice Key Management Utility (iKeyman) para generar un CSR y obtener un certificado de CA. Para obtener información sobre iKeyman, consulte “IBM Key Management Utility (iKeyman)” en la página 63.

Suites de cifrado

Para poder utilizar Sterling B2B Integrator, es necesario que revise previamente las listas de cifras predefinidas disponibles y personalizarlas según los requisitos de seguridad de la empresa.

Las suites de cifrado SDK de IBM, Java Technology Edition, Versión 7 se pueden encontrar aquí: http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html. Para otras SDK soportadas en Sterling B2B Integrator, consulte la documentación del proveedor de JDK para ver una lista de suites de cifrado soportadas.

Las intensidades de cifrado se configuran en `security.properties` o en `customer_overrides.properties`. Los niveles de suites de cifrados disponibles son:

- AllCipherSuite (la selección UI es **ALL**) - incluye todo lo que aparece listado en WEAK y STRONG.
- WeakCipherSuite (la selección UI es **WEAK**) - Añade suites de cifrado débiles que desea utilizar con Sterling B2B Integrator
- StrongCipherSuite (la selección UI es **STRONG**) - Añade suites de cifrado fuertes que desea utilizar con Sterling B2B Integrator
- CipherSuiteDefault (disponible en V5.2.6 and higher) - de forma predeterminada, incluye un subconjunto de cifrados soportados para IBM JDK7. Se utiliza si WeakCipherSuite e StrongCipherSuite están vacíos.

Adaptadores de cliente para SSL

El adaptador de cliente FTP, el adaptador de cliente HTTP y el adaptador de solicitante Sterling Connect:Direct FTP+ (con la opción Secure+) dan soporte a SSL.

Los adaptadores de cliente siguientes soportan SSL:

- Adaptador de cliente FTP
- Adaptador de cliente HTTP
- Adaptador de solicitante de Sterling Connect:Direct FTP+ (con la opción Secure+)

Los parámetros para SSL se pueden establecer en el perfil de socio comercial o para el adaptador. Para el adaptador de cliente FTP, estos parámetros se establecen en el servicio para empezar sesión de cliente FTP. Para el adaptador de cliente HTTP, estos parámetros se establecen en el servicio para empezar sesión de cliente HTTP. Los parámetros establecidos en el servicio para empezar sesión sustituyen los valores de un perfil de socio comercial.

Los parámetros de la tabla siguiente controlan SSL desde una perspectiva de cliente. Consulte la documentación del adaptador o servicio específico que está configurando.

Parámetro	**Descripción**
SSL	Determina la negociación de socket SSL.
CACertificateId (trusted_root)	Lista de certificados públicos de CA de confianza. En los datos de proceso, este parámetro se muestra como un ID de objeto.
CipherStrength	El nivel de cifrado que se debe aplicar a los datos que fluyen a través de la conexión de socket.
SystemCertificateId	Selecciónelo en la lista de certificados de sistema disponibles. Este certificado confirma la identidad del cliente al servidor.

Adaptadores de servidor para SSL

El adaptador de servidor FTP, el adaptador de servidor HTTP, el adaptador de servidor Sterling Connect:Direct (con la opción Secure+) y el adaptador de envío SMTP dan soporte a SSL.

Los siguientes adaptadores de servidor soportan SSL:

- Adaptador de servidor FTP

- Adaptador de servidor HTTP
- Adaptador de servidor Sterling Connect:Direct (con la opción Secure+)
- Adaptador de envío SMTP

Los parámetros de la tabla siguiente controlan SSL desde una perspectiva de servidor. Consulte la documentación del adaptador o servicio específico que está configurando.

Parámetro	Descripción
SSL	Indica si SSL está activo.
Frase de contraseña de certificado de clave	Contraseña que protege el certificado de clave de servidor. El sistema utiliza internamente esta frase de contraseña para inicializar las bibliotecas SSL.
CipherStrength	Intensidad de los algoritmos utilizados para cifrar datos.
Certificado de clave (Almacén del sistema)	Clave privada y certificado para la autenticación de servidor.
Certificado CA	Certificado utilizado, si existe, para validar el certificado de un cliente.

Incorporar un certificado

Para permitir la autenticación de cliente/servidor, necesita un certificado CA o de firma personal y un certificado de sistema.

Acerca de esta tarea

Puede incorporar un certificado CA o un certificado de firma personal a un almacén de certificados CA seleccionando **Socio comercial** > **Certificados digitales** > **CA** > **Incorporar certificado nuevo** en el **Menú de administración**.

Crear certificados de firma personal para pruebas

Para realizar pruebas, puede utilizar certificados de firma personal. Se pueden generar y gestionar en Sterling B2B Integrator.

Acerca de esta tarea

Para crear un certificado de firma personal:

Procedimiento

1. Seleccione **Socios comerciales** > **Certificados digitales** > **Certificados de sistema** > **Crear certificado de firma personal**.
2. Una vez que se ha creado, búsquelo y extráigalo en un archivo.
3. Vuelva a incorporar el certificado en Sterling B2B Integrator como un certificado CA seleccionando **Socios comerciales** > **Certificados digitales** > **CA** > **Incorporar certificado nuevo**.

Renegociación SSL/TLS (V5.2.6 o posterior)

Sterling B2B Integrator utiliza los parámetros de IBM JSSE para controlar el grado de restricción de la renegociación SSL/TLS. Los parámetros siguientes están disponibles para su actualización en el archivo `security.properties`.

Nombre de parámetro	Definición	Valores válidos
com.ibm.jsse2.extended.renegotiation.indicator	Utilice esta propiedad para forzar todas negociaciones que requieran RFC 5746, no solo las renegociaciones. Esta negociación solo sería práctica si todos los socios necesarios en la comunicación implementan RFC 5746. El valor predeterminado es OPTIONAL.	Los valores válidos son: • BOTH - Hace que el servidor IBM JSSE2 o el cliente IBM JSSE2 se conecte únicamente si el igual de la conexión ha indicado soporte para la renegociación RFC 5746. Nota: establecer la propiedad en BOTH provoca problemas de interoperabilidad con los clientes o servidores que no se han actualizado para dar soporte a RFC 5746. • CLIENT - Hace que el cliente IBM JSSE2 se conecte únicamente si el servidor ha indicado soporte para la renegociación RFC 5746. Nota: establecer la propiedad en CLIENT provoca problemas de interoperabilidad con los servidores que no se han actualizado para dar soporte a RFC 5746. • OPTIONAL - Este es el valor predeterminado. Utilizar esta opción significa que el servidor IBM JSSE2 o el cliente IBM JSSE2 no requiere el indicador de renegociación durante el reconocimiento inicial. • SERVER - Hace que el servidor IBM JSSE2 se conecte únicamente si el cliente ha indicado soporte para la renegociación RFC 5746. Nota: establecer la propiedad en SERVER provoca problemas de interoperabilidad con los clientes que no se han actualizado para dar soporte a RFC 5746.

Nombre de parámetro	Definición	Valores válidos
com.ibm.jsse2.renegotiate	Utilice esta propiedad para cambiar la posibilidad de renegociación de IBM JSSE2. El valor predeterminado es NONE.	Los valores válidos son: • ABBREVIATED - Este valor sustituye al existente y permite el reconocimiento abreviado no seguro durante la renegociación cuando se demuestra la continuidad de la sesión. Se permiten las renegociaciones RFC 5746. • ALL - Este valor sustituye al existente y permite el reconocimiento completo no seguro, y el reconocimiento abreviado no seguro, durante la renegociación. Se permiten las renegociaciones RFC 5746. • DISABLED - Este valor sustituye e inhabilita todas las renegociaciones no seguras y RFC 5746. • NONE - Este es el valor predeterminado. No se permite la renegociación de reconocimiento no seguro. Solo se permiten las renegociaciones RFC 5746.
com.ibm.jsse2. renegotiation .peer.cert.check	Utilice esta propiedad para cambiar la posibilidad de renegociación de IBM JSSE2 para requerir el soporte de igual especificado en RFC 5746. Este requisito solo es práctico si todos los socios necesarios en la comunicación han implementado RFC 5746. El valor predeterminado es OFF.	Los valores válidos son: • OFF - Este es el valor predeterminado. Detiene el cliente IBM JSSE2 o el servidor IBM JSSE2 que realiza una comprobación de identidad del certificado del igual. El resultado es permitir cambiar el certificado de igual durante la renegociación. • ON - Este valor hace que el cliente IBM JSSE2 o el servidor IBM JSSE2 realiza una comparación del certificado del igual. La razón es garantizar que el certificado no cambia durante la renegociación. La comparación es aplicable a las renegociaciones, tanto seguras como no seguras.

Resolución de problemas de SSL

Si recibe un mensaje de error, puede intentar solucionar el problema SSL.

Mensajes de error de certificado corrupto o inutilizable

Si recibe el siguiente mensaje de error:

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

La información del registro de perímetro (Perimeter) es la siguiente:

```
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)
```

Cuando se incorpora el certificado, Sterling B2B Integrator muestra un valor de estado de "Invalid Signature" en la pantalla de denominación. Si falla un proceso de negocio que realiza una POST HTTP de salida con SSL en el servicio de método HTTP con error, se visualiza el siguiente mensaje:

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

Obtenga el certificado CA adecuado para el socio comercial. Si el socio comercial está utilizando un certificado de firma personal, se puede utilizar el propio certificado como certificado CA.

CA y confianza directa

Cuando Sterling B2B Integrator es el cliente, si el servidor tiene un certificado emitido por una entidad emisora de certificados y dicho certificado tiene el nombre DNS del servidor en el asunto Nombres distinguidos relativos (RDN), puede poner el certificado CA raíz en el almacén de CA y confiar en el mismo. Si SSL aún no funciona, intente la confianza directa. Ponga el certificado de servidor en el almacén de CA y confíe en él.

Si el servidor está utilizando un certificado de firma personal, póngalo en el almacén de CA y confíe en él. En este caso también está realizando la confianza directa.

Uso de SSL sin certificado

No puede utilizar adaptadores habilitados para SSL sin tener el certificado o el certificado de sistema necesarios.

SSL no funciona con una suite de cifrado basada en CBC

Si ha seleccionado la suite de cifrado de modalidad CBC y SSL no funciona, debe desactivar la protección CBC.

Para V5.2.5 e inferior, realice los pasos siguientes:

1. Abra el archivo tmp.sh para editarlo.
2. Busque el distintivo de servidor para el sistema operativo que está configurando y añada el valor siguiente:

   ```
   -DDisableSSLEmptyRecords=true
   ```

3. Guarde y cierre el archivo.

Para V5.2.6 y superior, realice los pasos siguientes:

1. En el directorio <*Instalación B2Bi*>/bin, localice `InstallNoappsWindowsService.cmd.in` y `InstallContainerWindowsService.cmd.in` para Windows; localice `tmp.sh_platform_ifcresources_ext.in` para todos los demás sistemas operativos.
2. Edite el archivo para cambiar todas las instancias de la propiedad siguiente por false:

   ```
   jsse.enableCBCProtection=true
   ```

3. Ejecute el script `setupfiles`.

Configuración HTTPS para el GPM

El acceso HTTP seguro a través de SSL ya se soporta para la mayoría de aplicaciones web en Sterling B2B Integrator en el puerto HTTP base + 1.

Esta mejora de SSL:

- Habilita HTTPS (HTTP con cifrado SSL) para el Modelador de procesos gráficos (GPM)
- Permite inhabilitar y redirigir las aplicaciones web en el puerto HTTP base a otro puerto (utilizando HTTPS)
- Soporta el acceso seguro a las aplicaciones web mediante el despliegue de las aplicaciones web en una instancia de adaptador de servidor HTTP seguro
- Reduce los riesgos de seguridad

Si utiliza esta característica, deberá configurar el Modelador de procesos gráficos (GPM) para que se comunique con la aplicación web de panel de instrumentos utilizando HTTPS en lugar de HTTP. El acceso a las aplicaciones web desplegadas a través de un adaptador de servidor HTTP seguro puede ser más lento que cuando se accede en el puerto de base.

Nota: En V5.2.6 y superior, el protocolo de seguridad predeterminado es TLS 1.2 (para puerto HTTP de base + 1.). Si es necesario, puede cambiarlo por TLS 1.1 o TLS 1.0 actualizando el parámetro **`jsseProtocol`** en `properties_platform_ifcresources_ext`. Los valores válidos incluyen los parámetros siguientes:

- **`TLS1-TLS1.1`** - para TLS1.0 y TLS1.1
- **`TLS1.1-TLS1.2`** - para TLS1.1 y TLS1.2
- **`TLS1`** - para TLS1.0 únicamente
- **`TLS1.1`** para TLS1.1 únicamente
- **`TLS1.2`** - para TLS1.2 únicamente

Nuevos parámetros SSL

Se han añadido varios parámetros nuevos para la característica SSL mejorada. Debe configurar estos parámetros para facilitar la comunicación SSL entre el Modelador

de procesos gráficos (GPM) y el servidor. Estos parámetros nuevos deben definirse en sus respectivos archivos de propiedades.

Todas las propiedades personalizadas para el entorno se deben establecer en el archivo customer_overrides.properties para que no se sobrescriban durante una instalación de actualización o de parche. Las propiedades definidas en el archivo sandbox.cfg no se deben definir en customer_overrides.properties, ya que en customer_overrides.properties se ignorarán. Estas propiedades son las únicas que no están definidas en customer_overrides.properties.

La siguiente tabla describe los nuevos parámetros de SSL y proporciona el nombre del archivo de propiedades donde se puede encontrar el parámetro.

Nombre de parámetro	**Definición**	**Archivo de propiedades**
WEBAPP_LIST_PORT	Identifica el puerto que el cliente GPM debe utilizar para la comunicación con el servidor. Toma de forma predeterminado el puerto base durante la instalación. Si las aplicaciones web de panel de instrumentos y GPM se han desplegado en una instancia de adaptador de servidor HTTP seguro, este parámetro se debe modificar para que coincida con el puerto de la instancia de adaptador de servidor HTTP seguro. Si el puerto SSL base (puerto HTTP base +1) está siendo utilizado para el despliegue seguro de las aplicaciones GPM y de panel de instrumentos, este parámetro se debe modificar para que coincida con el puerto SSL base (SSL_PORT en sandbox.cfg).	Archivo sandbox.cfg
WEBAPP_PROTOCOL	Identifica el protocolo que se debe utilizar para la comunicación con la aplicación web de panel de instrumentos (http/https).	Archivo sandbox.cfg

Nombre de parámetro	Definición	Archivo de propiedades
SKIP_BASEPORT_ DEPLOYMENT_WARS	Indica qué aplicaciones web se deben omitir durante el despliegue de war en el puerto base. La lista de archivos war está delimitada por comas, es sensible a las mayúsculas y minúsculas y no tiene el sufijo .war. El valor predeterminado es no omitir ningún war. Después de que se hayan desplegado satisfactoriamente las aplicaciones web de panel de instrumentos y GPM en un adaptador de servidor HTTP seguro, este parámetro puede establecerse en =admin,dashboard,gbm para eliminar el acceso a esas aplicaciones web en el puerto base. La lista completa de aplicaciones web incluye: • myaft • portlets El valor ALL puede utilizarse como comodín para indicar que todos los war desplegados en el puerto HTTP base se deben omitir. Es posible que esto no sea necesario si el puerto base está bloqueado para el acceso externo. El valor ALL no se debe utilizar con ningún otro valor.	customer_overrides.properties
HTTPS_REDIRECT_WARS	Indica los war que se redirigirán automáticamente del puerto HTTP base al puerto SSL base o adaptador de servidor HTTP seguro. El valor ALL puede utilizarse para redirigir todos los war omitidos en el puerto HTTP base a HTTPS_LIST_PORT (el puerto SSL base o adaptador de servidor HTTP seguro). El valor ALL no se debe utilizar con ningún otro valor.	customer_overrides.properties
HTTPS_LIST_PORT	Indica el puerto de destino redirigido para las solicitudes realizadas en el puerto HTTP base. Se debe establecer en el valor del adaptador de servidor HTTP seguro o el puerto SSL base.	customer_overrides.properties

Nombre de parámetro	Definición	Archivo de propiedades
HTTPS_CLIENT_CERTS	Lista separada por comas de certificados de sistema cuyas claves públicas deben añadirse al almacén de confianza predeterminado. Estos certificados se utilizan para la verificación del lado de cliente durante el reconocimiento SSL cuando se inician llamadas HTTPS desde el servidor independiente del servidor de aplicaciones (ASI) que regresan al mismo. Este parámetro necesita claves de certificado de servidor que tengan un **SubjectAltName**. Si utiliza claves existentes sin este parámetro, esta funcionalidad fallará con mensajes muy confusos. **Nota:** El certificado configurado para HTTPS en puertoBase+1 (sslCert) se añade automáticamente al almacén de confianza y no necesita añadirse a esta lista.	customer_overrides.properties

Al configurar esta característica, si sólo define SKIP_BASEPORT_DEPLOYMENT_WARS, pero no HTTPS_REDIRECT_WARS y HTTPS_LIST_PORT, las aplicaciones web serán inaccesibles en el puerto base y el usuario no se redirigirá automáticamente al puerto HTTPS. Se trata de un escenario válido, si el usuario prefiere no redirigir automáticamente por razones de seguridad. Las aplicaciones web seguirán estando disponibles cuando se acceda a las mismas en el adaptador de servidor HTTP o el puerto SSL base.

Habilitar la redirección automática a HTTPS

Puede permitir la redirección automática a HTTPS.

Acerca de esta tarea

Se ha añadido soporte para permitir configurar una redirección automática a HTTPS para las aplicaciones web que se despliegan en un puerto seguro (puerto SSL base o de adaptador de servidor Http) y se omite en el puerto base. Esta configuración es opcional, pero se recomienda encarecidamente.

Nota: Todas las propiedades personalizadas para el entorno se deben establecer en el archivo customer_overrides.properties para que no se sobrescriban durante una instalación de actualización o de parche.

Para permitir la redirección automática a HTTPS:

Procedimiento

1. Vaya a `/<dir_instalación>/install/properties`.
2. Abra el archivo customer_overrides.properties y establezca los siguientes valores de parámetro que se indican a continuación:

```
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
HTTPS_LIST_PORT=<puerto_adaptador_servidor_http o puerto_ssl_base>
```

Estos parámetros están configurados para redirigir automáticamente un usuario a la instancia HTTPS de la aplicación web.

Nota: El archivo customer_overrides.properties no forma parte del código de sistema predeterminado. Se debe crear después de la instalación de sistema inicial y llenar para que coincida con el entorno.

3. Guarde y cierre el archivo.

Ejemplo de implementación

Ejemplo de implementación en el archivo customer_overrides.properties:

```
## Identifica los war para la redirección automática al puerto https.
## Utilice una lista separada por comas para especificar varios war
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica el puerto https para los war redirigidos. Si se especifica, éste
## debe coincidir con WEBAPP_LIST_PORT en sandbox.cfg
HTTPS_LIST_PORT=<puerto_adaptador_servidor_http o puerto_ssl_base>
```

Nota: Si se utiliza una instancia de adaptador de servidor HTTP segura, la configuración indica que todos los archivos war especificados como HTTPS_REDIRECT_WARS se deben desplegar en la misma instancia de adaptador de servidor HTTP.

HTTPS_CLIENT_CERTS

Si se utiliza una instancia de adaptador de servidor HTTP seguro, el certificado SSL utilizado para configurar la instancia de adaptador de servidor HTTP seguro debe añadirse a la lista de certificados de confianza.

Esto es necesario porque algunas de las pantallas del panel de instrumentos realizan llamadas https en el servidor ASI. Para que estas llamadas completen el reconocimiento SSL correctamente, los certificados se deben configurar en el almacén de confianza en el servidor ASI. Esta operación se realiza especificando el nombre de certificado en la lista HTTPS_CLIENT_CERTS.

Estos certificados de sistema deben tener los nombres DNS y la dirección o las direcciones IP especificados como nombres alternativos cuando se crea el certificado de sistema. La verificación de nombre de host SSL predeterminada proporcionada por el JDK requiere que el nombre del certificado presentado por el servidor SSL coincida con el nombre de host utilizado en el URL http o una de las series del atributo "SubjectAltName" en el certificado. Algunas pantallas del panel de instrumentos no funcionará sin la configuración de "SubjectAltName".

Los nombres alternativos se configuran a través de los campos "Lista de direcciones IP separadas por coma" y "Lista de nombres DNS separados por coma" en el asistente de creación de certificado de sistema (**Socio comercial** > **Certificados digitales** > **Sistema**).

Soporte HTTPS para el GPM

Java Web Start (JavaWS) se emplea para iniciar el GPM (Graphical Process Modeler - Modelador de procesos gráficos) utilizando HTTP. Soporta HTTPS y la importación dinámica de certificados de forma similar a los navegadores.

Durante el reconocimiento SSL, el servidor proporciona el certificado y JavaWS maneja la verificación de confianza. Si JavaWS no ha podido verificar el certificado,

se solicita al usuario que lo acepte o lo rechace. JavaWS no puede verificar automáticamente los certificados SSL y los usuarios deben verificarlos.

Importar certificados para Java Web Start

Si desea evitar una solicitud de certificado sin confianza durante la operación de Java Web Start (JavaWS), puede importar los certificados al almacén de máquina local antes de iniciar el Modelador de procesos gráficos (GPM).

Acerca de esta tarea

Esto puede reducir la confusión del usuario en el caso de que la máquina local del usuario no confíe en el certificado SSL asociado con el adaptador de servidor HTTP o el puerto SSL de base seguro.

Para importar certificados de raíz de confianza a JavaWS:

Procedimiento

1. Guarde el certificado de raíz de confianza en un archivo del sistema local.
2. Abra el **Panel de control de Java** en el sistema local (javaws.exe bajo `jre\bin`).
3. Abra el separador **Seguridad** y pulse **Certificados**.
4. Pulse **Importar** para examinar un certificado de raíz de confianza y selecciónelo.
5. Pulse **Abrir** para importar el nuevo certificado de raíz de confianza. Después de que se incorpore el certificado de raíz de confianza, JavaWS lo utiliza para la verificación de confianza durante el reconocimiento SSL.

Conmutar de HTTP a HTTPS utilizando el puerto SSL base

Puede conmutar de HTTP a HTTPS utilizando el puerto SSL base.

Acerca de esta tarea

Para conmutar de HTTP a HTTPS utilizando el puerto SSL base:

Procedimiento

1. Vaya a `/dir_instalación/install/properties`.
2. Abra el archivo sandbox.cfg.
3. Modifique los parámetros siguientes:

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

   El GPM (Modelador de procesos gráficos) utiliza estos parámetros para la comunicación con el servidor.
4. (Opcional, recomendado) Si desea desactivar el acceso a las aplicaciones web GPM y de panel de instrumentos en el puerto base y configurar la redirección automática al puerto HTTPS, especifique los parámetros siguientes en un archivo customer_overrides.properties:

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

Por ejemplo:

```
## Identifica los archivos war que se deben saltar durante el despliegue en el puerto de base.
## Utilizar la lista separada por comas para especificar varios war
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica los war para la redirección automática al puerto https.
## Utilice una lista separada por comas para especificar varios war
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica el puerto https para los war redirigidos. Si se especifica, éste
## debe coincidir con WEBAPP_LIST_PORT en sandbox.cfg
noapp.HTTPS_LIST_PORT=<puerto_base + 1>
```

5. Guarde y cierre el archivo.
6. Vaya a `/dir_instalación/install/bin`.
7. Detenga Sterling B2B Integrator.
8. Aplique los cambios de configuración. Escriba `./setupfiles.sh`.
9. Despliegue la nueva configuración. Escriba `./deployer.sh`.
10. Inicie Sterling B2B Integrator.
11. (Opcional) Si ha desactivado el acceso a las aplicaciones web GPM y de panel de instrumentos en el puerto base (Paso 4), verifique los cambios que ha efectuado. Por ejemplo, puede verificar:
    - El acceso de aplicación web de panel de instrumentos en http://host:baseport/dashboard es inaccesible o se redirige a https://host:<puerto_base + 1>/dashboard automáticamente.
    - El acceso de aplicación web GPM en http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp es inaccesible o se redirige a https://host:<puerto_base + 1>/gbm/pmodeler/ProcessModeler.jnlp automáticamente.

Conmutar de la modalidad HTTP a HTTPS utilizando un adaptador de servidor HTTP seguro

Puede conmutar de la modalidad HTTP a HTTPS utilizando un adaptador de servidor HTTP seguro.

Acerca de esta tarea

Para conmutar de la modalidad HTTP a la modalidad HTTPS:

Procedimiento

1. Cree una nueva instancia de adaptador de servidor HTTP con SSL habilitado. Debe configurar los siguientes parámetros como se especifica a continuación:
   - **Autenticación de usuario necesaria** se establece en **No**
   - **Usar SSL** se establece en **Debe**
2. Despliegue los archivos WAR necesarios en la instancia de adaptador de servidor HTTP con SSL habilitado.

   Nota: Todos los archivos WAR deben seleccionarse en el directorio `/dir_instalación/install/noapp/deploy` cuando configure la instancia de adaptador de servidor HTTP. Además, el nombre de contexto de la aplicación web de administración debe coincidir con el parámetro ADMIN_CONTEXT_PATH del archivo `/dir_instalación/install/properties/sandbox.cfg`. Para todas las demás aplicaciones web, el nombre de contexto debe ser el nombre del archivo war sin la extensión ".war".

   Esto es necesario para que los cambios realizados a través de un parche o revisión se reflejen automáticamente en el despliegue de adaptador de servidor HTTP.

Los archivos WAR necesarios incluyen:

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

Es posible que se necesiten archivos WAR adicionales para soportar las nuevas funciones que ha añadido al panel de instrumentos.

3. Abra el archivo sandbox.cfg y modifique los parámetros siguientes:

```
WEBAPP_PROTOCOL=https
WEBAPP_LIST_PORT=<puerto_adaptador_servidor_http_seguro>
```

Estos parámetros los utilizan el GPM para comunicarse con el servidor.

4. (Opcional, recomendado) Si desea desactivar el despliegue de las aplicaciones web GPM y de panel de instrumentos en el puerto de base, especifique los siguientes parámetros en el archivo customer_overrides.properties:

```
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=<puerto_adaptador_servidor_http_seguro>
```

Por ejemplo:

```
## Identifica los archivos war que se deben saltar durante el despliegue en el puerto de base.
## Utilizar la lista separada por comas para especificar varios war
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica los war para la redirección automática al puerto https.
## Utilice una la lista separada por comas para especificar varios war
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica el puerto https para los war redirigidos.
## Si se especifica, debe coincidir con WEBAPP_LIST_PORT en sandbox.cfg
noapp.HTTPS_LIST_PORT=<puerto_adaptador_servidor_http_seguro>
```

5. Si desea utilizar un certificado distinto para esta función, cambie `/dir_instalación/install/properties/customer_overrides.properties` por la línea siguiente: *noapp.sslCert={nombre_mención_de_su_propio_certificado}*. Si no especifica un certificado distinto, la función utiliza ASISslCert.
6. (Opcional) Si desea enviar cookies desde el navegador utilizando un protocolo seguro como HTTPS, vaya a `/dir_instalación/install/properties` y especifique el siguiente parámetro en un archivo customer_overrides.properties:

```
## enviar cookies como seguros a través de https
http.useSecureCookie=true
```

7. Vaya a `/dir_instalación/install/bin`.
8. Detenga Sterling B2B Integrator.
9. Aplique los cambios de configuración. Escriba `./setupfiles.sh`.
10. Despliegue la nueva configuración. Escriba `./deployer.sh`.
11. Inicie Sterling B2B Integrator.
12. Verifique que se puede acceder a la aplicación web de panel de instrumentos a través del adaptador de servidor HTTP accediendo a https://host:<*puerto_adaptador_servidor_http_seguro*>/dashboard.

13. Verifique que se puede acceder a la aplicación web GPM a través del adaptador de servidor HTTP seguro accediendo a https://host:<*puerto_adaptador_servidor_http_seguro*>/gbm/pmodeler/ProcessModeler.jnlp.
14. Guarde y cierre el archivo.
15. Si ha desactivado el despliegue de las aplicaciones web GPM y de panel de instrumentos en el puerto de base (Paso 4), verifique lo siguiente:
    - El acceso de aplicación web de panel de instrumentos en http://host:baseport/dashboard se redirige a https://host:<*puerto_adaptador_servidor_http_seguro*>/dashboard automáticamente.
    - El acceso de aplicación web GPM en https://host:puerto_seguro/gbm/pmodeler/ProcessModeler.jnlp se redirige automáticamente a https://host:<*puerto_adaptador_servidor_http_seguro*>/gbm/pmodeler/ProcessModeler.jnlp.

Conmutar de la modalidad HTTPS a la modalidad HTTP

Puede conmutar de la modalidad HTTPS a la modalidad HTTP.

Acerca de esta tarea

Para conmutar de la modalidad HTTPS a la modalidad HTTP:

Procedimiento

1. Vaya a `/dir_instalación/install/properties`.
2. Abra el archivo **sandbox.cfg**.
3. Modifique los parámetros siguientes:
   ```
   WEBAPP_PROTOCOL=http
   WEBAPP_LIST_PORT=<puerto_base>
   ```
4. Guarde y cierre el archivo.
5. (Opcional) Si se ha desactivado el despliegue de las aplicaciones web GPM y de panel de instrumentos en el puerto base al conmutar a la modalidad HTTPS, debe abrir el archivo customer_overrides.properties y poner un signo de comentario en los parámetros siguientes para que no se apliquen:

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

6. (Opcional) Guarde y cierre el archivo.
7. Vaya a `/dir_instalación/install/bin`.
8. Detenga Sterling B2B Integrator.
9. Aplique los cambios de configuración. Escriba `./setupfiles.sh`.
10. Despliegue la nueva configuración. Escriba `./deployer.sh`.
11. Inicie Sterling B2B Integrator.
12. Verifique lo siguiente:
    - Se puede acceder a la aplicación web de panel de instrumentos en http://host:baseport/dashboard
    - Se puede acceder a la aplicación web GPM en http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp
13. (Opcional) Retirar el despliegue de las aplicaciones web de la instancia de adaptador de servidor HTTP habilitado para SSL.

Módulo de seguridad de hardware (HSM) V5.2.3 - 5.2.5

Módulo de seguridad de hardware (HSM)

HSM es un dispositivo de seguridad basado en hardware que genera, almacena y protege las claves criptográficas. Puede almacenar certificados de sistema en una base de datos utilizando Sterling B2B Integrator o en un HSM.

Sterling B2B Integrator soporta los siguientes dispositivos HSM:

- SafeNet Eracom ProtectServer Orange External
- Dispositivos PCI ProtectServer Gold

Puede utilizar el HSM para:

- Crear certificados de sistema en el HSM
- Importar certificados de sistema de Sterling B2B Integrator
- Exportar certificados de sistema de Sterling B2B Integrator
- Eliminar certificados de sistema de HSM
- Ver detalles de certificado de sistema para certificados del HSM

Características de Sterling B2B Integrator para soporte HSM

Sterling B2B Integrator almacena una entrada en la tabla CERTS_AND_PRI_KEY para cada par de claves y certificado.

Esta entrada contiene información sobre:

- Claves y certificados, incluyendo el período de validez, el número de serie, las restricciones de uso, el emisor y el asunto utilizados por la interfaz de usuario para mostrarlos al usuario sin tener que acceder realmente a la clave o al certificado.
- Normalizaciones del nombre distinguido utilizado por el sistema en las búsquedas
- Modificaciones en el registro.
- Información de estado de revocación de certificado.
- Tipo de almacén de claves.
- Referencias a un objeto de almacén de claves binario almacenado en DATA_TABLE. Cuando se utiliza un almacén de claves de software, el objeto de referencia puede contener material clave. En el caso de un HSM, contiene información de referencia (nCipher) o un marcador (Eracom).

Parámetros de certificados de sistema HSM

La tabla siguiente proporciona los parámetros para los mandatos CreateSystemCert, ImportSystemCert y ExportSystemCert.

Parámetro	Descripción
autogen	Indica si se debe utilizar información generada por el sistema para controlar el acceso a la clave y al almacén de claves. Se debe establecer en false para las claves en los HSM.
alias	Nombre de clave almacenado en el HSM. Sólo los nombres de alias que contienen los caracteres a-z, A-Z, 0-9 o guión (-) y cuya longitud total no es superior a la longitud de GUID de sistema.

Parámetro	Descripción
Certtype	Tipo de certificado a importar. Se soportan cuatro tipos de archivos de certificado: pkcs12, pkcs8, pem y keystore. Sterling B2B Integrator sólo soporta claves pem cifradas con DES o 3DES. Utilice keystore para listar o importar el almacén de claves.
certname	Nombre a asignar al certificado en la base de datos de Sterling B2B Integrator.
file	Archivo PEM o keycert a importar.
keyname	Nombre de la clave de sistema de Sterling B2B Integrator a crear.
keypass	PIN para la señal que protege el HSM de SafeNet Eracom donde reside el almacén de claves.
key passphrase	Frase de contraseña para la clave privada. Este valor es opcional en la línea de mandatos. Si no se proporciona, se le solicitará. PIN para la señal en el HSM de SafeNet Eracom donde reside el almacén de claves.
keysize	Longitud, en bits, de los módulos RSA. Los valores válidos son 768, 1024, 2048, 3072 o 4096
keystoretype	Tipo de almacén de claves a importar. El valor válido es CRYPTOKI.
keystoreprovider	Tipo de proveedor. SafeNet Eracom es el único HSM soportado. ERACOM o ERACOM.n si está importando certificados a una ranura distinta de la ranura predeterminada 0.
keytype	Algoritmo de clave pública. RSA es el único algoritmo soportado.
ObjectID	ID del certificado de sistema.
pkcs12file	Archivo pkcs12 a importar.
password	Frase de contraseña de almacén para el archivo keycert o PEM.
pkcs12storepass	Frase de contraseña de almacén para el archivo PKCS12.
pkcs12keypass	Frase de contraseña utilizada para cifrar la clave privada en el archivo PKCS12.
provider	Proveedor del tipo de almacén de claves. ERACOM o ERACOM.n si está importando certificados a una ranura distinta de la ranura predeterminada 0.
rfc1779rdnsequence	El campo de serie de nombre distinguido contiene cualquiera de los campos identificados en la columna Valores válidos. Sólo es necesario el campo CN. Separe cada campo con una coma. Información válida: • CN = Nombre común • O = Organización • OU = Unidad organizativa • L = Ubicación • ST = Estado • C = País (proporcione un código alpha-2 ISO3166-1 de dos letras)
storetype	Tipo de almacén de claves. CRYPTOKI es el único tipo de almacén de claves soportado.
signingbit	Establece el bit de uso de clave de firma para el certificado de firma personal. Los valores válidos son true y false.

Parámetro	Descripción
serial	Número de serie de certificado.
system passphrase	Frase de contraseña de sistema de Sterling B2B Integrator. Este valor es opcional en la línea de mandatos.
store passphrase	Frase de contraseña para acceder al almacén de claves. PIN para la señal del HSM de SafeNet Eracom donde reside el almacén de claves. Este valor es opcional en la línea de mandatos.
systempass	Frase de contraseña de sistema de Sterling B2B Integrator.
storepass	PIN para la señal que protege el HSM de SafeNet Eracom donde reside el almacén de claves.
totrusttable	Determina si el certificado se añade a la tabla de certificados de confianza. Los valores válidos son true y false.
validityindays	Periodo de tiempo en días que el certificado es válido.

HSM de SafeNet Eracom

Para poder utilizar un HSM con Sterling B2B Integrator, debe configurar Sterling B2B Integrator para utilizar y reconocer el HSM de SafeNet Eracom.

Para instalar y configurar el HSM de SafeNet Eracom, siga las instrucciones proporcionadas por el proveedor; asegúrese de instalar Java Runtime. Utilice el proveedor para la ranura donde se almacenarán las claves de Sterling B2B Integrator al configurar y utilizar los programas de utilidad. Después de crear un PIN para la ranura de SafeNet Eracom, no cambie el PIN. Sterling B2B Integrator no puede acceder a una clave en el HSM si cambia el PIN.

La arquitectura de SafeNet Eracom divide el HSM en varias ranuras. Instale y configure las tarjetas o los HSM de acuerdo con las instrucciones del proveedor. Cada ranura tiene un proveedor de seguridad asociado y se puede proteger mediante un número de identificación personal (PIN) independiente. Puede crear una ranura independiente en el HSM para Sterling B2B Integrator y proteger la ranura con un PIN exclusivo. El proveedor de la ranura 0 predeterminada es ERACOM. Los proveedores de ranuras adicionales se denominan ERACOM.*n*, donde *n* es el número de la ranura. Asegúrese de que los componentes de Java Runtime están disponibles para interactuar con el dispositivo.

Configurar Sterling B2B Integrator para utilizar el HSM de SafeNet Eracom

Puede desea configurar Sterling B2B Integrator para utilizar el HSM de SafeNet Eracom.

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Añada las líneas siguientes a los archivos tmp.sh y tmp.sh.in:

   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib
   export LD_LIBRARY_PATH
   ```
3. Si está configurando un servidor basado en red, añada las siguientes líneas a los archivos tmp.sh y tmp.sh.in, donde *IP_o_nombre_host_dispositivo_red* es la dirección IP o el nombre de dominio totalmente calificado del servidor basado en red SafeNet Eracom:

   ```
   ET_HSM_NETCLIENT_SERVERLIST=IP_o_nombre_host_dispositivo_red
   ```

```
export ET_HSM_NETCLIENT_SERVERLIST
```

4. Copie jprov.jar del directorio /opt/Eracom/lib en el directorio */dir_instalación*/install/jdk/jre/lib/ext.
5. Añada una definición para cada proveedor de seguridad al archivo */dir_instalación*/install/bin/jdk/jre/lib/security/java.security. Para añadir una definición, identifique el número asignado al proveedor de Certicom y asigne n+1 al proveedor de SafeNet Eracom. Para todos los demás proveedores identificados después del proveedor de SafeNet Eracom, aumente el número de security.provider en 1.

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

   Si está utilizando una ranura distinta de cero en el HSM de SafeNet Eracom, especifique la ranura como se indica a continuación, donde *x* es el número de la ranura:

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

6. Defina TLSProviderPolicy en el archivo */dir_instalación*/install/properties/security.properties.
   - Si el proveedor se ha definido en la ranura 0, asegúrese de que la única línea no comentada para el parámetro TLSProviderPolicy es la siguiente:

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

   - Si el proveedor se ha definido en una ranura distinta de la 0, modifique el parámetro TLSProviderPolicy como se indica a continuación, donde *x* es la ranura que está configurando:

```
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. Defina el mandato KeyStoreProviderKey en el archivo */dir_instalación*/install/properties/security.properties:
   - Si el proveedor se ha definido en la ranura 0, asegúrese de que KeyStoreProviderMap se ha definido como:

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

   - Si el proveedor se ha definido en una ranura distinta de la 0, modifique el parámetro KeyStoreProviderMap como se indica a continuación, donde *x* es el número de ranura:

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

Dispositivos PCI y de red de SafeNet/Eracom y nCipher soportados

Sterling B2B Integrator soporta actualmente la tarjeta PCI ProtectServer Orange y el dispositivo de red Orange External de Safenet/Eracom, además de soportar nCipher.

Se soporta lo siguiente:

Fabricante	Tipos de dispositivos soportados
nCipher	• Serie nShield de tarjetas PCI • Dispositivos de red NetHSM
Safenet/Eracom	• Tarjeta PCI ProtectServer Gold • Tarjeta PCI ProtectServer Orange • Dispositivo de red ProtectServer Orange External

Utilizar un Módulo de seguridad de hardware

Crear certificados de sistema para almacenarlos en el HSM

Puede crear un certificado de sistema de firma personal para almacenarlo en el HSM.

Antes de empezar

Antes de empezar:

- Detenga Sterling B2B Integrator.
- Asegúrese de que la base de datos de Sterling B2B Integrator está en ejecución.

Acerca de esta tarea

Para crear un certificado de sistema de firma personal para almacenarlo en el HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [frase de contraseña de sistema] [frase de contraseña de almacén] [frase de contraseña de clave]`
3. Si no ha proporcionado la frase de contraseña de sistema, la frase de contraseña de almacén y la frase de contraseña de clave en la línea de mandatos, se le solicitará que las entre.

Listar certificados de sistema almacenados en el HSM

Puede listar información sobre los certificados de sistema almacenados en el HSM.

Acerca de esta tarea

Para listar información sobre los certificados de sistema almacenados en el HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Ejemplo

A continuación se muestra un ejemplo de la salida del mandato:

```
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
```

Importar un certificado de sistema HSM a la base de datos de Sterling B2B Integrator

Utilice este procedimiento cuando una clave y un certificado existen en el HSM y se han añadido al HSM independientemente de Sterling B2B Integrator. Debe importar la información de un certificado de sistema que está almacenado en un HSM a la base de datos para que Sterling B2B Integrator pueda utilizarla.

Acerca de esta tarea

En función del método utilizado para añadir la clave privada y el certificado al HSM, la función de lista puede mostrar entradas duplicadas para un solo par de clave y certificado.

Debe obtener el alias de certificado de sistema para poder importar información sobre un certificado de sistema a la base de datos.

Para importar el certificado de sistema:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

Eliminar certificados de sistema almacenados en el HSM

Puede suprimir de forma permanente el certificado de sistema del HSM. Los datos de clave privada que contiene no se pueden recuperar.

Acerca de esta tarea

Para eliminar un certificado de sistema almacenado en el HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./RemoveSystemCert.sh -r` *xxxx*

   Donde *xxxx* es el ID de objeto del certificado que desea eliminar.

Exportar certificados de sistema

Puede exportar certificados de sistema de Sterling B2B Integrator para que éstos se puedan importar al HSM.

Acerca de esta tarea

Los certificados de sistema en un HSM no se pueden exportar utilizando ExportSystemCert.sh.

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Escriba la frase de contraseña.

Ejemplo: Certificado de sistema HSM

Puede importar un certificado de sistema al HSM en formato keycert, pkcs12 o pem. La importación de un certificado de sistema añade la clave y el certificado al HSM y crea una entrada correspondiente en la base de datos de Sterling B2B Integrator.

Si importa una clave y un certificado de tipo pem, asegúrese de que la clave privada se crea en formato cifrado DES o DES triple.

A continuación se muestra un ejemplo de clave privada pem creada en formato DES triple:

```
-----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-----
```

Gestionar programas de utilidad de certificado de sistema

Pares de claves de HSM y solicitudes de firma de certificado

El programa de utilidad GenCSR genera un par de claves en un HSM y crea una solicitud de firma de certificado (CSR) PKCS10 con la clave pública de ese par de claves. Entonces puede someter la CSR a una entidad emisora de certificados (CA).

Cuando reciba un certificado emitido por la CA, utilice GenCSR para actualizar el certificado. El certificado de sistema no está disponible en Sterling B2B Integrator hasta que se actualiza con un certificado emitido por CA.

También puede utilizar este programa de utilidad para ver una lista de CSR, escribir información sobre una CSR en un archivo, suprimir una CSR o grabar en un archivo la información sobre un certificado emitido por CA almacenado en el HSM. La información acerca de las CSR se mantiene en la base de datos de Sterling B2B Integrator, mientras que las claves reales se almacenan en el HSM.

Para utilizar el programa de utilidad, primero determine qué acción desea realizar. A continuación, utilice el programa de utilidad GenCSR e identifique la acción en la línea de mandatos. Para cada acción, proporcione los argumentos necesarios para la acción en el archivo de propiedades. Se proporciona un archivo de propiedades de ejemplo denominado csr.properties.sample en el directorio */dir_instalación*/install/properties.

El programa de utilidad GenCSR puede encontrarse en el directorio */dir_instalación*/install/bin.

La sintaxis del mandato es: `GenCSR.sh -a ACTION -p PROPERTIES`

Parámetros de GenCSR

La tabla siguiente proporciona los parámetros utilizados al ejecutar el script GenCSR.

Parámetro	Descripción	Valores válidos
-a ACTION	Acción a realizar.	Las acciones válidas son: • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	Archivo de propiedades que contiene los parámetros adicionales necesarios para las acciones. Debe incluir la vía de acceso al archivo de propiedades.	Nombre de un archivo de propiedades. Por ejemplo: `csr_create.properties`

Actualizar el almacén de claves HSM con certificados emitidos por CA

Utilice el programa de utilidad GenCSR con el argumento de actualización para añadir información de certificado emitido por CA en el almacén de claves HSM.

Procedimiento

1. Asegúrese de que el archivo csr_update.properties se ha configurado correctamente.

   La tabla siguiente describe los parámetros necesarios en el archivo csr_update.properties para el argumento de actualización.

Parámetro	Descripción	Valores válidos
provider	Nombre del proveedor de almacén de claves.	ERACOM o ERACOM.n
keystoretype	Nombre del almacén de claves utilizado.	CRYPTOKI
certificate.request.Name	Nombre de la CSR a actualizar.	Nombre asignado a una CSR
add.trusted	Identifica si la información de certificado se añade a la tabla de certificados de confianza.	True | false
ca.cert.file	Vía de acceso y nombre del archivo donde se debe grabar la información sobre el certificado emitido por CA.	Vía de acceso y nombre de archivo válidos de un archivo de certificado emitido por CA

2. Actualice el almacén de claves HSM.

   La sintaxis del mandato es: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Listar solicitudes de firma de certificado

Utilice el programa de utilidad GenCSR con el argumento de lista para visualizar CSR en la base de datos de HSM. No se necesita ninguna configuración de archivo de propiedades para el argumento de lista.

Acerca de esta tarea

La sintaxis del mandato es: `./GenCSR.sh -a list`

Suprimir una solicitud de firma de certificado

Utilice el programa de utilidad GenCSR con el argumento de supresión (delete) para suprimir una CSR. Este programa de utilidad sólo suprime la CSR. No suprime los certificados de sistema que se han actualizado con un certificado emitido por CA.

Procedimiento

1. Asegúrese de que el archivo cacert.properties se ha configurado correctamente. Debe configurar el archivo de propiedades antes de utilizar el argumento de supresión. La tabla siguiente describe los parámetros necesarios en el archivo cacert.properties para el argumento de supresión.

Parámetro	Descripción	Valores válidos
certificate.request.Name	Nombre de la CSR a suprimir.	Nombre de una CSR
keystoretype	Nombre del almacén de claves utilizado.	CRYPTOKI
provider	Nombre del proveedor de almacén de claves.	ERACOM[.N]

2. Suprimir la CSR. La sintaxis de mandato es `./GenCSR.sh -a delete -p ../properties/cacert.properties`

Escribir información de CSR en un formato pkcs10

Utilice el programa de utilidad GenCSR con el argumento getpkcs10 para escribir un CSR en formato pkcs10 en el archivo especificado.

Procedimiento

1. Asegúrese de que el archivo csr_getpkcs10.properties se ha configurado correctamente.

   La tabla siguiente describe los parámetros necesarios en el archivo csr_getpkcs10.properties para el argumento getpkcs10. Debe configurar el archivo de propiedades antes de utilizar el argumento getpkcs10.

Parámetro	Descripción	Valores válidos
certificate.request.Name	Nombre de la CSR.	Nombre asignado a una CSR
keystoretype	Nombre del almacén de claves utilizado.	CRYPTOKI
csr.file	Vía de acceso completa al archivo en el que se debe escribir la información acerca de la CSR.	Vía de acceso y nombre de un archivo para escribir la información de CSR

2. Escriba la CSR en un archivo.

La sintaxis del mandato es `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Mover certificados de sistema al HSM

Puede mover certificados de firma personal o certificados emitidos por CA de la base de datos al HSM.

Acerca de esta tarea

Es más seguro para volver a generar claves y certificados utilizando CreateSystemCert.sh o GenCSR.sh.

Para mover certificados de firma personal o certificados emitidos por CA de la base de datos al HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Detenga Sterling B2B Integrator.
3. Inicie la base de datos.
4. Exporte el certificado de sistema a un archivo PKCS12:

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass
   pkcs12keypass
   ```
5. Busque el ID de objeto del certificado de sistema a eliminar. Escriba:

   ```
   ./RemoveSystemCert.sh -l.
   ```
6. Elimine el certificado de sistema de la base de datos. Escriba:

   `RemoveSystemCert.sh -r` *xxxx* Donde *xxxx* es el ID de objeto del certificado que desea eliminar.
7. Para importar el certificado de sistema que ha exportado al HSM y crear una entrada de base de datos correspondiente:

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

   Nota: Si mueve OpsDrv, OpsKey y UIKey al HSM, utilice el nombre exacto. De lo contrario, Sterling B2B Integrator no funcionará correctamente. Para todos los demás certificados de sistema, el nombre no es crítico. Al mover certificados de sistema distintos de OpsDrv, OpsKey y UIKey, el ID de objeto utilizado por servicios y adaptadores cambia. Vuelva a configurar los servicios que utilizan los certificados de sistema que se han eliminado.

Grabar certificado emitido por CA en un archivo

Utilice el programa de utilidad GenCSR con el argumento getcacert para grabar en un archivo el certificado emitido por la entidad emisora de certificados (CA).

Procedimiento

1. Asegúrese de que el archivo getcacert.properties se ha configurado correctamente.

   La tabla siguiente describe los parámetros necesarios en el archivo getcacert.properties para la acción getcacert. Debe configurar el archivo getcacert.properties antes de utilizar el argumento getcacert.

Parámetro	Descripción	Valores válidos
certificate.request.Name	Nombre de la CSR.	Nombre de certificado
keystoretype	Nombre del almacén de claves utilizado.	CRYPTOKI
ca.cert.file	Vía de acceso completa al archivo en el que se debe grabar la información acerca del certificado CA.	Nombre y vía de acceso de un archivo de certificado CA

2. Grabe el certificado en un archivo.

   La sintaxis del mandato es `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Generar certificados de sistema internos (OpsDrv, OpsKey, UIKey) en el HSM

Con Sterling B2B Integrator se instalan tres certificados de sistema para proteger las operaciones internas. El hecho de moverlos al HSM proporciona poca ventaja de seguridad. Su política de seguridad puede requerir que todos los certificados que contienen claves privadas se almacenen en el HSM.

Acerca de esta tarea

Al generar los certificados de sistema internos de Sterling B2B Integrator denominados OpsDrv, OpsKey y UIKey en el HSM, utilice los nombres exactos. De lo contrario, Sterling B2B Integrator no funcionará correctamente.

Para generar certificados de sistema internos:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Entre `./RemoveSystemCert.sh -l` para ver los certificados de la base de datos. Anote el ID de objeto para cada certificado de sistema.
3. Suprima los certificados de sistema de la base de datos ejecutando el siguiente mandato para cada certificado: `./RemoveSystemCert.sh -r` *xxxx* donde *xxxx* es el ID de objeto del certificado que desea eliminar.
4. Genere el certificado de sistema en el HSM para cada certificado, entrando:

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

Utilizar nCipher y SafeNetEracom

Correlación de proveedor de almacén de claves

Sterling B2B Integrator tiene el tipo de almacén de claves que es exclusivo entre los proveedores de servicios criptográficos; puede definir una correlación entre los tipos de almacén de claves y los proveedores necesaria para implementar el propio objeto de almacén de claves, los algoritmos de firma y los algoritmos de transporte clave.

El objeto de abstracción de información de clave y la clave contienen esta información con una referencia a com.sterlingcommerce.security.PrivateKeyInfo.

Esto permite a Sterling B2B Integrator utilizar una combinación de claves en los HSM y en los almacenes de software de la base de datos al mismo tiempo sin configuración adicional más allá de la carga inicial de la clave o la información de clave en la base de datos. Para Sterling B2B Integrator, todas las claves tienen el mismo aspecto, independientemente de dónde estén almacenadas.

La correlación se implementa como una propiedad denominada KeyStoreProviderMap en security.properties. Consta de un conjunto de entradas delimitadas por punto y coma (;). Cada entrada tiene seis elementos delimitados por comas y siguen este formato:

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

Los elementos se describen en la tabla siguiente:

Elemento	Descripción	Información adicional
KeyStoreType	Tipo de serie del almacén de claves	
KeyStoreProvider	Nombre del proveedor de servicio criptográfico que implementa el almacén de claves	
DoesAliasMatter	Indica si el alias de claves debe ser exclusivo para este tipo de almacén de claves	Este valor puede ser true o false. Las claves deben tener alias exclusivos en el caso de que sólo haya un almacén de claves por dispositivo.
SignatureProvider	Nombre del proveedor de servicio criptográfico a utilizar para crear firmas utilizando claves del almacén de claves	
EncryptionProvider	Nombre del proveedor de servicio criptográfico a utilizar al descifrar la información utilizando claves del almacén de claves	Esto es principalmente para operaciones de transporte de clave de RSA
KeyOnHSM	Indica si el almacén de claves está en un HSM	

La serie nula es un valor aceptable y se tratará como si no se hubiera especificado ningún proveedor. Una entrada debe tener como mínimo dos valores. Si una entrada contiene menos de seis valores, los valores se asignarán de izquierda a derecha al proveedor de almacén de claves, si el alias es importante al almacenar la clave, al proveedor de firmas, al proveedor de cifrado y si la clave están en un HSM para el tipo KeyStore. Los demás se tratarán como nulos y no se solicitará ningún proveedor específico para operaciones con claves de ese tipo.

El KeyStoreProviderMap predeterminado es actualmente:

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

Gestionar claves de HSM e información de claves

Sterling B2B Integrator tiene varios scripts java para gestionar las claves en los HSM.

A continuación, se listan los programas Java.

Programa	Finalidad
com.sterlingcommerce.db.RemoveSystemCert	Listar y suprimir certificados de sistema de Sterling B2B Integrator. Durante una supresión, el programa realiza el mejor esfuerzo para borrar la clave del almacén de claves y sobrescribir el objeto de almacén de claves en la base de datos.
com.sterlingcommerce.db.CreateCertEx	Generar un par de claves en un HSM y un certificado de firma personal que contenga la clave pública del par de claves.
com.sterlingcommerce.security.util. CertificateSigningRequest	Generar un par de claves en un HSM y crear y gestionar una solicitud de firma de certificado PKCS10 asociada. El PKCS10 se puede proporcionar a una entidad emisora para obtener un certificado firmado por la entidad emisora. Este programa se puede utilizar para cargar a continuación ese certificado en el almacén de claves y asociarlo con el par de claves correcto.
com.sterlingcommerce.db.ImportSystemCert	Importar una clave privada y un certificado en un formato soportado (PKCS12 o PEM) a un almacén de claves en un HSM. Importar información sobre una clave privada y un certificado de un HSM a la base de datos de Sterling B2B Integrator.

Cambios de JDK para soporte HSM de nCipher

Para que Sterling B2B Integrator utilice los HSM de nCipher, debe instalar los proveedores de servicio criptográfico java de nCipher. Para instalarlos, copie los siguientes archivos jar en el subdirectorio jre/lib/ext del JDK. Modifique java.security para cargar los proveedores nCipher.

El programa de instalación de nCipher pone los archivos siguientes en /opt/nfast/java/classes:

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

Debe añadir los proveedores nCipher después del proveedor IBM JCE y antes que el proveedor Certicom. Por ejemplo:

```
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
```

En los sistemas Solaris con el JDK de SUN, debe poner los proveedores nCipher después de los proveedores Sun JCA y JCE y antes de que el proveedor Certicom. Por ejemplo:

```
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
```

Configure una política TLSProvider utilizando el ejemplo en security.properties. Por ejemplo:

```
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
```

Cambios de JDK para soporte HSM de Eracom

Para que Sterling B2B Integrator utilice los HSM de Eracom, debe instalar el proveedor de servicio criptográfico java de Eracom. Para instalarlo, ponga los archivos .jar apropiados en el subdirectorio jre/lib/ext del JDK y, a continuación, modifique java.security para cargar los proveedores nCipher.

El programa de instalación de nCipher pone estos archivos en /opt/nfast/java/classes:

- jcprov.jar
- jprov.jar

Debe añadir el proveedor Eracom después del proveedor de Certicom. Por ejemplo:

```
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
```

Nota: Eracom tiene un proveedor que se puede especificar para cada ranura de la tarjeta. En el caso del proveedor para la ranura 8, utilice:

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

Cambios de entorno Linux para soporte HSM de nCipher

nCipher recomienda que cree una cuenta de usuario especial para ejecutar el hardserver de nCipher.

La cuenta desde la que ejecuta Sterling B2B Integrator necesita tener permisos equivalentes o es necesario que ejecute Sterling B2B Integrator desde la cuenta especial de nCipher o como root. Si realiza una de estas acciones y está utilizando MySQL, debe cambiar los permisos para MySQL o iniciar MySQL desde la cuenta normal antes de invocar run.sh.

Cambios de entorno Linux para soporte HSM de Eracom

Para utilizar el dispositivo Eracom, debe proporcionar información adicional en las variables de entorno a la sesión que accede al dispositivo.

Los cambios recomendados en PATH, LD_LIBRARY_PATH y MANPATH son los siguientes:

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

Además, si está utilizando un dispositivo de red en lugar de una tarjeta PCI local, debe proporcionar ET_HSM_NETCLIENT_SERVERLIST, como se indica a continuación:

```
ET_HSM_NETCLIENT_SERVERLIST=IP_o_nombreHost_dispositivo_red
```

Debe exportar estas variables a tmp.sh.

Módulo de seguridad de hardware (HSM) V5.2.6 o posterior

Módulo de seguridad de hardware (HSM)

HSM es un dispositivo de seguridad basado en hardware que genera, almacena y protege las claves criptográficas. Puede almacenar certificados de sistema en una base de datos utilizando Sterling B2B Integrator o en un HSM.

Sterling B2B Integrator soporta los siguientes dispositivos HSM:

- SafeNet Luna SA
- nCipher nShield Connect

Puede utilizar el HSM para:

- Crear certificados de sistema en el HSM
- Importar certificados de sistema de Sterling B2B Integrator
- Exportar certificados de sistema de Sterling B2B Integrator
- Eliminar certificados de sistema de HSM
- Ver detalles de certificado de sistema para certificados del HSM

Características de Sterling B2B Integrator para soporte HSM

Sterling B2B Integrator almacena una entrada en la tabla CERTS_AND_PRI_KEY para cada par de claves y certificado.

Esta entrada contiene información sobre:

- Claves y certificados, incluyendo el período de validez, el número de serie, las restricciones de uso, el emisor y el asunto utilizados por la interfaz de usuario para mostrarlos al usuario sin tener que acceder realmente a la clave o al certificado.
- Normalizaciones del nombre distinguido utilizado por el sistema en las búsquedas
- Modificaciones en el registro.
- Información de estado de revocación de certificado.
- Tipo de almacén de claves.
- Referencias a un objeto de almacén de claves binario almacenado en DATA_TABLE. Cuando se utiliza un almacén de claves de software, el objeto de referencia puede contener material clave. En el caso de un HSM, contiene información de referencia (nCipher) o un marcador (Luna).

Parámetros de certificados de sistema HSM

La tabla siguiente proporciona los parámetros para los mandatos CreateSystemCert, ImportSystemCert y ExportSystemCert.

Parámetro	Descripción
autogen	Indica si se debe utilizar información generada por el sistema para controlar el acceso a la clave y al almacén de claves. Se debe establecer en false para las claves en los HSM.
alias	Nombre de clave almacenado en el HSM. Sólo los nombres de alias que contienen los caracteres a-z, A-Z, 0-9 o guión (-) y cuya longitud total no es superior a la longitud de GUID de sistema.
Certtype	Tipo de certificado a importar. Se soportan cuatro tipos de archivos de certificado: pkcs12, pkcs8, pem y keystore. Sterling B2B Integrator sólo soporta claves pem cifradas con DES o 3DES. Utilice keystore para listar o importar el almacén de claves.
certname	Nombre a asignar al certificado en la base de datos de Sterling B2B Integrator.
file	Archivo PEM o keycert a importar.
keyname	Nombre de la clave de sistema de Sterling B2B Integrator a crear.
keypass	PIN para la señal que protege el HSM de SafeNet o nCipher donde reside el almacén de claves.
key passphrase	Frase de contraseña para la clave privada. Este valor es opcional en la línea de mandatos. Si no se proporciona, se le solicitará.
keysize	Longitud, en bits, de los módulos RSA. Los valores válidos son 1024, 2048, 3072 o 4096
keystoretype	Tipo de almacén de claves a importar. Los valores válidos son nCipher.sworld, Luna y PKCS11IMPLKS (5.2.6.2 en adelante).
keystoreprovider	Tipo de proveedor. Los valores válidos son nCipherKM, LunaProvider y IBMPKCS11Impl (5.2.6.2 en adelante).
keytype	Algoritmo de clave pública. RSA es el único algoritmo soportado.
ObjectID	ID del certificado de sistema.
pkcs12file	Archivo pkcs12 a importar.
password	Frase de contraseña de almacén para el archivo keycert o PEM.
pkcs12storepass	Frase de contraseña de almacén para el archivo PKCS12.
pkcs12keypass	Frase de contraseña utilizada para cifrar la clave privada en el archivo PKCS12.
provider	Proveedor del tipo de almacén de claves. Los valores válidos son nCipherKM, LunaProvider y IBMPKCS11Impl (5.2.6.2 en adelante).

Parámetro	Descripción
rfc1779rdnsequence	El campo de serie de nombre distinguido contiene cualquiera de los campos identificados en la columna Valores válidos. Sólo es necesario el campo CN. Separe cada campo con una coma. Información válida: • CN = Nombre común • O = Organización • OU = Unidad organizativa • L = Ubicación • ST = Estado • C = País (proporcione un código alpha-2 ISO3166-1 de dos letras)
storetype	Tipo de almacén de claves. Los valores válidos son nCipher.sworld, Luna y PKCS11IMPLKS (5.2.6.2 en adelante).
signingbit	Establece el bit de uso de clave de firma para el certificado de firma personal. Los valores válidos son true y false.
serial	Número de serie de certificado.
system passphrase	Frase de contraseña de sistema de Sterling B2B Integrator. Este valor es opcional en la línea de mandatos.
store passphrase	Frase de contraseña para acceder al almacén de claves. Este valor es opcional en la línea de mandatos. Si no se proporciona, se le solicitará.
systempass	Frase de contraseña de sistema de Sterling B2B Integrator.
storepass	PIN para la señal que protege el HSM de SafeNet o nCipher donde reside el almacén de claves.
totrusttable	Determina si el certificado se añade a la tabla de certificados de confianza. Los valores válidos son true y false.
validityindays	Periodo de tiempo en días que el certificado es válido.

Utilizar un Módulo de seguridad de hardware

Crear certificados de sistema para almacenarlos en el HSM

Puede crear un certificado de sistema de firma personal para almacenarlo en el HSM.

Antes de empezar

Antes de empezar:

- Detenga Sterling B2B Integrator.
- Asegúrese de que la base de datos de Sterling B2B Integrator está en ejecución.

Acerca de esta tarea

Para crear un certificado de sistema de firma personal para almacenarlo en el HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial`

```
validityindays [frase de contraseña de sistema]  [frase de contraseña de
almacén] [frase de contraseña de clave]
```

3. Si no ha proporcionado la frase de contraseña de sistema, la frase de contraseña de almacén y la frase de contraseña de clave en la línea de mandatos, se le solicitará que las entre.

Listar certificados de sistema almacenados en el HSM

Puede listar información sobre los certificados de sistema almacenados en el HSM.

Acerca de esta tarea

Para listar información sobre los certificados de sistema almacenados en el HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Ejemplo

A continuación se muestra un ejemplo de la salida del mandato:

```
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
```

Nota: A partir de V5.2.6.2 y en adelante el valor válido para Keystoretype es PKCS11IMPLKS.

Importar un certificado de sistema HSM a la base de datos de Sterling B2B Integrator

Utilice este procedimiento cuando una clave y un certificado existen en el HSM y se han añadido al HSM independientemente de Sterling B2B Integrator. Debe importar la información de un certificado de sistema que está almacenado en un HSM a la base de datos para que Sterling B2B Integrator pueda utilizarla.

Acerca de esta tarea

En función del método utilizado para añadir la clave privada y el certificado al HSM, la función de lista puede mostrar entradas duplicadas para un solo par de clave y certificado.

Debe obtener el alias de certificado de sistema para poder importar información sobre un certificado de sistema a la base de datos.

Para importar el certificado de sistema:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

Eliminar certificados de sistema almacenados en el HSM

Acerca de esta tarea

Este procedimiento suprime de forma permanente el certificado de sistema del HSM. Los datos de clave privada que contiene no se pueden recuperar.

Para eliminar un certificado de sistema almacenado en el HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./RemoveSystemCert.sh -r` *xxxx*

   Donde *xxxx* es el ID de objeto del certificado que desea eliminar.

Exportar certificados de sistema

Puede exportar certificados de sistema de Sterling B2B Integrator para que éstos se puedan importar al HSM.

Acerca de esta tarea

Los certificados de sistema en un HSM no se pueden exportar utilizando ExportSystemCert.sh.

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Escriba: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Escriba la frase de contraseña.

Ejemplo: Certificado de sistema HSM

Puede importar un certificado de sistema al HSM en formato keycert, pkcs12 o pem. La importación de un certificado de sistema añade la clave y el certificado al HSM y crea una entrada correspondiente en la base de datos de Sterling B2B Integrator.

Si importa una clave y un certificado de tipo pem, asegúrese de que la clave privada se crea en formato cifrado DES o DES triple.

A continuación se muestra un ejemplo de clave privada pem creada en formato DES triple:

```
-----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-----
```

Gestionar programas de utilidad de certificado de sistema

Pares de claves de HSM y solicitudes de firma de certificado

El programa de utilidad GenCSR genera un par de claves en un HSM y crea una solicitud de firma de certificado (CSR) PKCS10 con la clave pública de ese par de claves. Entonces puede someter la CSR a una entidad emisora de certificados (CA).

Cuando reciba un certificado emitido por la CA, utilice GenCSR para actualizar el certificado. El certificado de sistema no está disponible en Sterling B2B Integrator hasta que se actualiza con un certificado emitido por CA.

También puede utilizar este programa de utilidad para ver una lista de CSR, escribir información sobre una CSR en un archivo, suprimir una CSR o grabar en un archivo la información sobre un certificado emitido por CA almacenado en el HSM. La información acerca de las CSR se mantiene en la base de datos de Sterling B2B Integrator, mientras que las claves reales se almacenan en el HSM.

Para utilizar el programa de utilidad, primero determine qué acción desea realizar. A continuación, utilice el programa de utilidad GenCSR e identifique la acción en la línea de mandatos. Para cada acción, proporcione los argumentos necesarios para la acción en el archivo de propiedades. Se proporciona un archivo de propiedades de ejemplo denominado csr.properties.sample en el directorio */dir_instalación*/install/properties.

El programa de utilidad GenCSR puede encontrarse en el directorio */dir_instalación*/install/bin.

La sintaxis del mandato es: `GenCSR.sh -a ACTION -p PROPERTIES`

Parámetros de GenCSR

La tabla siguiente proporciona los parámetros utilizados al ejecutar el script GenCSR.

Parámetro	Descripción	Valores válidos
-a ACTION	Acción a realizar.	Las acciones válidas son: • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	Archivo de propiedades que contiene los parámetros adicionales necesarios para las acciones. Debe incluir la vía de acceso al archivo de propiedades.	Nombre de un archivo de propiedades. Por ejemplo: `csr_create.properties`

Actualizar el almacén de claves HSM con certificados emitidos por CA

Acerca de esta tarea

Utilice el programa de utilidad GenCSR con el argumento de actualización para añadir información de certificado emitido por CA en el almacén de claves HSM.

Procedimiento

1. Asegúrese de que el archivo csr_update.properties se ha configurado correctamente.

   La tabla siguiente describe los parámetros necesarios en el archivo csr_update.properties para el argumento de actualización.

Parámetro	Descripción	Valores válidos
provider	Nombre del proveedor de almacén de claves.	IBMPKCS11IMPL (a partir de V5.2.6.2 y en adelante) o nCipherKM o LunaProvider
keystoretype	Nombre del almacén de claves utilizado.	PKCS11IMPLKS (a partir de V5.2.6.2 y en adelante) o nCipher.sworld o Luna **Nota:** El valor 'keystoretype' debe ser síncrono con el valor 'provider'.
certificate.request.Name	Nombre de la CSR a actualizar.	Nombre asignado a una CSR
add.trusted	Identifica si la información de certificado se añade a la tabla de certificados de confianza.	True | false
ca.cert.file	Vía de acceso y nombre del archivo donde se debe grabar la información sobre el certificado emitido por CA.	Vía de acceso y nombre de archivo válidos de un archivo de certificado emitido por CA

2. Actualice el almacén de claves HSM.

   La sintaxis del mandato es: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Listar solicitudes de firma de certificado

Utilice el programa de utilidad GenCSR con el argumento de lista para visualizar CSR en la base de datos de HSM. No se necesita ninguna configuración de archivo de propiedades para el argumento de lista.

Acerca de esta tarea

La sintaxis del mandato es: `./GenCSR.sh -a list`

Suprimir una solicitud de firma de certificado

Utilice el programa de utilidad GenCSR con el argumento de supresión (delete) para suprimir una CSR. Este programa de utilidad sólo suprime la CSR. No suprime los certificados de sistema que se han actualizado con un certificado emitido por CA.

Procedimiento

1. Asegúrese de que el archivo cacert.properties se ha configurado correctamente. Debe configurar el archivo de propiedades antes de utilizar el argumento de supresión. La tabla siguiente describe los parámetros necesarios en el archivo cacert.properties para el argumento de supresión.

Parámetro	Descripción	Valores válidos
certificate.request.Name	Nombre de la CSR a suprimir.	Nombre de una CSR
keystoretype	Nombre del almacén de claves utilizado.	PKCS11IMPLKS (a partir de V5.2.6.2 y en adelante) o nCipher.sworld o Luna
provider	Nombre del proveedor de almacén de claves.	IBMPKCS11IMPL (a partir de V5.2.6.2 y en adelante) o nCipherKM o LunaProvider **Nota:** El valor 'keystoretype' debe ser síncrono con el valor 'provider'.

2. Suprimir la CSR. La sintaxis de mandato es `./GenCSR.sh -a delete -p ../properties/cacert.properties`

Escribir información de CSR en un formato pkcs10

Acerca de esta tarea

Utilice el programa de utilidad GenCSR con el argumento getpkcs10 para escribir un CSR en formato pkcs10 en el archivo especificado.

Procedimiento

1. Asegúrese de que el archivo csr_getpkcs10.properties se ha configurado correctamente.

   La tabla siguiente describe los parámetros necesarios en el archivo csr_getpkcs10.properties para el argumento getpkcs10. Debe configurar el archivo de propiedades antes de utilizar el argumento getpkcs10.

Parámetro	Descripción	Valores válidos
certificate.request.Name	Nombre de la CSR.	Nombre asignado a una CSR
keystoretype	Nombre del almacén de claves utilizado.	PKCS11IMPLKS (a partir de V5.2.6.2 y en adelante) o nCipher.sworld o Luna
csr.file	Vía de acceso completa al archivo en el que se debe escribir la información acerca de la CSR.	Vía de acceso y nombre de un archivo para escribir la información de CSR

2. Escriba la CSR en un archivo.

   La sintaxis del mandato es `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Mover certificados de sistema al HSM

Puede mover certificados de firma personal o certificados emitidos por CA de la base de datos al HSM.

Acerca de esta tarea

Es más seguro para volver a generar claves y certificados utilizando CreateSystemCert.sh o GenCSR.sh.

Para mover certificados de firma personal o certificados emitidos por CA de la base de datos al HSM:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Detenga Sterling B2B Integrator.
3. Inicie la base de datos.
4. Exporte el certificado de sistema a un archivo PKCS12:

   ```
   ./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass
   pkcs12keypass
   ```
5. Busque el ID de objeto del certificado de sistema a eliminar. Escriba:

   ```
   ./RemoveSystemCert.sh -l.
   ```
6. Elimine el certificado de sistema de la base de datos. Escriba:

   `RemoveSystemCert.sh -r` *xxxx* Donde *xxxx* es el ID de objeto del certificado que desea eliminar.
7. Para importar el certificado de sistema que ha exportado al HSM y crear una entrada de base de datos correspondiente:

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

   Nota: Si mueve OpsDrv, OpsKey y UIKey al HSM, utilice el nombre exacto. De lo contrario, Sterling B2B Integrator no funcionará correctamente. Para todos los demás certificados de sistema, el nombre no es crítico. Al mover certificados de sistema distintos de OpsDrv, OpsKey y UIKey, el ID de objeto utilizado por servicios y adaptadores cambia. Vuelva a configurar los servicios que utilizan los certificados de sistema que se han eliminado.

Grabar certificado emitido por CA en un archivo

Acerca de esta tarea

Utilice el programa de utilidad GenCSR con el argumento getcacert para grabar en un archivo el certificado emitido por la entidad emisora de certificados (CA).

Procedimiento

1. Asegúrese de que el archivo getcacert.properties se ha configurado correctamente.

   La tabla siguiente describe los parámetros necesarios en el archivo getcacert.properties para la acción getcacert. Debe configurar el archivo getcacert.properties antes de utilizar el argumento getcacert.

Parámetro	Descripción	Valores válidos
certificate.request.Name	Nombre de la CSR.	Nombre de certificado
keystoretype	Nombre del almacén de claves utilizado.	PKCS11IMPLKS (a partir de V5.2.6.2 y en adelante) o nCipher.sworld o Luna
ca.cert.file	Vía de acceso completa al archivo en el que se debe grabar la información acerca del certificado CA.	Nombre y vía de acceso de un archivo de certificado CA

2. Grabe el certificado en un archivo.

   La sintaxis del mandato es `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Generar certificados de sistema internos (OpsDrv, OpsKey, UIKey) en el HSM

Con Sterling B2B Integrator se instalan tres certificados de sistema para proteger las operaciones internas. El hecho de moverlos al HSM proporciona poca ventaja de seguridad. Su política de seguridad puede requerir que todos los certificados que contienen claves privadas se almacenen en el HSM.

Acerca de esta tarea

Al generar los certificados de sistema internos de Sterling B2B Integrator denominados OpsDrv, OpsKey y UIKey en el HSM, utilice los nombres exactos. De lo contrario, Sterling B2B Integrator no funcionará correctamente.

Para generar certificados de sistema internos:

Procedimiento

1. Vaya a */dir_instalación*/install/bin.
2. Entre `./RemoveSystemCert.sh -l` para ver los certificados de la base de datos. Anote el ID de objeto para cada certificado de sistema.
3. Suprima los certificados de sistema de la base de datos ejecutando el siguiente mandato para cada certificado: `./RemoveSystemCert.sh -r` *xxxx* donde *xxxx* es el ID de objeto del certificado que desea eliminar.
4. Genere el certificado de sistema en el HSM para cada certificado, entrando:

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

Configurar dispositivos nCipher y SafeNet Luna

Correlación de proveedor de almacén de claves

Sterling B2B Integrator tiene el tipo de almacén de claves que es exclusivo entre los proveedores de servicios criptográficos; puede definir una correlación entre los tipos de almacén de claves y los proveedores necesaria para implementar el propio objeto de almacén de claves, los algoritmos de firma y los algoritmos de transporte clave.

El objeto de abstracción de información de clave y la clave contienen esta información con una referencia a com.sterlingcommerce.security.PrivateKeyInfo.

Esto permite a Sterling B2B Integrator utilizar una combinación de claves en los HSM y en los almacenes de software de la base de datos al mismo tiempo sin configuración adicional más allá de la carga inicial de la clave o la información de clave en la base de datos. Para Sterling B2B Integrator, todas las claves tienen el mismo aspecto, independientemente de dónde estén almacenadas.

La correlación se implementa como una propiedad denominada KeyStoreProviderMap en security.properties. Consta de un conjunto de entradas delimitadas por punto y coma (;). Cada entrada tiene seis elementos delimitados por comas y siguen este formato:

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

Los elementos se describen en la tabla siguiente:

Elemento	Descripción	Información adicional
KeyStoreType	Tipo de serie del almacén de claves	
KeyStoreProvider	Nombre del proveedor de servicio criptográfico que implementa el almacén de claves	
DoesAliasMatter	Indica si el alias de claves debe ser exclusivo para este tipo de almacén de claves	Este valor puede ser true o false. Las claves deben tener alias exclusivos en el caso de que sólo haya un almacén de claves por dispositivo.
SignatureProvider	Nombre del proveedor de servicio criptográfico a utilizar para crear firmas utilizando claves del almacén de claves	
EncryptionProvider	Nombre del proveedor de servicio criptográfico a utilizar al descifrar la información utilizando claves del almacén de claves	Esto es principalmente para operaciones de transporte de clave de RSA
KeyOnHSM	Indica si el almacén de claves está en un HSM	

La serie nula es un valor aceptable y se tratará como si no se hubiera especificado ningún proveedor. Una entrada debe tener como mínimo dos valores. Si una entrada contiene menos de seis valores, los valores se asignarán de izquierda a derecha al proveedor de almacén de claves, si el alias es importante al almacenar la clave, al proveedor de firmas, al proveedor de cifrado y si la clave están en un HSM para el tipo KeyStore. Los demás se tratarán como nulos y no se solicitará ningún proveedor específico para operaciones con claves de ese tipo.

El KeyStoreProviderMap predeterminado es actualmente:

```
nCipher = nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true
SafeNet Luna = Luna,LunaProvider,true,LunaProvider,LunaProvider,true
Utilice "PKCS11IMPLKS,IBMPKCS11Impl,true,IBMPKCS11Impl,IBMPKCS11Impl,true" tanto
para nCipher como para SafeNet Luna a partir de V5.2.6.2 y en adelante.
```

Cambios de JDK para soporte HSM de nCipher

Para que Sterling B2B Integrator utilice los HSM de nCipher, debe instalar los proveedores de servicio criptográfico java de nCipher. Para instalarlos, copie los siguientes archivos jar en el subdirectorio jre/lib/ext del JDK. Modifique java.security para cargar los proveedores nCipher.

Nota:

1. La siguiente configuración no es necesaria si va a crear claves o certificados utilizando la implementación "PKCS11IMPLKS" a partir de V5.2.6.2.
2. Para seguir utilizando las claves o certificados después de actualizar a V5.2.6.2, siga estos pasos.

El programa de instalación de nCipher pone estos archivos en /opt/nfast/java/classes:

- jcetools.jar

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

Debe añadir los proveedores nCipher después del proveedor IBM JCE y antes que el proveedor Certicom.

También debe eliminar IBMJCEFIPS de la lista.

Por ejemplo:

```
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
```

Utilice el siguiente ejemplo a partir de V5.2.6.2 para dar soporte a las claves o certificados existentes.

```
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
```

Cambios de JDK para soporte HSM de SafeNet Luna

Para que Sterling B2B Integrator utilice los HSM de SafeNet Luna, debe instalar el proveedor de servicio criptográfico java de SafeNet Luna. Para instalarlo, ponga los archivos .jar apropiados en el subdirectorio jre/lib/ext del JDK y, a continuación, modifique java.security para cargar los proveedores Luna.

Nota:

1. La siguiente configuración no es necesaria si va a crear claves o certificados utilizando la implementación "PKCS11IMPLKS" a partir de V5.2.6.2.
2. Para seguir utilizando las claves o certificados después de actualizar a V5.2.6.2, siga estos pasos.

El programa de instalación de nCipher pone estos archivos en /opt/nfast/java/classes:

- libLunaAPI.so
- LunaProvider.jar

Debe añadir el proveedor Luna después del proveedor IBM JCE y antes que el proveedor Certicom.

También debe eliminar IBMJCEFIPS de la lista.

Por ejemplo:

```
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
```

Utilice el siguiente ejemplo a partir de V5.2.6.2 para dar soporte a las claves o certificados existentes.

```
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
```

Configurar HSM utilizando IBM PKCS11IMPLKS (V5.2.6.2 o posterior)

Configurar HSM utilizando la implementación IBM PKCS11 IMPLKS (V5.2.6.2 o posterior)

Acerca de esta tarea

A partir de la versión 5.2.6.2, el sistema da soporte a la implementación IBM PKCS11 para dispositivos HSM. HSM implementa la API Java JCE. Esta interfaz accede a las claves del dispositivo.

Procedimiento

1. Se ha añadido un nuevo archivo de propiedades **hsm.properties.in** para dar soporte a PKCS11IMPLKS/IBMPKCS11Impl.

   La tabla siguiente lista las propiedades que son específicas para configurar HSM.

Atributo	Descripción
HSM_KEYSTORE_TYPE	Si HSM_ENABLED está establecido en *true*, el valor del atributo debe ser *IBMPKCS11IMPLKS*.
HSM_KEYSTORE_PROVIDER	Si HSM_ENABLED está establecido en *true*, el valor del atributo debe ser *IBMPKCS11Impl*.
HSM_KEYSTORE_FILE	<Debe dejarse en blanco>

Atributo	Descripción
HSM_ADAPTER_TYPE	ncipher o safeNet. Para ncipher, ejecute el siguiente mandato mientras crea o actualiza claves o certificados - Para UNIX: export CKNFAST_OVERRIDE_SECURITY_ASSURANCES= "longterm;tokenkeys" Para Windows: set CKNFAST_OVERRIDE_SECURITY_ASSURANCES ="longterm;tokenkeys"
HSM_ENABLED	Este atributo debe establecerse en *true* para soporte HSM
HSM_PRNG_ALGORITHM	Si HSM_ENABLED está establecido en *true*, el valor del atributo debe ser *PKCS11DeviceRNG*.
HSM_CONFIG_FILE_LOCATION	Si HSM_ENABLED está establecido en *true*, el valor del atributo debe establecerse en la ubicación del archivo de configuración IBMPKCS11

2. Actualice o cree el archivo de configuración necesario para la configuración de HSM en función del tipo de HSM.

   Para el tipo de HSM, puede ver el archivo de configuración del dispositivo tal como se muestra a continuación o puede pedir soporte a IBM para obtener el archivo de configuración. Puede actualizar cualquiera de los valores predeterminados como sea necesario. Debe editar el valor *library* si la ubicación es diferente del valor predeterminado.

```
Para un dispositivo SafeNet Luna:

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}
```

Para un dispositivo nCipher:

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

Nota: SafeNet Luna no permite importar una clave privada creada externamente. Debe crearlas y almacenarlas en el dispositivo HSM.