

IBM WebSphere Partner Gateway Enterprise Edition y  
Advanced Edition



# Guía del socio

*Versión 6.1.1*



IBM WebSphere Partner Gateway Enterprise Edition y  
Advanced Edition



# Guía del socio

*Versión 6.1.1*

**Nota:**

Antes de utilizar esta información y el producto al que da soporte, lea la información que se incluye en el apartado "Avisos" en la página 101.

**27 de marzo de 2008**

Esta edición se aplica a la versión 6.1.1, release 1, modificación 1, de IBM<sup>(TM)</sup> WebSphere<sup>(TM)</sup> Partner Gateway Advanced Edition (5724-L68) y Enterprise Edition (5724-L69), y a todos los releases y modificaciones posteriores hasta que se indique lo contrario en nuevas ediciones.

Para enviarnos sus comentarios acerca de este documento, escríbanos un mensaje de correo electrónico a [doc-comments@us.ibm.com](mailto:doc-comments@us.ibm.com). Esperamos recibir su opinión.

Cuando envíe información a IBM, proporcionará un derecho no exclusivo a IBM para que utilice o distribuya la información de la forma que crea conveniente sin que ello suponga ninguna obligación para usted.

© Copyright International Business Machines Corporation 2004, 2008. Reservados todos los derechos.

---

# Contenido

|   |            |
|---|------------|
| <b>Acerca de esta publicación</b> . . . . .   | <b>vii</b> |
| A quién va dirigida . . . . .   | vii        |
| Convenios tipográficos . . . . .  | vii        |
| Documentos relacionados . . . . .   | viii       |
| <b>Novedades</b> . . . . .  | <b>ix</b>  |
| Novedades del release 6.1.1 . . . . .   | ix         |
| Novedades del release 6.1. . . . .  | ix         |
| <b>Capítulo 1. Introducción</b> . . . . .   | <b>1</b>   |
| Comunidad de concentrador . . . . .   | 1          |
| Administrador de concentrador . . . . .   | 1          |
| Socio interno . . . . .   | 1          |
| Socios externos . . . . .   | 1          |
| Iconos de la Consola de comunidad . . . . .   | 2          |
| Uso de la Consola de comunidad . . . . .  | 3          |
| <b>Capítulo 2. Configuración de su entorno de WebSphere Partner Gateway</b> . . . . . | <b>5</b>   |
| Inicio de sesión en la Consola de comunidad . . . . .                                 | 5          |
| Verificación del perfil del socio . . . . .   | 6          |
| Visualización y edición del perfil de socio . . . . .                                 | 6          |
| Creación de un destino . . . . .  | 7          |
| Revisión de posibilidades B2B . . . . .   | 7          |
| Subida de certificados digitales . . . . .  | 9          |
| Términos de certificado . . . . .   | 10         |
| Tipos de certificado y formatos soportados . . . . .                                  | 11         |
| Servidor SSL y autenticación de cliente . . . . .                                     | 12         |
| Utilización de certificados para habilitar el cifrado . . . . .                       | 20         |
| Utilización de certificados para habilitar la firma digital . . . . .                 | 24         |
| Creación de grupos de consola . . . . .   | 28         |
| Creación de usuarios . . . . .  | 29         |
| Creación de un nuevo usuario . . . . .  | 29         |
| Configuración de usuario de FTP . . . . .   | 30         |
| Adición de usuarios a grupos . . . . .  | 30         |
| Creación de información de contacto . . . . .   | 31         |
| Creación de alertas y adición de contactos . . . . .                                  | 32         |
| Creación de una alerta basada en volumen . . . . .                                    | 33         |
| Creación de una alerta basada en suceso . . . . .                                     | 35         |
| Adición de un nuevo contacto a una alerta existente. . . . .                          | 37         |
| Creación de una dirección nueva . . . . .   | 38         |
| <b>Capítulo 3. Creación de destinos</b> . . . . .                                     | <b>39</b>  |
| Visión general . . . . .  | 39         |
| Configuración de un destino HTTP . . . . .  | 39         |
| Detalles del destino. . . . .   | 40         |
| Configuración del destino . . . . .   | 40         |
| Configuración de un destino HTTPS . . . . .   | 41         |
| Detalles del destino. . . . .   | 41         |
| Configuración del destino . . . . .   | 41         |
| Configuración de un destino FTP . . . . .   | 42         |
| Detalles del destino. . . . .   | 42         |
| Configuración del destino . . . . .   | 42         |
| Configuración de un destino SMTP . . . . .  | 43         |
| Detalles del destino. . . . .   | 43         |

|   |    |
|---|----|
| Configuración del destino . . . . .                             | 43 |
| Configuración de un destino JMS . . . . .                       | 44 |
| Detalles del destino. . . . .                                   | 44 |
| Configuración del destino . . . . .                             | 44 |
| Configuración de un destino de directorio de archivos . . . . . | 45 |
| Detalles del destino. . . . .                                   | 46 |
| Configuración del destino . . . . .                             | 46 |
| Configuración de un destino FTPS. . . . .                       | 47 |
| Detalles del destino. . . . .                                   | 47 |
| Configuración del destino . . . . .                             | 47 |
| Configuración de un destino de scripts FTP . . . . .            | 48 |
| Creación de scripts FTP . . . . .                               | 48 |
| Mandatos de scripts FTP . . . . .                               | 48 |
| Destinos de scripts FTP . . . . .                               | 49 |
| Detalles del destino. . . . .                                   | 49 |
| Configuración del destino . . . . .                             | 49 |
| Atributos definidos por el usuario. . . . .                     | 50 |
| Planificación . . . . .   | 50 |
| Configuración de manejadores . . . . .                          | 51 |
| Especificación de un destino predeterminado . . . . .           | 51 |

**Capítulo 4. Gestión de conexiones de comunidad y usuarios: Administración de cuentas . . . . . 53**

|  |    |
|--|----|
| Gestión de destinos. . . . .   | 53 |
| Visualización de una lista de destinos . . . . .                               | 53 |
| Visualización o edición de detalles de destino . . . . .                       | 53 |
| Ver, seleccionar o editar los destinos predeterminados . . . . .               | 54 |
| Visualización del destino de Donde se utiliza . . . . .                        | 54 |
| Supresión de un destino . . . . .  | 54 |
| Gestión de certificados. . . . .   | 55 |
| Visualización y edición de detalles de certificados digitales . . . . .        | 55 |
| Inhabilitación de un certificado digital . . . . .                             | 55 |
| Gestión de grupos . . . . .  | 55 |
| Visualización de miembros de grupo y asignación de usuarios a grupos . . . . . | 55 |
| Visualización, edición o asignación de permisos de grupo . . . . .             | 56 |
| Visualización o edición de detalles de grupo . . . . .                         | 56 |
| Supresión de un grupo . . . . .  | 56 |
| Gestión de usuarios . . . . .  | 56 |
| Supresión de usuarios . . . . .  | 58 |
| Gestión de contactos . . . . .   | 58 |
| Visualización o edición de detalles de contacto . . . . .                      | 58 |
| Eliminación de un contacto . . . . .   | 59 |
| Gestión de alertas . . . . .   | 60 |
| Visualización o edición de contactos y detalles de alerta . . . . .            | 60 |
| Búsqueda de alertas . . . . .  | 60 |
| Inhabilitación o habilitación de una alerta . . . . .                          | 61 |
| Eliminación de una alerta. . . . .   | 61 |
| Notificación de sucesos . . . . .  | 61 |
| Gestión de direcciones. . . . .  | 62 |
| Edición de una dirección . . . . .   | 62 |
| Supresión de una dirección . . . . .   | 62 |

**Capítulo 5. Visualización de sucesos y documentos: Visores . . . . . 63**

|  |    |
|--|----|
| Visor de sucesos. . . . .                            | 63 |
| Tipos de suceso . . . . .                            | 64 |
| Realización de tareas del Visor de sucesos . . . . . | 64 |
| Búsqueda de sucesos . . . . .                        | 64 |
| Visualización de detalles de suceso . . . . .        | 65 |
| Visor AS . . . . .                                   | 66 |
| Realización de tareas del Visor AS. . . . .          | 66 |

|  |    |
|--|----|
| Búsqueda de mensajes . . . . .   | 66 |
| Visualización de detalles de mensaje . . . . .                                     | 67 |
| Visor ebMS . . . . .   | 68 |
| Realización de tareas del visor ebMS . . . . .                                     | 68 |
| Búsqueda de procesos de ebMS. . . . .  | 69 |
| Visualización de los detalles del proceso de ebMS . . . . .                        | 69 |
| Visualización de documentos sin formato . . . . .                                  | 70 |
| Visualización del estado del documento . . . . .                                   | 70 |
| Visor de RosettaNet . . . . .  | 70 |
| Realización de tareas del Visor de RosettaNet . . . . .                            | 70 |
| Búsqueda de procesos de RosettaNet . . . . .                                       | 71 |
| Visualización de procesos de RosettaNet. . . . .                                   | 71 |
| Visualización de documentos sin formato . . . . .                                  | 72 |
| Visor de documentos . . . . .  | 72 |
| Búsqueda de documentos . . . . .   | 73 |
| Visualización de detalles de documento, sucesos y documentos sin formato . . . . . | 75 |
| Visualización de errores de validación de datos . . . . .                          | 76 |
| Uso de la característica Detener proceso . . . . .                                 | 77 |
| Cola de destino . . . . .  | 77 |
| Visualización de la lista de destinos . . . . .                                    | 78 |
| Visualización de documentos en cola . . . . .                                      | 80 |
| Eliminación de documentos de la cola de entrega. . . . .                           | 80 |
| Visualización de los detalles de destino . . . . .                                 | 81 |
| Cambio del estado de destino . . . . .   | 81 |

**Capítulo 6. Análisis de tipo de documento: Herramientas . . . . . 83**

|  |    |
|--|----|
| Análisis de documentos . . . . .                           | 83 |
| Estados de documento. . . . .                              | 84 |
| Visualización de documentos en el sistema . . . . .        | 84 |
| Visualización de detalles de procesos y sucesos . . . . .  | 85 |
| Proceso de archivos XML personalizados . . . . .           | 85 |
| Informe de volumen de documentos . . . . .                 | 86 |
| Creación de un informe de volumen de documentos . . . . .  | 86 |
| Exportación del informe de volumen de documentos . . . . . | 87 |
| Impresión de informes. . . . .                             | 87 |
| Probar conexión de socio . . . . .                         | 87 |
| Códigos de resultado de servidor web . . . . .             | 88 |
| Informes de EDI. . . . .                                   | 90 |
| Búsqueda de FA retrasados de EDI . . . . .                 | 90 |
| Búsqueda de transacciones rechazadas de EDI. . . . .       | 92 |
| Informes de FTP. . . . .                                   | 94 |
| Estadísticas de FTP. . . . .                               | 94 |
| Conexiones FTP . . . . .                                   | 95 |

**Glosario . . . . . 97**

**Avisos . . . . . 101**

|  |     |
|--|-----|
| Información de la interfaz de programación . . . . . | 103 |
| Marcas registradas y marcas de servicio . . . . .    | 103 |

**Índice. . . . . 105**





---

## Acerca de esta publicación

IBM WebSphere Partner Gateway es un sistema de proceso de documentos electrónicos utilizado para gestionar una comunidad comercial de empresa a empresa (B2B). B2B ha evolucionado a lo largo de los últimos años para ayudar a las empresas a realizar muchos tipos de transacciones automatizadas (por ejemplo, órdenes de compra y facturas) rápida, cómoda y económicamente.

Esta guía proporciona a los socios de la comunidad toda la información necesaria para configurar la consola y para realizar tareas diarias.

---

## A quién va dirigida

Las partes implicadas en una comunidad del concentrador o comercial de IBM WebSphere Partner Gateway son el socio interno, el administrador del concentrador y los socios externos. Cada una de estas partes tiene usuarios de administración con distintos niveles de privilegios. Además, los usuarios de administración añadirán usuarios normales con privilegios de acceso de consola específicos.

---

## Convenios tipográficos

Este documento utiliza los siguientes convenios tipográficos:

| Convenio                             | Descripción   |
|--------------------------------------|---|
| Font monoespaciado                   | El texto en este font indica texto que escribe el usuario, valores de argumentos u opciones de mandatos, ejemplos y ejemplos de código o información que el sistema imprime en la pantalla (texto de mensajes o solicitudes).   |
| <b>Negrita</b>                       | El texto en negrita indica los controles de la interfaz gráfica de usuario (por ejemplo, nombres de botones en línea, nombres de menú u opciones de menú) y cabeceras de columna en tablas y texto.   |
| <i>Cursiva</i>                       | El texto en cursiva indica énfasis, títulos de libros, términos nuevos y términos que están definidos en el texto, nombres de variable o letras del alfabeto utilizadas como letras.  |
| <i>Font monoespaciado en cursiva</i> | El texto en font monoespaciado en cursiva indica nombres de variables dentro del texto en font monoespaciado.   |
| Texto en color subrayado             | El texto en color subrayado indica una referencia cruzada. Pulse el texto para ir al objeto de la referencia.   |
| Texto con contorno azul              | (Sólo en archivos PDF) Un contorno azul alrededor del texto indica una referencia cruzada. Pulse el texto con el contorno alrededor para ir al objeto de la referencia. Este convenio es el equivalente para los archivos PDF del convenio "Texto en color subrayado" incluido en esta tabla. |
| {DIR INSTAL}                         | Representa el directorio en el que está instalado el producto.  |
| UNIX:/Windows:                       | Los párrafos que comienzan por una de estas palabras indican diferencias entre sistemas operativos.   |
| “ ”(comillas)                        | (Sólo en archivos PDF) Las comillas se utilizan para marcar referencias cruzadas a otros apartados del documento.   |
| { }                                  | En la línea de sintaxis, se colocan llaves alrededor de un conjunto de opciones de entre las que debe elegir solamente una.   |

---

|      |   |
|------|---|
| [ ]  | En una línea de sintaxis, se colocan corchetes alrededor de parámetros opcionales.  |
| ...  | En una línea de sintaxis, los puntos suspensivos indican una repetición del parámetro anterior. Por ejemplo, opción[,...] significa que puede especificar múltiples opciones separadas con comas.   |
| < >  | Los corchetes angulares se colocan alrededor de un nombre para distinguirlos entre ellos. Por ejemplo, <nombre_servidor><nombre_conector>tmp.log.   |
| \, / | Las barras inclinadas invertidas (\) se utilizan como separadores de componentes en vías de acceso de directorios en instalaciones Windows. En el caso de instalaciones UNIX, sustituya las barras inclinadas invertidas con barras inclinadas (/). |

---



---

## Documentos relacionados

La documentación completa que se proporciona con este producto incluye información exhaustiva sobre la instalación, la configuración, la administración y la utilización de WebSphere Partner Gateway Enterprise Edition y Advanced Edition.

Puede descargar la documentación o leerla directamente en línea en el siguiente sitio:

<http://www.ibm.com/software/integration/wspartnergateway/library/infocenter>

**Nota:** Cierta información importante sobre este producto puede estar disponible en las notas técnicas y los anuncios de soporte técnico emitidos después de la publicación de este documento. Se pueden encontrar en el sitio web de soporte de WebSphere Partner Gateway:

<http://www.ibm.com/software/integration/wspartnergateway/support/>

Seleccione el área de interés del componente y examine la sección de Notas técnicas y anuncios.

---

## Novedades

Esta sección describe las características nuevas de IBM WebSphere Partner Gateway.

---

### Novedades del release 6.1.1

WebSphere Partner Gateway 6.1.1 da soporte a las siguientes características nuevas:

- En los releases anteriores, el soporte de autenticación básica sólo estaba disponible para los mensajes de servicios web. Esta característica ahora se amplía a todos los protocolos. La recomendación para la autenticación básica es la utilización de una conexión HTTP segura, es decir, HTTPS en lugar de HTTP.
- Además de la firma y el cifrado, se proporciona soporte de compresión y descompresión para los mensajes de RNIF.
- Se proporciona soporte para la validación de Cuerpo SOAP y Sobre SOAP. Asimismo, se puede desensobrar un Sobre SOAP.
- El tiempo de espera máximo síncrono y el número máximo de conexiones síncronas se pueden controlar localmente para cada receptor HTTP.
- El servidor FTP se integra en WebSphere Partner Gateway para dar soporte al protocolo AS3, la pasarela de FTP Scripting, el receptor de FTP Scripting, y el receptor y la pasarela FTP / FTPS.
- El documento de errores puede enviarse al socio iniciador, al socio receptor, o a ambos. El flujo de documentos de errores puede configurarse en la consola de WebSphere Partner Gateway y puede enviarse en formato WebSphere Partner Gateway o en formato de servicios Web.
- Se ha mejorado el rendimiento del archivador.
- Se proporciona soporte para varios socios internos.
- Puede reenviar varios documentos Entrantes o Salientes simultáneamente.
- Se proporciona soporte para la modalidad FIPS. El producto se puede configurar para funcionar en modalidad FIPS o en la modalidad predeterminado.
- Se proporcionan las funcionalidades Suprimir y Donde se utiliza para Destino, Correlaciones de validación Definiciones de documento, Interacciones y Usuarios.
- Se proporciona soporte de compresión de archivos grandes para documentos AS2 y AS3.
- Se proporciona soporte para cifrado y firmas.
- Las dependencias de tipo de configuración para la migración también incluyen Códigos de sucesos y Notificaciones de alerta. Además, se ha mejorado la funcionalidad de la migración de socios para proporcionar soporte para importar/exportar definiciones de sucesos alertables.
- Se ofrece soporte para la subida de múltiples certificados. Se incluye un nuevo asistente en la consola para subir y configurar certificados.
- El producto da soporte ahora a AIX 6.1, RHEL 5 (32 y 64 bits), SLES 10 (64 bits) y Windows Server 2003 de 64 bits.

---

### Novedades del release 6.1

WebSphere Partner Gateway V6.1 da soporte a las características nuevas siguientes:

- Soporte a nuevos protocolos empresariales: AS3, SOAP con archivos adjuntos, CIDX y ebXML Message Service (ebMS) 2.0
- El soporte mejorado a documentos XML personalizados incluye una mejor organización, un soporte a expresiones completas de XPath, campos de búsqueda, atributos definidos por el usuario y soporte síncrono
- Nuevo soporte a IPv6 y mejor FTP Scripting para dar soporte a AS3
- Reorganización de los atributos de definición de documentos
- Atributos de la definición de nuevo documento para utilizarlos con las salidas de usuario.
- No hay rechazo configurable por tipo de documento y nivel de socio de comercialización
- El visor del documento tiene campos de búsqueda adicionales definidos por el usuario.
- Soporte al visor de AS mejorado basado en el estado de devolución de MDN
- Asistente de configuración de EDI y Asistente de importación de EIF (anteriormente proporcionados con el paquete de soporte GA02)
- Nueva modalidad de notificación de alertas para enviar notificaciones a todas las partes relacionadas (socios de origen y destino o todos los contactos suscritos, lo que reduce la configuración de alertas)
- Permisos de pasarela y reenvío disponibles actualmente para usuarios que no sean el administrador de concentrador
- Nuevo grupo de usuarios para permitir que varios usuarios tengan la posibilidad de ser administradores de concentrador
- Soporte a LDAP para la autenticación de inicio de sesión
- Utilización del registro cronológico y del rastreo de WebSphere Application Server para los componentes de WebSphere Partner Gateway
- Los datos de configuración de archivo de propiedad están actualmente ubicados centralmente y gestionados mediante la consola de WebSphere Partner Gateway
- WebSphere MQ ya no es un producto de requisito previo; el soporte a WebSphere Platform Messaging se utiliza ahora para las comunicaciones internas
- Archivo selectivo según socio y/o tipo de documento
- Migración de la configuración de WebSphere Partner Gateway mediante la exportación e importación de definiciones de una instancia de WebSphere Partner Gateway a otra
- Una opción de instalación de una máquina simplificada (modalidad simple)
- WebSphere Application Server Network Deployment se utiliza ahora para despliegues de varias máquinas que habilitan la agrupación en clúster y la gestión de infraestructura central
- Soporte para utilizar WebSphere Process Server, versión 6.1 como integración de fondo

**Notas:**

1. La API administrativa basada en XML está en desuso en la versión 6.1.
2. WebSphere Partner Gateway, versión 6.1 no da soporte al algoritmo RC5.

---

# Capítulo 1. Introducción

---

## Comunidad de concentrador

La comunidad de concentrador de IBM WebSphere Partner Gateway se compone de tres entidades conectadas a un concentrador central para el intercambio en tiempo real de documentos empresariales: administrador de concentrador, socio interno y socios externos.

### Administrador de concentrador

El administrador de concentrador es una empresa responsable de gestionar el funcionamiento diario de la comunidad de concentrador. El administrador de concentrador mantiene la infraestructura de hardware y software de la comunidad de concentrador de forma permanente. Estas responsabilidades incluyen:

- Resolución de problemas y reparación.
- Garantía de que la comunidad de concentrador está correctamente configurada para todos los socios.
- Asistencia en la configuración de nuevos socios externos en la comunidad de concentrador.
- Planificación estratégica del crecimiento futuro que garantice que la comunidad de concentrador funciona con eficacia plena.

El rol del administrador de concentrador se puede contratar a una empresa de terceros de la comunidad de concentrador, o el socio interno que compró WebSphere Partner Gateway puede elegir desempeñar la función de administrador de concentrador.

### Socio interno

El socio interno es la empresa principal y la fuerza motriz de la comunidad de concentrador. Esta empresa es responsable de la compra y construcción de la comunidad de concentrador, incluida la definición de los procesos empresariales electrónicos transferidos entre ellos y sus socios externos.

El socio interno también puede elegir ser el administrador de concentrador.

### Socios externos

Los socios externos son las empresas que hacen negocios con el socio interno a través de la comunidad de concentrador. Los socios externos deben completar un proceso de configuración para conectarse a la comunidad de concentrador. Una vez conectados, los socios externos pueden intercambiar documentos de empresa electrónicos con el socio interno.

## Iconos de la Consola de comunidad

Los iconos de la siguiente tabla son exclusivos de la Consola de comunidad de WebSphere Partner Gateway

Tabla 1. Iconos de la Consola de comunidad









































| Icono   | Nombre de icono                                   |
|---|---|
|    | Contraer  |
|    | Copiar  |
|    | Crear rol. El rol no está activo                  |
|    | Contiene datos                                    |
|    | Activar   |
|    | Suprimir  |
|    | Mostrar documento sin formato                     |
|    | Documento en curso                                |
|    | No se ha podido procesar el documento             |
|   | El documento se ha procesado correctamente        |
|  | Descargar correlación                             |
|  | Editar  |
|  | Editar valores de atributo                        |
|  | Desactivar edición                                |
|  | Editar valores de atributo de RosettaNet          |
|  | Expandir  |
|  | Exportar información                              |
|  | Exportar informe                                  |
|  | Destino inhabilitado                              |
|  | Ocultar criterios de búsqueda                     |
|  | Modificar   |
|  | No se contienen datos                             |
|  | Abrir calendario                                  |
|  | Habilitar/inhabilitar la ordenación del documento |
|  | Hacer una pausa                                   |

Tabla 1. Iconos de la Consola de comunidad (continuación)

| Icono   | Nombre de icono   |
|---|---|
|    | Imprimir  |
|    | Entrada necesaria   |
|    | Iniciar   |
|    | Dejar de procesar; opción de usuario cuando el documento está en curso para solicitar que el servidor deje de procesar el documento |
|    | Flujo de datos síncronos; no se visualiza ningún icono para las transacciones asíncronas  |
|    | Subir correlación   |
|    | Ver detalles  |
|    | Ver configuración de atributos de definición de documentos  |
|    | Ver sistema de ayuda  |
|    | Ver miembros  |
|    | Ver documento original  |
|   | Ver permisos  |
|  | Ver los miembros de grupo   |
|  | Ver errores de validación   |
|  | Donde se utiliza  |

## Uso de la Consola de comunidad

Después de configurar WebSphere Partner Gateway, utilizará dos herramientas de consola regularmente: el Visor de sucesos y el Análisis de documentos.

Utilice el Visor de sucesos, en el módulo Visores, para buscar sucesos. La mayoría de los tipos de documento se reenvían varias veces, por lo tanto un documento falla y genera una alerta, es algo que debería investigar y corregir para evitar anomalías similares en el futuro.

Puede localizar un suceso específico y, a continuación, buscar porqué ha ocurrido. El Visor de sucesos le permite buscar sucesos por hora, fecha, tipo de suceso, nombre de suceso y ubicación de suceso. La administración de concentrador también puede buscar por socio, OP de origen e IP de suceso.

**Nota:** No todos los usuarios pueden acceder a los elementos Depuración.

Los datos generados por el Visor de sucesos le ayudarán a identificar el suceso y el documento que crearon el suceso. También puede ver el documento sin formato, que identifica el campo, el valor y el motivo del error.

La segunda herramienta utilizada más comúnmente es el Análisis de documentos, una característica en el módulo Herramientas. Se utiliza para saber cuántos documentos se han recibido, cuántos están en progreso y de aquellos que están completados, cuántos han fallado y cuántos fueron satisfactorios. Utilice esta herramienta para saber por qué fallaron aquellos documentos que han fallado.

El módulo Administración de cuentas de la consola se utiliza principalmente al configurar WebSphere Partner Gateway y, desde entonces, para su mantenimiento.



---

## Capítulo 2. Configuración de su entorno de WebSphere Partner Gateway

En este apartado se describen las tareas que debe efectuar el socio externo para preparar a WebSphere Partner Gateway para los usuarios y el entorno del socio.

Para configurar WebSphere Partner Gateway para su empresa, deberá realizar las siguientes actividades desde la Consola de comunidad en el siguiente orden.

1. "Inicio de sesión en la Consola de comunidad"
2. "Verificación del perfil del socio" en la página 6
3. "Creación de un destino" en la página 7
4. "Revisión de posibilidades B2B" en la página 7
5. "Subida de certificados digitales" en la página 9
6. "Creación de grupos de consola" en la página 28
7. "Creación de usuarios" en la página 29
8. "Configuración de usuario de FTP" en la página 30
9. "Creación de información de contacto" en la página 31
10. "Creación de alertas y adición de contactos" en la página 32
11. "Creación de una dirección nueva" en la página 38

---

### Inicio de sesión en la Consola de comunidad

Este apartado proporciona los pasos para visualizar la Consola de comunidad e iniciar sesión en ella. La resolución de pantalla recomendada es 1024 x 786.

**Nota:** La consola de comunidad de WebSphere Partner Gateway necesita que se active el soporte de cookies a fin de mantener la información de sesión. No se almacenará ninguna información personal en la cookie y caducará cuando el navegador esté cerrado.

1. Abra un navegador web y especifique el siguiente URL para visualizar la consola:

`http://<nombre de host>.<dominio>:58080/console` (no seguro)

`https://<nombre de host>.<dominio>:58443/console` (seguro)

Donde *<nombre de host>* y *<dominio>* son el nombre y la ubicación del sistema que aloja al componente consola de comunidad.

**Nota:** Estos URL asumen que se utilizan los números de puerto predeterminados. Si cambia los números de puerto predeterminados, sustitúyalos por los valores especificados.

En la mayoría de los casos, el administrador de concentrador le ha enviado el nombre de usuario, la contraseña de inicio y el nombre de inicio de sesión de la empresa que utilizará para iniciar la sesión en la Consola de comunidad. Necesitará esta información para realizar el siguiente procedimiento. Si no ha recibido esta información, póngase en contacto con su administrador de concentrador.

Para iniciar la sesión en la Consola de comunidad (estas instrucciones son tanto para los socios internos como para los externos):

1. Especifique el **Nombre de usuario** para su empresa.
2. Especifique la **Contraseña** para su empresa.
3. Especifique el **Nombre de inicio de sesión de empresa**, por ejemplo, IBM.
4. Pulse el botón **Iniciar sesión**. Cuando inicie la sesión por primera vez, deberá crear una nueva contraseña.
5. Especifique una nueva contraseña y, a continuación, escriba la nueva contraseña una segunda vez en el recuadro de texto Verificar.
6. Pulse **Guardar**. El sistema mostrará la pantalla de entrada inicial de la consola.

**Nota:** Si se configura WebSphere Partner Gateway utilizando LDAP, tiene que especificar el nombre de usuario y la contraseña de LDAP. El Nombre de inicio de sesión de empresa no es relevante en este caso, por lo que no se le solicitará que especifique esta información. Además, el sistema no le solicitará que cambie la contraseña.

---

## Verificación del perfil del socio

Utilice la característica Socios de administración de cuentas para ver y editar la información que identifica a su empresa en el sistema.

Los socios pueden editar todos los atributos de su perfil excepto el nombre de inicio de sesión de empresa. Los socios también pueden añadir y eliminar los ID de empresa, los ID de correo electrónico relacionados con todos los ID de empresa, y las direcciones IP. Las direcciones IP o nombres de sistema principal se pueden especificar para las siguientes modalidades de funcionamiento: Producción, Prueba, Gestor de CPS y Socio CPS.

Esta característica también incluye una opción para restablecer todas las contraseñas de usuario. Puede que desee utilizar esta característica si siente que las contraseñas de usuario se han comprometido.

## Visualización y edición del perfil de socio

1. Pulse **Administración de cuentas > Perfiles > Socio**.
2. Pulse el icono Mi perfil para editar. El sistema mostrará la pantalla Detalles de socio.
3. Edite su perfil, según sus necesidades (algunos valores no se pueden editar). Para obtener una explicación de los valores, consulte la Tabla 2 en la página 7.

Tabla 2. Valores en pantallas de socios

| Valor                                       | Descripción  |
|---|--|
| Nombre de inicio de sesión de empresa       | Identifica el participante para el sistema. Máximo de 15 caracteres. No se pueden incluir los siguientes caracteres especiales: , . ! # ; : \ / & ?. Los socios no pueden editar este valor.   |
| Nombre de visualización de socio            | El nombre que el socio desea que aparezca en la comunidad de concentrador. Máximo de 30 caracteres.  |
| Tipo de socio                               | Tipo de socio: socio externo o interno. Los socios sólo pueden editar este valor si la propiedad <code>bcg.allow.partner.type.edit</code> se ha establecido en <code>True</code> . El valor predeterminado es <code>False</code> .   |
| Estado                                      | Habilitado o Inhabilitado. Si está inhabilitado, el socio no estará visible en los criterios de búsqueda ni en las listas desplegables.  |
| Tipo de proveedor                           | Identifica el rol del socio, por ejemplo, Fabricante de contrato o Distribuidor.   |
| Sitio web                                   | Identifica el sitio web del socio.   |
| ID de empresa                               | Número DUNS, DUNS+4 o de formato libre que el sistema utiliza para direccionamientos. Puede añadir números de ID de empresa adicionales. <ul style="list-style-type: none"> <li>• Los números DUNS deben tener nueve dígitos.</li> <li>• Los números DUNS+4 deben tener trece dígitos.</li> <li>• Los números de ID de formato libre aceptan hasta 60 caracteres numéricos, alfanuméricos y especiales.</li> </ul> <p><b>Nota:</b> Los ID de empresa deben llevar como prefijo los calificadores que se utilicen en el documento EDI. El formato es Calificador EDI más "-" y el ID. Por ejemplo, un EDI X12 que utilice DUNS será 01-123456789.</p> |
| ID de correo electrónico                    | Un ID de correo electrónico válido de cada ID de empresa. Puede añadir otros ID de correo electrónico adicionales para todos los ID de empresa. Este campo no es visible si no hay ningún ID de empresa.   |
| Dirección IP o Nombre del sistema principal | <ul style="list-style-type: none"> <li>• Modalidad de funcionamiento, por ejemplo, Socio CPS</li> <li>• Dirección IP o nombre de host del socio.</li> </ul>  |

4. Pulse el botón **Guardar**.

---

## Creación de un destino

Debe crear y mantener un destino predeterminado. Si no lo hace, no podrá crear conexiones. Consulte el apartado Capítulo 3, "Creación de destinos", en la página 39 para obtener información sobre cómo crear destinos.

---

## Revisión de posibilidades B2B

**Nota:** En instalaciones más pequeñas, este proceso debería realizarlo el administrador de concentrador.

Utilice esta característica para ver y editar posibilidades B2B de concentrador completo predefinidas y para habilitar posibilidades B2B locales adicionales, si fuese necesario.

Una posibilidad B2B identifica un tipo específico de proceso empresarial que se puede intercambiar entre usted y otros miembros de la comunidad. Las posibilidades de proceso de documentos o B2B se definen utilizando definiciones

de tipos de documento. Una definición de tipo de documento ofrece al sistema toda la información necesaria para recibir, procesar y direccionar documentos entre miembros de comunidad.

Cada posibilidad se compone de hasta cinco definiciones diferentes de tipo de documento:

**Paquete.** Formatos de empaquetado de documentos de identificación utilizados para transmitir documentos a través de Internet. Por ejemplo, RNIF, AS1, AS2 y AS3.

**Protocolo.** Identifica la estructura y la ubicación de información en el documento. El sistema necesita esta información para procesar y direccionar el documento.

**Tipo de documento.** Identifica el proceso empresarial que se procesará entre el socio interno y sus socios externos.

**Actividad.** Función empresarial que realiza el proceso.

**Acción.** Los documentos individuales que forman un proceso empresarial completo. Los documentos se procesan entre el socio interno y el socio externo.

Cada definición de tipo de documento contiene atributos (es decir, información) que definen la funcionalidad de la definición. Un atributo es una pieza de información que se asocia con un tipo de documento específico. El sistema utiliza esta información para diversas funciones como la validación de documentos o la comprobación de cifrados.

#### **Revisión y edición de posibilidades B2B:**

1. Pulse **Administración de cuentas > Perfiles > B2B Posibilidades**. El sistema muestra la pantalla Posibilidades B2B.
  - Si una carpeta aparece junto a un paquete y Habilitado aparece en la columna Habilitado, el administrador de concentrador le habrá habilitado esta posibilidad.
  - Una marca de selección bajo Establecer origen o Establecer destino le informará de que puede utilizar esta posibilidad en dicho rol (es decir, como origen, destino o ambos).
  - El icono Crear rol debajo de Establecer origen o Establecer destino le informará de que la posibilidad no está habilitada en dicho rol (es decir, como origen, destino o ambos).
  - La columna Habilitado muestra el estado del paquete: Habilitado o Inhabilitado.

**Nota:** El destino, el origen o ambas posibilidades deben establecerse antes de habilitarla.

2. Establezca la posibilidad para iniciar (**Establecer origen**), recibir (**Establecer destino**), o para iniciar y recibir el contexto de tipo de documento. En un PIP bidireccional, Establecer origen y Establecer destino son lo mismo para todas las acciones, sin tener en cuenta el hecho de que la solicitud surge de un socio y la confirmación correspondiente surge de otro.
3. Establezca la posibilidad para iniciar (**Establecer origen**), recibir (**Establecer destino**), o iniciar y recibir para cada definición de tipo de documento de nivel inferior.

4. Pulse el icono Editar para ver y, si lo desea, cambiar las definiciones de tipo de documento de nivel inferior (por ejemplo, Protocolo o Tipo de documento). También puede cambiar los atributos de una definición de tipo de documento (por ejemplo, Hora de realización o Número de reintentos). Cuando utilice esta pantalla por primera vez, los atributos se establecerán en el nivel global. No obstante, puede restablecerlos en el nivel local si lo desea. Si establece un atributo en el nivel local sobrescribirá la configuración global de su entorno, pero no cambiará la configuración global.
  - Si realiza un cambio en cualquier nivel, éste se propagará a todos los niveles inferiores.
  - Si lo desea, puede seleccionar y editar una carpeta individual que esté bajo un paquete. Un cambio realizado de esta forma no se propagará a niveles inferiores.
  - Puede sobrescribir la opción incorporada “seleccionar todo” deseleccionando de abajo a arriba.
  - Las señales, por ejemplo, los acuses de recibo, son específicas de RosettaNet. Hay tres señales bajo cada acción: acuse de recibo, excepción general y excepción de acuse de recibo. Puede establecer atributos para las señales.
  - No rechazo necesario
  - ID empresarial de AS

Si ha cambiado un atributo, pulse **Guardar**.

---

## Subida de certificados digitales

Un certificado digital es una credencial de identificación en línea, parecido a un pasaporte o un carnet de identidad. Un certificado digital se puede utilizar para identificar una persona o una organización.

Las firmas digitales son cálculos basados en un documento electrónico que utilizan la criptografía de claves públicas. En este proceso, la firma digital está vinculada con el documento que se está firmando, así como con el firmante, y no se puede reproducir. Con el paso de la factura de firma digital federal, las transacciones electrónicas firmadas digitalmente tienen el mismo peso legal que las transacciones firmadas con tinta.

WebSphere Partner Gateway utiliza certificados digitales para verificar la autenticidad de las transacciones de documentos empresariales entre el socio interno y los socios externos. También se utilizan para realizar cifrado y descifrado.

Puede especificar un certificado primario y secundario para los documentos salientes para asegurarse de que no se interrumpa el intercambio de documentos. El primario se utiliza para todas las transacciones. El secundario se utiliza si el primario ha caducado o se ha revocado.

Los certificados digitales se suben y se identifican durante el proceso de configuración.

Si se detecta que un certificado ha caducado o se ha revocado, se inhabilita y se refleja como tal en la consola. Si el certificado primario ha caducado o se ha revocado, se inhabilita y el certificado secundario se establece como primario. Cuando se detecta que un certificado ha caducado o se ha revocado, se genera un suceso.

La opción Utilización de certificado está disponible en función del tipo de certificado seleccionado. En el perfil de operador del concentrador, la Utilización de certificado se puede establecer para un certificado de Firma digital o Cliente SSL. En el perfil de socio, la Utilización de certificado se puede establecer para el certificado de Cifrado. Si se debe utilizar el mismo certificado para distintos propósitos, por ejemplo, para Firma digital y Cifrado en el perfil de operador del concentrador, se debe cargar dos veces, una para la Firma digital y otra vez para el certificado de Cifrado. Sin embargo, si el certificado se utiliza para la Firma digital y para el cliente SSL, se pueden establecer los recuadros de selección correspondientes en la misma entrada de certificado.

Estos certificados también se pueden cargar dos veces, una para la Firma digital y otra para el Cliente SSL. Si este es el caso, se debe seguir el mismo patrón para los certificados secundarios. Por ejemplo, si los certificados principales se han cargado como certificados diferentes para la Firma digital y el Cliente SSL, los certificados secundarios también se deben cargar como entradas de certificado diferentes (aunque el certificado sea el mismo).

Para la construcción y validación de certpath, es necesario que suba todos los certificados en la cadena de certificados. Por ejemplo, si la cadena de certificados contiene los certificados A -> B -> C -> D, donde A -> B significa que A es el emisor de B, los certificados A, B y C se deben subir a los certificados raíz. Si uno de los certificados no está disponible, el certpath no se creará y la transacción no se efectuará. Los certificados CA se pueden obtener de los depósitos de certificados mantenidos por las autoridades certificadoras o del socio que ha proporcionado el certificado. Los certificados raíz e intermediario sólo se pueden subir en el perfil del Operador de concentrador.

**Nota:** Para poder utilizar los procedimientos de las siguientes secciones, se deben cargar antes los certificados en el sistema. Para obtener más información sobre la carga de certificados, consulte la *Guía de configuración del concentrador*.

Puede crear alertas de caducidad de certificado que se le notificarán cuando un certificado esté a punto de caducar. Para obtener más información, consulte el apartado "Creación de alertas y adición de contactos" en la página 32. Los certificados caducados se guardan en la base de datos de IBM WebSphere Partner Gateway y no se pueden borrar del sistema.

## Términos de certificado

**Autoridad certificadora (CA).** Autoridad que emite y gestiona las credenciales de seguridad y las claves públicas para el cifrado de mensajes. Cuando una persona o una empresa solicitan un certificado digital, una CA comprueba con una autoridad de registro (RA) la información que la persona o la empresa les ha entregado. Si la RA verifica la información enviada, la CA emitirá un certificado.

Entre los ejemplos de CA se encuentran VeriSign y Thawte.

**Certificado digital.** Un certificado digital es la versión electrónica de una tarjeta de ID. Establece su identidad al realizar transacciones B2B a través de Internet. Los certificados digitales se obtienen de la Autoridad certificadora (CA) y se componen de tres elementos:

- La parte de clave pública del par de claves pública y privada.
- Información que le identifica.

- La firma digital de una entidad de confianza (CA) que prueba la validez del certificado.

**Firma digital.** Código digital creado con una clave privada. Las firmas digitales permiten a los miembros de la comunidad de concentrador autenticar transmisiones mediante verificación de la firma. Al firmar un archivo, se crea un código digital que es exclusivo tanto para el contenido del archivo como para la clave privada. La clave pública se utiliza para verificar la firma.

**Cifrado.** Método de codificación para volver la información ilegible para cualquiera excepto para el receptor en cuestión, que debe descifrar la información para leerla.

**Descifrado.** Método de descodificación de la información cifrada que la vuelve de nuevo legible. La clave privada del receptor se utiliza para el descifrado.

**Clave.** Código digital utilizado para cifrar, firmar, descifrar y verificar archivos. Las claves pueden venir en pares de clave, una privada y otra pública.

**Sin repudio.** Evitar el rechazo de acciones u obligaciones previas. Para transacciones electrónicas de B2B, las firmas digitales se utilizan para validar el remitente e indicar la hora de la transacción. De esta forma se evita que las partes implicadas reclamen que la transacción no se autorizase o no fuera válida.

**Clave privada.** La parte secreta de un par de claves. Esta clave se utiliza para firmar y descifrar información. Sólo usted tiene acceso a su clave privada. Su clave privada también se utiliza para generar una firma digital basada en el contenido del documento.

**Clave pública.** La parte pública de un par de claves. Esta clave se utiliza para cifrar información y verificar firmas. Una clave pública se puede distribuir a otros miembros de la comunidad de concentrador. El conocimiento de la clave pública de una persona no ayuda a que nadie descubra la correspondiente clave privada.

**Clave con firma personal.** Clave pública que ha sido firmada por la correspondiente clave privada como prueba de propiedad.

**Certificado X.509.** Certificado digital utilizado para probar la identidad y la propiedad de la clave pública a través de una red de comunicación. Contiene el nombre del emisor (es decir, la CA), la información de identificación del usuario y la firma digital del emisor.

El certificado identifica a su organización y el periodo de tiempo que el certificado es válido.

## Tipos de certificado y formatos soportados

Todos los certificados deben estar en formato DER o ASCII Privacy Enhanced Mail (PEM). Los certificados se pueden convertir de un formato a otro.

Hay varios tipos de certificado:

- **Certificado de cliente SSL (socios externos y socio interno).** Un certificado de transporte. Si el transporte saliente es HTTPS, necesitará un certificado de cliente de SSL. En la mayoría de los casos, el certificado de cliente de SSL debe estar firmado por una CA. Si el certificado se utiliza en un entorno de prueba, puede tener una firma personal.

Debe subir el certificado a WebSphere Partner Gateway a través de la consola y enviar una copia del certificado al Operador de concentrador.

- **Certificado de servidor SSL.** Habilita la autenticación del servidor SSL. La CA del certificado de servidor SSL debe intercambiarse entre los socios.
- **Certificado de cifrado (socios externos y socio interno).** Si los miembros de la comunidad de concentrador cifran archivos, la parte de clave pública del certificado de cifrado deberá enviarse a los miembros de la comunidad de concentrador. La parte correspondiente de clave privada del certificado de cifrado deberá subirse al nivel de operador de concentrador a través de la consola. Debe subir la parte pública del certificado del socio a WebSphere Partner Gateway a través de la consola y enviar una copia del certificado al Operador de concentrador.
- **Certificado de firma digital (socios externos y socio interno).** Si los miembros de la comunidad de concentrador firman los documentos, la parte pública del certificado deberán subirla al concentrador, a nivel de socio, como certificado de firma. Si el gestor de concentrador tiene que firmar los documentos que envía a los miembros de la comunidad de concentrador, deberá enviar la parte pública del certificado de gestor de concentrador a los miembros de la comunidad de concentrador. El certificado de firma del concentrador deberá subirse a través de la consola al operador de concentrador.
- **Certificado VTP (socio interno).** Este certificado es utilizado por el Gestor de documentos de WebSphere Partner Gateway para la característica Simulador de socios externos. Este certificado se copia en el sistema de archivos en lugar de subirse a través de la consola.

Los certificados VTP copiados en el sistema de archivos están activos para todos los socios creados a través de la consola. Se utilizan para validar los documentos firmados recibidos desde el Simulador de socios. Además, los certificados copiados en el sistema de archivos no estarán visibles a través de la consola.

## Servidor SSL y autenticación de cliente

Si la autenticación de cliente no es necesaria, deberá producirse lo siguiente:

- Si el certificado del servidor web de comunidad de concentrador es un certificado con firma personal, los socios deberán tener una copia del mismo.
- Si el certificado del servidor web de comunidad de concentrador procede de una Autoridad certificadora, los socios deberán tener una copia del certificado raíz e intermedio de CA.

Si la autenticación de cliente es necesaria, deberá producirse lo siguiente:

- Si el certificado del servidor web de comunidad de concentrador es un certificado con firma personal, los socios deberán tener una copia del mismo.
- Si el certificado del servidor web de comunidad de concentrador procede de una Autoridad certificadora, los socios deberán tener una copia del certificado raíz e intermedio de CA.
- El servidor de destino debe tener una copia del certificado del socio si éste lleva una firma personal y se carga en el almacén de claves de confianza.
- El servidor de destino debe tener una copia del certificado de las autoridades certificadoras si aquel está autenticado por una CA y se carga en el almacén de claves de confianza.

**Nota:** Las versiones anteriores de WebSphere Partner Gateway no daban soporte al formato de dirección de IPv6. WebSphere Partner Gateway 6.1 sí da soporte a este formato. Asegúrese de que al menos uno de los servidores esté



configurado para dar soporte al formato de direcciones IPv6. La configuración del formato IPv6 sólo es necesaria en el servidor.

## Configuración de certificados SSL entrantes

Esta sección describe cómo configurar la autenticación de servidor y la autenticación de cliente para solicitudes de conexiones entrantes de los socios.

Se realiza una solicitud entrante cuando el socio envía un documento a WebSphere Partner Gateway. Si la comunidad no utiliza SSL, no necesita un certificado SSL entrante o saliente.

**Nota:** Para FTPS entrante, WebSphere Partner Gateway utiliza un Servidor FTP proporcionado por el cliente, por lo que cualquier configuración de SSL entrante corresponde a ese producto de Servidor FTP específico utilizado por el usuario.

**Paso 1: Obtenga un certificado SSL:** WebSphere Application Server utiliza el certificado SSL cuando recibe solicitudes de conexión de socios a través de SSL. Es el certificado que el receptor presenta para identificar el concentrador ante el socio. Este certificado de servidor puede estar autofirmado o puede estar firmado por una CA. En la mayoría de casos utilizará un certificado CA para aumentar la seguridad. Podría utilizar un certificado autofirmado en un entorno de prueba. Utilice iKeyman o la consola administrativa de WebSphere Application Server para generar un par de certificado y clave. Consulte la documentación disponible de IBM para obtener más información sobre el uso de iKeyman o la consola administrativa de WebSphere Application Server.

Después de generar el par de certificado y clave, utilice el certificado para el tráfico SSL entrante para todos los socios. Si tiene varios receptores o consolas, copie el almacén de claves resultante en cada instancia. Si el certificado se genera utilizando la consola administrativa de WebSphere Application Server, la clave y el certificado se pueden importar en otro almacén de claves de otro servidor mediante la consola administrativa de WebSphere Application Server. Si el certificado está autofirmado, proporciónelo a los socios. Para obtener este certificado, utilice iKeyman para extraer el certificado público a un archivo.

*Generación de un certificado autofirmado:* Si va a utilizar certificados de servidor autofirmados, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman, que se encuentra en `/<dir_instalación_WAS>/bin`. Si es la primera vez que utiliza iKeyman, suprima el certificado "ficticio" que reside en el almacén de claves.
2. Abra el almacén de claves de receptor o consola mediante iKeyman, y utilice iKeyman para generar un certificado autofirmado y un par de claves para el almacén de claves de receptor o consola.
3. Use iKeyman para extraer en un archivo el certificado que contendrá la clave pública.  
Guarde el almacén de claves en un archivo JKS, PKCS12 o JCEKS.
4. Distribuya el certificado entre sus socios. El método favorito para la distribución es enviar el certificado en un archivo empaquetado protegido con contraseña y por correo electrónico. Sus socios deben llamarle y solicitar la contraseña para el archivo empaquetado.
5. Mediante la consola administrativa de WebSphere Application Server, establezca el nuevo certificado en la configuración de SSL y en los valores de receptor y consola. Puede hacerlo seleccionando el alias del nuevo certificado en el almacén de claves en la configuración de cada nodo o servidor.

*Obtención de un certificado generado por CA:* Si va a utilizar un certificados firmado por una CA, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman, que se encuentra en el directorio `/<dir_instalación_WAS>/bin`.
2. Use iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
3. Envíe una solicitud de firma de certificado (CSR) a una CA.
4. Cuando reciba el certificado firmado de la CA, use iKeyman para colocar el certificado firmado en el almacén de claves.
5. Distribuya el certificado CA entre todos los socios, si es necesario.
6. Mediante la consola administrativa de WebSphere Application Server, establezca el nuevo certificado en la configuración de SSL y en los valores de receptor y consola. Puede hacerlo seleccionando el alias del nuevo certificado en el almacén de claves en la configuración de cada nodo o servidor.

**Nota:** La consola administrativa de WebSphere Application Server también puede utilizarse para completar los pasos anteriores.

**Paso 2: Autentique clientes:** Si desea autenticar a los socios que envían documentos, realice los pasos de esta sección.

*Instalación del certificado de cliente:* Para la autenticación de cliente, utilice el siguiente procedimiento:

1. Obtenga el certificado del socio.
2. Si el certificado está autofirmado, instale el certificado en el almacén de confianza utilizando iKeyman o la consola administrativa de WebSphere Application Server.
3. Si el certificado está emitido por una CA, añada los certificados CA relacionados en el almacén de confianza relacionado utilizando iKeyman o la consola administrativa de WebSphere Application Server.

**Nota:** Cuando añada más socios a la comunidad de concentrador, puede utilizar iKeyman o la consola administrativa de WebSphere Application Server para añadir sus certificados al almacén de confianza. Si un socio deja la comunidad, puede utilizar iKeyman o la consola administrativa de WebSphere Application Server para eliminar los certificados del socio del almacén de confianza.

*Configuración de autenticación de cliente:* Después de instalar el certificado o los certificados, configure WebSphere Application Server para utilizar la autenticación de cliente ejecutando el script de programa de utilidad `bcgClientAuth.jacl`.

1. Vaya al siguiente directorio: `/<DirProducto>/bin`
2. Para activar la autenticación de cliente, llame al script de la manera siguiente:  

```
./bcgwsadmin.sh -f /<DirProducto>/scripts/bcgClientAuth.jacl  
-conntype NONE set
```

**Nota:** Para desactivar la autenticación de cliente, llame al script de la manera siguiente:

```
./bcgwsadmin.sh -f /<DirProducto>/receiver/scripts/bcgClientAuth.jacl  
-conntype NONE clear
```

Debe reiniciar el servidor `bcgreceiver` para que estos cambios entren en vigor. La autenticación de cliente también puede habilitarse mediante la consola administrativa de WebSphere Application Server. Un valor de "Soportado" quiere

decir que el servidor solicitará un certificado de cliente, pero, si el certificado de cliente no está disponible, el reconocimiento de SSL aún puede establecerse. Un valor de "Necesario" quiere decir que debe enviarse el certificado de cliente. En caso contrario, fallará el reconocimiento de SSL.

*Validación del certificado del cliente:* Hay una característica adicional que puede utilizarse con la autenticación de cliente de SSL. Esta característica está habilitada mediante la Consola de comunidad. Para HTTPS, WebSphere Partner Gateway comprueba los certificados con los ID de empresa en los documentos entrantes. Para utilizar esta característica, cree el perfil del socio, importe el certificado de cliente y márkelo como SSL.

1. Importe el certificado de cliente.
  - a. Pulse **Administrador de cuentas > Perfiles > Socio** y busque el perfil del socio.
  - b. Pulse **Certificados**.
  - c. Pulse **Cargar certificado**.
  - d. Pulse **Examinar** y navegue hasta el directorio en que ha guardado el certificado.
  - e. Seleccione **Cliente SSL** como tipo de certificado.
  - f. Escriba una descripción del certificado (que es necesario).
  - g. Cambie el estado a **Habilitado**.
  - h. Si desea seleccionar una modalidad de operación distinta de **Producción** (el valor predeterminado), selecciónelo de la lista.
  - i. Pulse **Finalizar**.
2. Actualice el destino del cliente.
  - a. Pulse **Administrador de cuentas > Perfiles > Socio** y busque el perfil del socio.
  - b. Pulse **Destinos**.
  - c. Seleccione el destino HTTPS que ha creado anteriormente. Si aún no ha creado el destino HTTPS, consulte "Configuración de un destino HTTPS" en la página 41.
  - d. Pulse el icono **Editar** para editar el destino.
  - e. Seleccione **Sí** para **Validar certificado de cliente SSL**.
  - f. Pulse el botón **Guardar**.

**Configuración de almacén de claves y almacén de confianza separados para receptor y consola:** Por omisión, WebSphere Partner Gateway versión 6.1 utiliza el almacén de claves y el almacén de confianza para receptor y consola. Sin embargo, puede configurar un almacén de claves y un almacén de confianza separados para receptor y consola en la instalación de modalidad distribuida.

Para configurar el almacén de claves y el almacén de confianza, cree y establezca un almacén de claves y un almacén de confianza separados para receptor y consola. Además, cree configuraciones de SSL por separado. Las configuraciones de SSL pueden establecerse en el nivel de clúster o de servidor. Es más sencillo establecer la configuración de SSL en el nivel de clúster, ya que la configuración es aplicable a todos los servidores de ese clúster, y no necesita configurar cada servidor por separado.

*Cómo establecer la configuración de SSL en el nivel de clúster:* Mientras se establece la configuración de SSL con un nuevo almacén de claves y un almacén de confianza en el nivel de clúster, no debe establecerse ninguna configuración de SSL en el

nivel de servidor. Si se ha establecido una configuración de SSL en el nivel de servidor, no se utilizará la configuración de SSL en el nivel de clúster, sino que se utilizará el establecido para el servidor.

Siga estos pasos para establecer la configuración de SSL para bcgconsoleCluster:

1. Cree un almacén de claves para el clúster de consola. El almacén de claves debe crearse en el ámbito del clúster bcgconsole navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
2. Cree un almacén de confianza para el clúster de consola. El almacén de confianza debe crearse en el ámbito del clúster bcgconsole navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
3. Cree una configuración de SSL para el clúster de consola en el ámbito de clúster de consola navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Configuraciones de SSL**. Establezca el almacén de claves y el almacén de confianza que se crearon en los pasos anteriores. Actualice los alias de certificados en la lista pulsando **Obtener alias de certificados** y seleccione el alias necesario que se utilizará para la autenticación de servidor. Establezca el gestor de confianza en **IbmPKIX**.
4. Establezca esta configuración de SSL en bcgconsoleCluster alterando temporalmente la configuración de SSL heredada. Actualice los alias de certificados en la lista pulsando **Actualizar los alias de certificados** y seleccione el alias necesario que se utilizará para la autenticación de servidor.
5. Reinicie bcgconsoleCluster.

Siga estos pasos para establecer la configuración de SSL para bcgreceiverCluster:

1. Cree un almacén de claves para el clúster de receptor. El almacén de claves debe crearse en el ámbito del clúster bcgreceiver navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
2. Cree un almacén de confianza para el clúster de receptor. El almacén de confianza debe crearse en el ámbito del clúster bcgconsole navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
3. Cree una configuración de SSL para el clúster de receptor en el ámbito de clúster de receptor navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Configuraciones de SSL**, y establezca el almacén de claves y el almacén de confianza que se crearon en los pasos anteriores. Obtenga los alias de certificado pulsando **Obtener alias de certificado** y seleccione el alias necesario para que se utilice para la autenticación de servidores. Establezca el gestor de confianza en **IbmPKIX**.
4. Establezca esta configuración de SSL en bcgreceiverCluster alterando temporalmente la configuración de SSL heredada. Actualice los alias de certificados en la lista pulsando **Actualizar los alias de certificados** y seleccione el alias necesario que se utilizará para la autenticación de servidor.
5. Reinicie bcgreceiverCluster.

Para obtener más información sobre cómo trabajar con almacenes de claves, almacenes de confianza, configuración de SSL y configuraciones de puntos finales, consulte la sección *Cómo asegurar las aplicaciones y su entorno de la documentación de WebSphere Application Server*.

**Nota:**

*Configuración de NodeDefaultTrustStore en NodeDefaultSSLSetting, en modalidad distribuida:* Este valor debe establecerse para la modalidad simple distribuida. Sin embargo, esto también es aplicable para la modalidad totalmente distribuida si deben utilizarse un almacén de claves y un almacén de confianza comunes para el receptor y la consola. Si se federa de un nodo en una célula, los certificados de firmante de nodo se añaden a CellDefaultTrustStore. De forma predeterminada, NodeDefaultSSLSetting hace referencia a CellDefaultTrustStore como almacén de confianza. Para el receptor y la consola de WebSphere Partner Gateway, puede que no sea deseable utilizar certificados de firmantes de otros nodos. Para utilizar un almacén de confianza dedicado para los nodos en que está instalado WebSphere Partner Gateway, NodeDefaultTrustStore puede establecerse en NodeDefaultSSLSettings como almacén de confianza.

Los pasos para realizar este cambio son:

1. En la consola administrativa de WebSphere Application Server, navegue hasta **Seguridad > Certificado de SSL y gestión de claves > Gestionar configuraciones de seguridad de punto final > <nombre\_nodo> > SSL configurations > NodeDefaultSSLSettings**.
2. En el campo Nombre de almacén de confianza, seleccione **NodeDefaultTrustStore**.

**Nota:** Asegúrese de que NodeDefaultTrustStore se configura para el almacén de confianza que desea utilizar; por ejemplo, bcgSecurityTrust.jks.

3. Pulse **Aplicar**.
4. En la página siguiente de la consola, pulse **Guardar** para actualizar los cambios en la configuración maestra.
5. Reinicie los servidores en ese nodo.

**Nota:** Para la modalidad totalmente distribuida, los cambios antedichos deben realizarse para todos los nodos que contengan los servidores bcgreceiver y bcgconsole. Para la modalidad simple distribuida, estos cambios deben realizarse para todos los nodos que contengan bcgservr.

*Cómo añadir certificados de firmante a trust.p12 si se establece NodeDefaultTrustStore para el nodo que contenga servidores de WebSphere Partner Gateway:* Actualmente, NodeDefaultTrustStore hace referencia a trust.p12. Si NodeDefaultTrustStore se establece para el nodo que contiene servidores de WebSphere Partner Gateway, no se utilizará bcgSecurityTrust.jks. Los certificados de firmante de bcgSecurityTrust.jks tiene que añadirse a trust.p12 como sea necesario.

## **Configuración de certificados SSL salientes**

Se realiza una solicitud saliente cuando WebSphere Partner Gateway envía un documento a un socio. Si la comunidad no utiliza SSL, no necesita un certificado SSL entrante o saliente.

**Paso 1: Autentique el servidor:** Cuando se utiliza SSL para enviar documentos salientes a los socios, WebSphere Partner Gateway solicita un certificado del servidor a los socios. Puede utilizarse el mismo certificado CA para varios socios. El certificado debe tener el formato X.509 DER.

**Nota:** Puede convertir el formato con el programa de utilidad iKeyman. Siga estos pasos para utilizar iKeyman para convertir el formato:

1. Inicie iKeyman.

2. Cree un nuevo almacén de claves en blanco o abra un almacén de claves existente.
3. En Contenido de base de datos de claves, seleccione **Certificados de firmante**.
4. Añada el certificado de ARM utilizando la opción **Añadir**.
5. Extraiga el mismo certificado como datos DER binarios mediante la opción **Extraer**.
6. Cierre iKeyman.

Instale el certificado autofirmado del socio en el perfil de Operador de concentrador. Si una CA firmó el certificado y tanto el certificado raíz de CA como cualquier otro certificado que forme parte de la cadena de certificados no están instalados ya en el perfil de Operador de concentrador, instale los certificados en el perfil de Operador de concentrador.

1. Pulse **Administrador de cuentas > Perfiles > Certificados** para visualizar la página Lista de certificados.  
Asegúrese de que ha iniciado la sesión en la consola de comunidad como operador de concentrador o socio interno.
2. Pulse **Cargar PKCS12**.

**Nota:** El archivo PKCS12 que se carga debe contener sólo una clave privada y el certificado asociado. También puede cargar el certificado y la clave privada formateada con PKCS#8 por separado.

3. Seleccione **Cliente SSL** como tipo de certificado.
4. Escriba una descripción del certificado (que es necesario).
5. Cambie el estado a **Habilitado**.
6. Pulse **Examinar** y navegue hasta el directorio en que ha guardado el certificado.
7. Seleccione el certificado y pulse **Abrir**.
8. Especifique la contraseña.
9. Si desea seleccionar una modalidad de operación distinta de **Producción** (el valor predeterminado), selecciónelo de la lista.
10. Si tiene dos certificados SSL, indique si éste es el certificado primario o secundario seleccionando **Primario** o **Secundario** de la lista **Utilización de certificado**.
11. Pulse **Cargar** y, a continuación, pulse **Guardar**.

**Nota:** No tiene que realizar los pasos anteriores si el certificado CA ya está instalado.

**Paso 2: Autentique clientes:** Si es necesaria la autenticación de cliente SSL, el socio, a su vez, solicita un certificado al concentrador. Utilice la consola de comunidad para importar el certificado en WebSphere Partner Gateway. Puede generar el certificado utilizando iKeyman. Si el certificado es autofirmado, debe proporcionarse al socio. Si es un certificado firmado por una CA, el certificado raíz CA debe entregarse a los socios para que puedan añadirlo a sus certificados de confianza.

Puede tener más de un certificado SSL. Uno es el certificado primario, que es el utilizado de forma predeterminada. El otro es un certificado secundario, que se utiliza si caduca el certificado primario.

*Utilización de un certificado autofirmado:* Si va a utilizar un certificado autofirmado, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman.
2. Use iKeyman para generar un certificado autofirmado y un par de claves.
3. Use iKeyman para extraer en un archivo el certificado que contendrá la clave pública.
4. Distribuya el certificado entre sus socios. El método favorito para la distribución es enviar el certificado en un archivo empaquetado protegido con contraseña y por correo electrónico. Sus socios deben llamarle y solicitar la contraseña para el archivo empaquetado.
5. Use iKeyman para exportar el certificado autofirmado y el par de claves privadas en forma de archivo PKCS12.
6. Instale el certificado autofirmado y la clave mediante la consola de comunidad.
  - a. Pulse **Administrador de cuentas > Perfiles > Certificados** para visualizar la página Lista de certificados.  
Asegúrese de que ha iniciado la sesión en la consola de comunidad como operador de concentrador.
  - b. Pulse **Cargar PKCS12**.

**Nota:** El archivo PKCS12 que se carga debe contener sólo una clave privada y el certificado asociado. También puede cargar el certificado y la clave privada formateada con PKCS#8 por separado.

- c. Seleccione **Cliente SSL** como tipo de certificado.
- d. Escriba una descripción del certificado (que es necesario).
- e. Cambie el estado a **Habilitado**.
- f. Pulse **Examinar** y navegue hasta el directorio en que ha guardado el certificado.
- g. Seleccione el certificado y pulse **Abrir**.
- h. Especifique la contraseña.
- i. Si desea seleccionar una modalidad de operación distinta de **Producción** (el valor predeterminado), selecciónelo de la lista.
- j. Si tiene dos certificados SSL, indique si éste es el certificado primario o secundario seleccionando **Primario** o **Secundario** de la lista **Utilización de certificado**.
- k. Pulse **Cargar** y, a continuación, pulse **Guardar** .

Si carga certificados primarios y secundarios para la autenticación de cliente SSL y firma digital y carga los certificados primarios como entradas separadas, asegúrese de que los certificados secundarios correspondientes se cargan como dos entradas diferentes.

*Utilización de un certificado firmado por CA:* Si va a utilizar un certificados firmado por una CA, utilice el procedimiento siguiente:

1. Use iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
2. Envíe una solicitud de firma de certificado (CSR) a una CA.
3. Cuando reciba el certificado firmado de la CA, use iKeyman para colocar el certificado firmado en el almacén de claves.
4. Distribuya el certificado CA firmado entre todos los socios.

## Utilización de certificados para habilitar el cifrado

Esta sección describe certificados de cifrado.

### Creación e instalación de certificados de cifrado entrantes

El concentrador utiliza este certificado para descifrar archivos cifrados recibidos de los socios. El concentrador utiliza la clave privada para descifrar los documentos. El cifrado se utiliza para impedir que otros usuarios que no sean el remitente y el receptor vean los documentos en tránsito.

Observe la siguiente restricción importante sobre cómo recibir mensajes AS2 cifrados de socios. Si un socio envía un mensaje AS2 cifrado pero utiliza un certificado erróneo, el descifrado será erróneo. No obstante, no se devuelve ningún MDN al socio para indicar el error. Para que el socio reciba los MDN en esta situación, cree una conexión con el socio con la siguiente definición de documento:

- Paquete: **AS** a Paquete: **Ninguno**
- Protocolo: **Binario** a Protocolo: **Binario**
- Tipo de documento: **Binario** a Tipo de documento: **Binario**

La conexión creada debe ser una conexión AS a Ninguno, es decir, crea una conexión activando la función AS B2B en un socio y Ninguno B2B en el otro. Asegúrese de que la pasarela de origen en el lado AS es una pasarela SMTP (en caso de AS1), pasarela HTTP (en caso de AS2) o pasarela FTP (en caso de AS3), que se configura con la dirección de MDN. Así pues, el error de descifrado de MDN se devuelve a la conexión de Ninguno Binario a través de esta AS.

### Paso 1: Obtenga un certificado:

*Generación de un certificado autofirmado:* Si va a utilizar un certificado autofirmado, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman.
2. Use iKeyman para generar un certificado autofirmado y un par de claves.
3. Use iKeyman para extraer en un archivo el certificado que contendrá la clave pública.
4. Distribuya el certificado entre sus socios. Es necesario que importen el archivo a su producto B2B para su uso como un certificado de cifrado. Aconséjeles que lo utilicen cuando quieran enviar archivos cifrados al socio interno. Si el certificado firmado por CA, proporcione también el certificado CA.
5. Use iKeyman para guardar el certificado autofirmado y el par de claves privadas en forma de archivo PKCS12.
6. Navegue hasta **Perfil > {Operador de concentrador/socio interno} > certificados > Crear nuevo certificado.**
7. En la lista desplegable **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado.
8. Pulse **Buscar** para buscar unos socios específicos o un subconjunto de ellos.
9. Pulse **Examinar** junto a **Ubicación de certificado** para cargar el certificado.
10. Pulse **Siguiente.**
11. En **Proporcionar detalles de certificado**, especifique la siguiente información de certificado: **Certificado sin secundarios**, **Certificado CA raíz** o **Certificado CA intermedio.**
12. Asocie este certificado a **Cifrado.**
13. En **Utilización de certificado**, seleccione **Primario** o **Secundario.**



14. Seleccione **habilitado** o **inhabilitado** en **Estado** en función de si quiere habilitar o inhabilitar el certificado después de la carga
15. Seleccione la **Modalidad de operación**.
16. Pulse **Finalizar** para guardar los cambios y cierre el asistente.

*Utilización de un certificado firmado por CA:* Si va a utilizar un certificados firmado por una CA, utilice el procedimiento siguiente:

1. Inicie el programa de utilidad iKeyman.
2. Use iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
3. Envíe una solicitud de firma de certificado (CSR) a una CA.
4. Cuando reciba el certificado firmado de la CA, use iKeyman para colocar el certificado firmado en el almacén de claves.

**Paso 2: Distribuya el certificado:** Distribuya el certificado CA firmado entre todos los socios.

### **Instalación de certificados de cifrado salientes**

El certificado de cifrado saliente se utiliza cuando el concentrador envía documentos cifrados a los socios. WebSphere Partner Gateway cifra documentos con las claves públicas de los socios, y los socios descifran los documentos con sus claves privadas.

El socio puede tener más de un certificado de cifrado. Uno es el certificado primario, que es el utilizado de forma predeterminada. El otro es un certificado secundario, que se utiliza si caduca el certificado primario.

**Paso 1: Obtenga un certificado de socio:** Obtenga el certificado de cifrado del socio. El certificado debe tener el formato X.509 DER. Tenga en cuenta que WebSphere Partner Gateway sólo da soporte a los certificados X5.09.

**Paso 2: Instale el certificado del socio:** Instale el certificado mediante la consola de comunidad bajo el perfil del socio realizando el procedimiento siguiente:

1. Navegue hasta **Perfil > Socio externo > certificados > Cargar certificado**.
2. En la página **Seleccionar socio, Ubicación de archivos, Contraseña** del asistente, especifique los valores siguientes:
  - En **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado. Pulse **Buscar** para buscar un socio específico o un subconjunto de socios. Si el socio es un Operador de concentrador o un Socio interno, especifique la ubicación del certificado, la ubicación de la clave privada y la contraseña (OR) Proporcione el almacén de confianza o el almacén de claves con la contraseña. Como Socio externo, especifique la ubicación de certificado (OR) proporciona la ubicación del almacén de confianza que contiene la cadena de certificados.
  - **Ubicación de certificado:** pulse **Examinar** para seleccionar la ubicación del certificado público.
3. Pulse **Siguiente** para ir a la página **Detalles de certificado** del asistente.
4. En la página **Detalles de certificado** del asistente, especifique los detalles siguientes del certificado:
  - **Nombre del certificado sin secundarios** - El nombre del certificado sin secundarios. El nombre de campo depende de si el certificado es un certificado sin secundarios, un certificado CA raíz o un certificado CA intermedio.

- **Descripción** - La descripción del certificado sin secundarios.
  - **Tipo de certificado** - Asocie este certificado a Cifrado.
  - **Utilización de certificado** - Asocie una utilización con el certificado. Los valores son Primario y Secundario.
  - **Modalidad de operación** - Especifique la modalidad de operación.
  - **Estado** - Seleccione habilitado o inhabilitado en función de si desea habilitar o inhabilitar un certificado después de la carga. El botón **Siguiente** sólo se habilita si se habilita el certificado.
  - **Gestión de conjuntos**- Puede asociar un certificado a un conjunto existente o crear un conjunto nuevo. Si el certificado es un certificado secundario, sólo puede asociarse a un conjunto existente. Puede asociar el certificado a cualquier conjunto para un socio interno con tipo cifrado o para un socio externo con tipo SSL (autorización de cliente entrante) o Firma (Verificar).
5. Pulse **Siguiente** para ir a la página **Conjunto del asistente**. Si el certificado es primario, no tiene que crear conjuntos y asociar el certificado a un conjunto y una conexión participante. Si ha seleccionado el recuadro de selección **Crear nuevo conjunto**, se abrirá la página **Crear nuevo conjunto** del asistente. En caso contrario, se abrirá la página **Añadir al conjunto existente** del asistente. Si el archivo contiene una clave privada del socio interno o el certificado público del socio externo utilizado por SSL / Firma digital, puede pulsar **Finalizar**.
  6. En la página **Crear nuevo conjunto** del asistente, especifique los detalles del nuevo conjunto. Para los certificados primarios, no tiene que crear conjuntos y asociar un certificado a ellos. Especifique los valores siguientes:
    - **Nombre de conjunto** - El nombre del conjunto.
    - **Descripción** - La descripción del conjunto.
    - **Estado** - Seleccione habilitado o inhabilitado. Si está inhabilitado, no se habilitará el botón **Siguiente**.
    - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
  7. En la página **Añadir al conjunto existente** del asistente, seleccione uno o varios conjuntos para añadir el certificado. Especifique los valores siguientes:
    - **Seleccionar de la lista de conjuntos disponibles para el tipo de certificado seleccionado** - En la lista, seleccione uno o varios conjuntos para añadir el certificado.
    - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
  8. En **Crear nuevo conjunto** o **Añadir al conjunto existente**, pulse **Siguiente** para ir a la página **Valores predeterminados** del asistente. El botón **Siguiente** sólo estará habilitado si el estado del conjunto es habilitado.
  9. Seleccione **habilitado** o **inhabilitado** en **Estado** en función de si quiere habilitar o inhabilitar el certificado después de la carga
- Nota:** Si ha seleccionado el recuadro de selección **Establecer como conjunto predeterminado** en la página anterior (Crear nuevo conjunto o Añadir al conjunto existente), tiene que asociar el conjunto a una modalidad de operación. Se visualizarán las utilidades de certificado según las modalidades de operación. El cifrado se inhabilitará para socios internos. Cliente SSL y Firma digital se inhabilitarán para socios externos.
10. Pulse **Siguiente** para ir a la página **Configuración del asistente**. En caso de que pulse **Finalizar** y falten certificados raíz o CA intermedios, se le solicitará

que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** si desea realizar la carga en una fase posterior.

11. En la página Configuración del asistente, especifique los valores siguientes:

**Nota:** La página Configuración muestra una lista de utilizaciones de (conjunto de) certificados respecto a las modalidades de operación. El nombre de conjunto actual se lleva previamente para todos, pero puede restablecerlo.

- **Desde socio** - Este campo se llena previamente con el valor del socio interno.
  - **A socio** - Esta lista desplegable se llena previamente con la lista de todos los socios externos. También puede seleccionar el valor "Todos" para incluir todos los socios externos.
  - **De paquete** - En la lista desplegable, seleccione el paquete de objetos de definiciones de flujo de documentos del socio interno.
  - **A paquete** - En la lista, seleccione el paquete de objetos de definiciones de flujo de documentos del socio externo.
12. Pulse **Añadir más conexiones** si desea asociar el conjunto a otras conexiones participantes.
  13. Pulse **Añadir certificado secundario** para añadir un certificado secundario al conjunto actual.
  14. Pulse **Finalizar** para cargar el certificado. En caso de que falten certificados raíz o CA intermedios, se le solicitará que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** en la ventana de solicitud si desea realizar la carga en una fase posterior.

Repita este paso si el socio tiene un segundo certificado de cifrado.

**Paso 3: Instale los certificados emitidos por CA:** Si una CA firmó el certificado y tanto el certificado raíz de CA como cualquier otro certificado que forme parte de la cadena de certificados no están instalados ya en el perfil de Operador de concentrador, instale los certificados ahora siguiendo este procedimiento:

**Nota:** No tiene que realizar este paso si el certificado emitido por la CA ya está instalado.

1. Navegue hasta **Perfil > Operador de concentrador > certificados > Crear nuevo certificado**.
2. En la lista desplegable **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado.
3. Pulse **Buscar** para buscar unos socios específicos o un subconjunto de ellos.
4. Pulse **Examinar** junto a **Ubicación de almacén de confianza (o) almacén de claves**.
5. Para Certificado y Almacén de confianza, especifique **Contraseña**.
6. Si es Almacén de confianza, especifique el **Tipo de almacén de claves** y pulse **Siguiente**.
7. En la página **Seleccionar certificado de entidad de destino para subir**, seleccione el certificado que va a cargar.

**Nota:** Cuando cargue certificados utilizando un almacén de confianza que tenga más de un certificado, **Selecione la lista de certificados CA raíz e intermedios que desee subir** se llena con todos los certificados. También puede cargar varios certificados.

8. Pulse **Finalizar**.

**Paso 4: Habilitar cifrado:** Habilite el cifrado en el paquete (nivel superior), socio o nivel de conexión (nivel inferior). El valor puede alterar temporalmente otros valores en el nivel de conexión. El resumen de la conexión le informará si falta algún atributo necesario.

Por ejemplo, para alterar los atributos de una conexión de socio, pulse **Administrador de cuentas > Conexiones** y, a continuación, seleccione los socios. Pulse **Atributos** y, a continuación, edite el atributo (por ejemplo, **AS cifrado**).

Cuando aparece el mensaje de error No se ha encontrado ningún certificado de cifrado válido, ni el certificado primario ni el secundario son válidos. Puede que los certificados hayan caducado o se hayan revocado. Si los certificados han caducado o se han revocado, también podrá verse el suceso correspondiente (Certificado caducado o revocado) en el Visor de sucesos. Tenga en cuenta que estos dos sucesos podrían estar separados por otros sucesos.

Para visualizar el Visor de sucesos, realice lo siguiente:

1. Pulse **Visores > Visor de sucesos**.
2. Seleccione los criterios de búsqueda adecuados.
3. Pulse el botón **Buscar**.

Consulte la publicación *Guía del administrador de WebSphere Partner Gateway* para obtener información sobre el uso del Visor de sucesos.

## Utilización de certificados para habilitar la firma digital

### Creación de un certificado de firma saliente

El Gestor de documentos utiliza este certificado cuando envía documentos firmados salientes a los socios. Se utilizan el mismo certificado y clave para todos los puertos y protocolos.

Puede tener más de un certificado de firma digital. Uno es el certificado primario, que es el utilizado de forma predeterminada. El otro es un certificado secundario, que se utiliza si caduca el certificado primario.

**Generación de un certificado autofirmado:** Si va a utilizar un certificado autofirmado, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman.
2. Use iKeyman para generar un certificado autofirmado y un par de claves.
3. Use iKeyman para extraer en un archivo el certificado que contendrá la clave pública.
4. Distribuya el certificado entre sus socios. El método favorito para la distribución es enviar el certificado en un archivo empaquetado protegido con contraseña y por correo electrónico. Sus socios deben llamarle y solicitar la contraseña para el archivo empaquetado.
5. Use iKeyman para exportar el certificado autofirmado y el par de claves privadas en forma de archivo PKCS12.

### Instalación de certificado firmado saliente:

1. Navegue hasta **Perfil > {Operador de concentrador/Socio interno} > certificados > Cargar certificado**.
2. En la página **Seleccionar socio, Ubicación de archivos, Contraseña** del asistente, especifique los valores siguientes:
  - En **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado. Pulse **Buscar** para buscar un socio específico o un subconjunto de socios. Si el socio es un Operador de concentrador o un Socio interno, especifique la ubicación del certificado, la ubicación de la clave privada y la contraseña (OR) Proporcione el almacén de confianza o el almacén de claves con la contraseña. Como Socio externo, especifique la ubicación de certificado (OR) proporciona la ubicación del almacén de confianza que contiene la cadena de certificados.
  - **Clave privada:** pulse **Examinar** para seleccionar la clave privada del certificado.
  - **Contraseña:** si el certificado tiene una contraseña, especifique el valor.
  - **Ubicación del almacén de confianza (o) almacén de claves:** pulse **Examinar** para seleccionar la ubicación del almacén de claves. El almacén de claves es una colección de claves privadas junto con certificados CA y raíz de confianza.
  - **Contraseña:** especifique la contraseña de Ubicación de almacén de claves.
  - **Tipo:** seleccione el tipo de almacén de confianza (o) almacén de claves. Los valores disponibles en la lista desplegable son: JKS, JCEKS y PKCS12.
3. Pulse **Siguiente** para ir a la página **Detalles de certificado** del asistente. La página **Seleccionar certificados de entidad de destino y CA** del asistente se abrirá cuando cargue certificados mediante un almacén de confianza que tenga más de un certificado. Se muestra la lista de certificados disponibles en el almacén de confianza.
4. En la página **Seleccionar certificados de entidad de destino y CA** del asistente, especifique los valores siguientes:
  - **El almacén de claves contiene más de un certificado de entidad final.** **Seleccione el certificado que desee cargar-** La lista desplegable tiene una lista de todos los certificados de entidad final. Seleccione el certificado que desee cargar
  - **Contraseña** - Si el almacén de claves tiene una contraseña, seleccione este recuadro de selección y especifique la contraseña en el recuadro de texto.
  - **Seleccione la lista de certificados CA raíz e intermedios que desee subir-** En el recuadro de lista, seleccione los certificados raíz y CA intermedio que desee cargar.
5. Pulse **Siguiente** para ir a la página **Detalles de certificado** del asistente.
6. En la página **Detalles de certificado** del asistente, especifique los detalles siguientes del certificado:
  - **Nombre del certificado sin secundarios** - El nombre del certificado sin secundarios. El nombre de campo depende de si el certificado es un certificado sin secundarios, un certificado CA raíz o un certificado CA intermedio.
  - **Descripción** - La descripción del certificado sin secundarios.
  - **Tipo de certificado** - Asocie este certificado a Cifrado.
  - **Utilización de certificado** - Asocie una utilización con el certificado. Los valores son Primario y Secundario.
  - **Modalidad de operación** - Especifique la modalidad de operación.

- **Estado** - Seleccione habilitado o inhabilitado en función de si desea habilitar o inhabilitar un certificado después de la carga. El botón **Siguiente** sólo se habilita si se habilita el certificado.
- **Gestión de conjuntos**- Puede asociar un certificado a un conjunto existente o crear un conjunto nuevo. Si el certificado es un certificado secundario, sólo puede asociarse a un conjunto existente. Puede asociar el certificado a cualquier conjunto para un socio interno con tipo cifrado o para un socio externo con tipo SSL (autorización de cliente entrante) o Firma (Verificar).

**Nota:** Para el operador de concentrador, no habrá gestión de conjuntos. Los certificados se asociarán al conjunto predeterminado que se cree.

7. Pulse **Siguiente** para ir a la página **Conjunto del asistente**. Si el certificado es primario, no tiene que crear conjuntos y asociar el certificado a un conjunto y una conexión participante. Si ha seleccionado el recuadro de selección **Crear nuevo conjunto**, se abrirá la página **Crear nuevo conjunto** del asistente. En caso contrario, se abrirá la página **Añadir al conjunto existente** del asistente. Si el archivo contiene una clave privada del socio interno o el certificado público del socio externo utilizado por SSL / Firma digital, puede pulsar **Finalizar**.
8. En la página **Crear nuevo conjunto** del asistente, especifique los detalles del nuevo conjunto. Para los certificados primarios, no tiene que crear conjuntos y asociar un certificado a ellos. Especifique los valores siguientes:
  - **Nombre de conjunto** - El nombre del conjunto.
  - **Descripción** - La descripción del conjunto.
  - **Estado** - Seleccione habilitado o inhabilitado. Si está inhabilitado, no se habilitará el botón **Siguiente**.
  - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
9. En la página **Añadir al conjunto existente** del asistente, seleccione uno o varios conjuntos para añadir el certificado. Especifique los valores siguientes:
  - **Seleccionar de la lista de conjuntos disponibles para el tipo de certificado seleccionado** - En la lista, seleccione uno o varios conjuntos para añadir el certificado.
  - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
10. En **Crear nuevo conjunto** o **Añadir al conjunto existente**, pulse **Siguiente** para ir a la página **Valores predeterminados** del asistente. El botón **Siguiente** sólo estará habilitado si el estado del conjunto es habilitado.
11. Seleccione **habilitado** o **inhabilitado** en **Estado** en función de si quiere habilitar o inhabilitar el certificado después de la carga

**Nota:** Si ha seleccionado el recuadro de selección **Establecer como conjunto predeterminado** en la página anterior (**Crear nuevo conjunto** o **Añadir al conjunto existente**), tiene que asociar el conjunto a una modalidad de operación. Se visualizarán las utilidades de certificado según las modalidades de operación. El cifrado se inhabilitará para socios internos. Cliente SSL y Firma digital se inhabilitarán para socios externos.

12. Pulse **Siguiente** para ir a la página **Configuración del asistente**. En caso de que pulse **Finalizar** y falten certificados raíz o CA intermedios, se le solicitará que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** si desea realizar la carga en una fase posterior.

13. En la página Configuración del asistente, especifique los valores siguientes:

**Nota:** La página Configuración muestra una lista de utilizaciones de (conjunto de) certificados respecto a las modalidades de operación. El nombre de conjunto actual se lleva previamente para todos, pero puede restablecerlo.

- **Desde socio** - Este campo se llena previamente con el valor del socio interno.
  - **A socio** - Esta lista desplegable se llena previamente con la lista de todos los socios externos. También puede seleccionar el valor "Todos" para incluir todos los socios externos.
  - **De paquete** - En la lista desplegable, seleccione el paquete de objetos de definiciones de flujo de documentos del socio interno.
  - **A paquete** - En la lista, seleccione el paquete de objetos de definiciones de flujo de documentos del socio externo.
14. Pulse **Añadir más conexiones** si desea asociar el conjunto a otras conexiones participantes.
15. Pulse **Añadir certificado secundario** para añadir un certificado secundario al conjunto actual.
16. Pulse **Finalizar** para cargar el certificado. En caso de que falten certificados raíz o CA intermedios, se le solicitará que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** en la ventana de solicitud si desea realizar la carga en una fase posterior.

Si carga certificados primarios y secundarios para la autenticación de cliente SSL y firma digital y carga los certificados primarios como entradas separadas, asegúrese de que los certificados secundarios correspondientes se cargan como dos entradas diferentes.

**Obtención de un certificado firmado por CA:** Si va a utilizar un certificados firmado por una CA, utilice el procedimiento siguiente:

1. Inicie el programa de utilidad iKeyman.
2. Use iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
3. Envíe una solicitud de firma de certificado (CSR) a una CA.
4. Cuando reciba el certificado firmado de la CA, use iKeyman para colocar el certificado firmado en el almacén de claves.
5. Distribuya el certificado CA firmado entre todos los socios.

### **Instalación de un certificado de firma entrante**

El Gestor de documentos utiliza el certificado firmado por el socio para verificar la firma del remitente cuando reciba documentos. Los socios le enviarán sus certificados de firma autofirmados en formato X.509 DER. A su vez, instale los certificados de los socios mediante la consola de comunidad bajo el perfil del socio correspondiente.

Para instalar el certificado, utilice el procedimiento siguiente.

1. Reciba el certificado de firma X.509 del socio en formato DER.
2. Navegue hasta **Perfil > Socio externo > certificados > Cargar certificado**.
3. Pulse **Buscar** para buscar unos socios específicos o un subconjunto de ellos.
4. Pulse **Examinar** junto a **Ubicación de certificado** para cargar el certificado.
5. Pulse **Siguiente** para ir a la página **Detalles de certificado** del asistente.

6. Asocie este certificado a **Firma digital**.
7. Seleccione **habilitado** o **inhabilitado** en **Estado** en función de si quiere habilitar o inhabilitar el certificado después de la carga
8. Seleccione la **Modalidad de operación**. Si es operador de concentrador, no tiene la opción de seleccionar la **modalidad de operación**.
9. Pulse **Finalizar** para guardar los cambios y cierre el asistente.
10. Si una CA firma el certificado y tanto el certificado raíz de CA como cualquier otro certificado que forme parte de la cadena de certificados no están instalados ya en el perfil de Operador de concentrador, instale los certificados ahora. Esto sólo es aplicable al almacén de confianza o al almacén de claves.
  - a. Pulse **Administrador de cuentas > Perfiles > Certificados** para visualizar la página Lista de certificados.

Asegúrese de que ha iniciado la sesión en la consola de comunidad como operador de concentrador e instale el certificado en su propio perfil.
  - b. Pulse **Cargar certificado**.
  - c. Seleccione **Raíz e intermedio**.
  - d. Escriba una descripción del certificado (que es necesario).
  - e. Cambie el estado a **Habilitado**.
  - f. Pulse **Examinar** y navegue hasta el directorio en que ha guardado el certificado.
  - g. Seleccione el certificado y pulse **Abrir**.
  - h. Pulse **Cargar** y, a continuación, pulse **Guardar** .

**Nota:** No tiene que realizar el paso anterior si el certificado CA ya está instalado.

11. Habilite la firma en el paquete (nivel superior), socio o nivel de conexión (nivel inferior). El valor puede alterar temporalmente otros valores en el nivel de conexión. El resumen de la conexión le informará si falta algún atributo necesario.

Por ejemplo, para alterar los atributos de una conexión de socio, pulse **Administrador de cuentas > Conexiones** y, a continuación, seleccione los socios. Pulse **Atributos** y, a continuación, edite el atributo (por ejemplo, **AS firmado**).

---

## Creación de grupos de consola

Utilice la característica Grupo para crear un grupo para un tipo específico de usuario, con privilegios de consola específicos. Por ejemplo, puede que desee crear un grupo Comprobadores para usuarios a los que se les asigne probar la conectividad durante el ciclo de realización de pruebas. Después de crear el grupo Comprobadores, asignaría permisos al grupo según las características de consola a las que los usuarios del grupo deben tener acceso durante el ciclo de realización de pruebas.

El sistema crea automáticamente los grupos Administrador y Predeterminados con los valores de permisos predeterminados. Los valores de permisos predeterminados pueden ser modificados por cualquier grupo de usuarios o de administradores de concentrador, así como por el grupo de administradores del socio.



**Aviso:** El administrador y los grupos predeterminados son generados por el sistema y no se pueden editar ni suprimir. El grupo del Administrador de concentrador tiene un grupo adicional, Administración de concentrador.

Para crear grupos:

1. Pulse **Administración de cuentas > Perfiles > Grupos**. El sistema mostrará la pantalla Lista de grupos.
2. Pulse el botón **Crear** de la esquina superior derecha de la pantalla. El sistema mostrará la pantalla Detalles del grupo.
3. Especifique el **Nombre** y la **Descripción** del nuevo grupo.
4. Pulse **Guardar**. Para añadir grupos adicionales, repita estos pasos.

---

## Creación de usuarios

Utilice esta característica para crear perfiles de usuario. El sistema utiliza perfiles de socio para controlar el acceso a la consola, la entrega de alertas y la visibilidad de los usuarios.

Un perfil de usuario incluye el nombre y la información de contacto (dirección de correo electrónico y números de teléfono) del usuario, su estado de inicio de sesión (Habilitado o Inhabilitado), el estado de alerta del usuario (Habilitado o Inhabilitado) y la visibilidad (Local o Global). El nombre de usuario es exclusivo.

- Si el estado de inicio de sesión de un usuario es **Habilitado**, el usuario podrá iniciar la sesión en la Consola de comunidad. Si el estado de inicio de sesión de un usuario es **Inhabilitado**, el usuario no podrá iniciar la sesión en la Consola de comunidad.
- Si el estado de alerta de un usuario es **Habilitado**, el usuario podrá recibir notificaciones de alerta. Si el estado de alerta de un usuario es **Inhabilitado**, el usuario no podrá recibir notificaciones de alerta.
- Si la visibilidad de un usuario es **Local**, el usuario sólo estará visible para su organización. Si la visibilidad de un usuario es **Global**, el usuario estará visible para toda la comunidad de concentrador.

También puede generar automáticamente una contraseña para el usuario.

## Creación de un nuevo usuario

Utilice esta característica para añadir un nuevo usuario. Después de definir sus usuarios y grupos, podrá añadir usuarios a los grupos.

1. Pulse **Administración de cuentas > Perfiles > Usuarios**. El sistema mostrará la pantalla Lista de usuarios.
2. Pulse el botón **Crear** de la esquina superior derecha de la pantalla. El sistema muestra la pantalla Detalles del usuario.
3. Especifique el **Nombre de usuario** (NOMBRE DE inicio de sesión para el usuario).
4. Seleccione el **Estado** en función de si desea **Habilitar** o **Inhabilitar** el acceso a la consola para este usuario.
5. Especifique el nombre de usuario (**Nombre de pila** y **Nombre de familia**.)
6. Escriba la dirección de **correo electrónico** que utilizará el sistema para enviar notificaciones de alerta al usuario.
7. Especifique el **Teléfono** y los **Números de fax** del usuario.
8. Seleccione el **Entorno local de idioma**, el **Entorno local de formato** y el **Huso horario**.

9. Seleccione el **Estado de alerta** en función de si desea Habilitar o Inhabilitar la notificación de alerta para este usuario. Si la habilita, el usuario recibirá todas las alertas suscritas. Si no, los usuarios no recibirán alertas.

**Nota:** El valor suscrito lo rellena el sistema.

10. Seleccione la **visibilidad suscrita** del usuario en función de si el usuario sólo está visible para la organización (local) o para toda la comunidad de concentrador (global).
11. Pulse el botón **Generar automáticamente contraseña** para generar una contraseña automáticamente. Si decide seleccionar una contraseña para este usuario, especifique la contraseña en los recuadros de texto Contraseña y Volver a entrar contraseña.
12. Pulse **Guardar**. Repita estos pasos para añadir usuarios adicionales.

## Configuración de usuario de FTP

Para habilitar el usuario actual como usuario de FTP, realice lo siguiente:

1. Pulse **Administración de cuentas > Perfiles > Usuarios**. El sistema mostrará la pantalla Lista de usuarios.
2. Seleccione el usuario necesario y pulse el icono **Editar**.
3. Pulse **Configuración de FTP**.
4. Especifique el **Directorio de inicio**, que es la vía de acceso relativa respecto al valor especificado para `bcg.ftp.config.rootdirectory`. Este campo es necesario.
5. Habilite o inhabilite **Permiso de grabación** en el directorio de inicio.
6. Habilite o inhabilite el permiso para **Crear/Eliminar directorio**.
7. Seleccione **Nº máx. de inicios de sesión**, que es el máximo de inicios de sesión simultáneos que están permitidos. Si selecciona Límite personalizado, especifique el valor personalizado en el recuadro de texto.
8. Seleccione **Nº máx. de inicios de sesión desde la misma dirección IP**, que es el máximo de inicios de sesión simultáneos que están permitidos desde la misma dirección IP. Si selecciona Límite personalizado en la lista, especifique el valor personalizado en el recuadro de texto.
9. Seleccione **Tiempo de inactividad máximo**, que es el tiempo máximo de inactividad tras el que se descarta la conexión de usuario. Si selecciona Límite personalizado en la lista, especifique el valor personalizado en el recuadro de texto.
10. Seleccione **Cargas máximas**, que es la velocidad de subida máxima en bytes/seg. Si selecciona Límite personalizado en la lista, especifique el valor personalizado en el recuadro de texto.
11. Seleccione **Descarga máx.**, que es la velocidad de descarga máxima en bytes/seg. Si selecciona Límite personalizado en la lista, especifique el valor personalizado en el recuadro de texto.
12. Pulse **Guardar**.

## Adición de usuarios a grupos

1. Pulse **Administración de cuentas > Perfiles > Usuarios**. El sistema mostrará la pantalla Lista de usuarios.
2. Pulse el icono Ver detalles para ver los detalles de miembros de grupo del usuario de destino.
3. Pulse el icono Editar para editar las pertenencias a grupo del usuario.

4. Seleccione un grupo y pulse **Añadir a grupo** o **Eliminar de grupo** para añadir un usuario a un grupo o eliminarlo de él.
5. Pulse el icono Desactivar edición cuando termine de editar.

---

## Creación de información de contacto

Utilice la característica Contactos para crear información de contacto para el personal clave. Utilizará esta información para identificar a las personas que deben recibir una notificación cuando se producen sucesos y el sistema genera notificaciones de alerta.

Dependiendo del tamaño de su organización, puede que desee enviar notificaciones a distintos contactos cuando se produzcan determinados tipos de suceso. Por ejemplo, cuando un documento no pueda validarse, debería notificárselo al personal de seguridad para que puedan evaluar el problema. Cuando las transmisiones del socio interno excedan los límites normales, debería notificárselo a su administrador de red para garantizar que el sistema está manejando el aumento de transmisiones eficazmente.

Después de crear sus contactos, volverá a la característica Alerta para enlazar los contactos con cada alerta que haya creado.

Para crear nuevos contactos:

1. Pulse **Administración de cuentas > Perfiles > Contactos**. El sistema mostrará una lista de contactos actuales.
2. Pulse el botón **Crear** de la esquina superior derecha de la pantalla. El sistema mostrará la pantalla Detalles de contacto.
3. Especifique el **Nombre de pila** y el **Nombre de familia** del contacto.
4. Escriba la **Dirección** del contacto.
5. Seleccione el **Tipo de contacto** de la lista desplegable (por ejemplo, Jefe de B2B o Jefe de empresa).
6. Escriba la dirección de **correo electrónico** del contacto.
7. Escriba el **Teléfono** y el **Número de fax** del contacto.
8. Seleccione el **Entorno local de idioma**, el **Entorno local de formato** y el **Huso horario**.
9. Seleccione el **Estado de alerta** en función de si desea Habilitar o Inhabilitar la notificación de alerta para este contacto. Cuando esté habilitada, el contacto recibirá todas las alertas suscritas. Cuando esté inhabilitada, el contacto no recibirá alertas.

**Nota:** El valor suscrito lo rellena el sistema.

10. Seleccione la **Visibilidad suscrita** del contacto. Si selecciona Local, el contacto sólo estará visible para su organización. Si selecciona Global, el contacto es visible para el administrador de concentrador y el socio interno. Ambas partes pueden suscribir el contacto a alertas.
11. Pulse **Guardar**. Hay varias formas de añadir el contacto a una alerta:  
Para añadir un contacto a una alerta existente, consulte el apartado "Adición de un nuevo contacto a una alerta existente" en la página 37.  
Para crear una alerta basada en volumen y añadir contactos a la alerta, consulte el apartado "Creación de una alerta basada en volumen" en la página 33.

Para crear una alerta basada en sucesos y añadir contactos a la alerta, consulte el apartado “Creación de una alerta basada en suceso” en la página 35.

---

## Creación de alertas y adición de contactos

La entrega de información sobre los problemas del sistema a las personas adecuadas en el momento correcto es la clave para una resolución rápida de los problemas.

Las alertas de WebSphere Partner Gateway se utilizan para notificar al personal clave sobre fluctuaciones poco corrientes en el volumen de transiciones recibidas, o cuando se producen errores en el proceso de los documentos de empresa.

Una opción complementaria en el módulo Visor, Visor de sucesos, le ayuda a identificar mejor los errores, solucionar los problemas y resolver los errores de proceso.

Una alerta se compone de un mensaje de correo electrónico basado en texto enviado a contactos suscritos o a una lista de distribución de personal clave. Las alertas se basan en la aparición de un suceso de sistema (alerta basada en sucesos) o en el volumen del flujo de documentos esperado (alerta basada en volumen).

- Utilice una alerta basada en volumen para recibir notificación de un aumento o una disminución del volumen de transmisiones.

Por ejemplo, si es un socio externo, puede crear una alerta basada en volumen que le notifique si no recibe transmisiones del socio interno en días laborables (establecer el Volumen en Volumen cero, establecer Frecuencia en Diaria, y seleccionar De lunes a viernes en la opción Días de la semana). Esta alerta puede resaltar las dificultades de transmisión de la red del socio interno.

Si es un socio externo, también puede crear una alerta basada en volumen que le avise cuando el número de transmisiones del socio interno supere flujo normal. Por ejemplo, si normalmente recibe aproximadamente 1.000 transmisiones al día, puede establecer el Volumen esperado en 1.000 y la Desviación de porcentaje en un 25%. La alerta le enviará una notificación cuando reciba más de 1.250 transmisiones al día (también se le enviará una notificación cuando el volumen de las transmisiones caiga por debajo de 750). Esta alerta puede identificar una demanda creciente por parte del socio interno, lo cual, en algún momento, le podría suponer tener que añadir más servidores al su entorno.

Tenga en cuenta que las alertas basadas en el volumen supervisan el volumen con respecto al tipo de documentos seleccionado al crear la alerta. WebSphere Partner Gateway sólo busca documentos que contengan el tipo de documentos seleccionado en la alerta y genera alertas únicamente cuando se cumplen todos los criterios de alerta.

- Utilice una alerta basada en sucesos para recibir una notificación cuando se produzcan errores en el proceso de documentos. Por ejemplo, puede que desee crear una alerta que le notifique si los documentos no se pueden procesar debido a errores de validación o porque se han recibido documentos duplicados. También puede crear alertas que le permitan conocer cuándo un certificado está a punto de caducar.

Utilizará los códigos de suceso predefinidos de WebSphere Partner Gateway para crear alertas basadas en sucesos. Existen cinco tipos de evento: Depuración, Información, Aviso, Error, Crítico. Dentro de cada tipo de suceso, hay muchos sucesos. Puede ver y seleccionar los sucesos predefinidos en la pantalla Alerta: Sucesos. Por ejemplo, 240601 Anomalía en reintento de AS, o 108001 No un certificado.

**Nota:** El socio externo sólo puede crear una alerta basada en volumen en el volumen de documentos enviados al socio interno. Para que el socio externo configure una alerta basada en volumen en el volumen de documentos enviado del socio interno al socio externo, el socio externo debería solicitar al administrador de concentrador que configurara una alerta basada en volumen de parte del socio externo, especificando al socio externo como propietario de la alerta.

**Consejo:**

- Utilice una alerta basada en volumen para recibir una notificación si se espera
- El volumen de transmisión del socio externo o del socio interno desciende por debajo de los límites de funcionamiento. Esta alerta puede resaltar las dificultades de transmisión de la red del socio externo o del socio interno.
- Utilice una alerta basada en sucesos para recibir notificaciones sobre errores en el proceso de documento. Por ejemplo, puede crear una alerta basada en sucesos que le notifique si los documentos no han podido procesarse debido a errores de validación.

## Creación de una alerta basada en volumen

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Pulse el botón **Crear** de la esquina superior derecha de la pantalla. El sistema muestra la pestaña Definición de alertas.
3. Seleccione **Alerta de volumen** para **Tipo de alerta** (se trata del valor predeterminado). El sistema mostrará los recuadros de texto apropiados para una alerta de volumen.
4. Escriba un **Nombre de alerta** para la alerta.
5. Seleccione un **Socio** con derechos para crear una alerta basada en volumen (sólo socio interno y administrador de concentrador).
6. Seleccione **Paquete**, **Protocolo**, y **Tipo de documento** en las listas desplegadas.

El Paquete, Protocolo y Tipo de documento seleccionados deben coincidir con el Paquete, Protocolo y Tipo de documento del socio externo de origen.

7. Seleccione una de las tres opciones de volumen (Esperado, Rango o Volumen cero y, a continuación, siga con el punto 8 en la página 34:
  - **Esperado** - Seleccione Esperado si desea que se genere una alerta cuando el volumen del tipo de documento se desvíe de una cantidad exacta. Siga los pasos siguientes para crear una alerta en un volumen de tipo de documento esperado:
    - a. En el recuadro de texto de Volumen, especifique el número de tipos de documento que espera recibir en un margen de tiempo seleccionado en el punto 8. Especifique sólo números positivos; la alerta no funcionará si introduce un número negativo.
    - b. En el recuadro de texto Desviación de porcentaje, especifique un número que defina el límite a partir del cual se puede desviar el volumen de flujo de documentos antes de que se active la alerta. Por ejemplo:
      - Si Volumen = 20 y Desviación de porcentaje = 10, un volumen de flujo de documentos menor que 18 o mayor que 22 activará una alerta.

- Si Volumen = 20 y Desviación de porcentaje = 0, cualquier volumen de flujo de documentos distinto de 20 activará una alerta.
  - **Rango.** Seleccione Rango para generar una alerta si el volumen de flujo de documentos queda fuera de un rango mínimo-máximo. Lleve a cabo los siguientes pasos para crear una alerta basada en un rango de valores:
    - a. En el recuadro de texto Mín., especifique el número mínimo de tipos de documentos que espera recibir en un margen de tiempo seleccionado en 8. Sólo se activa la alerta si el volumen de flujo de documentos queda por debajo de esta cantidad.
    - b. En el recuadro de texto Máx., especifique el número máximo de tipos de documento que espera recibir en un margen de tiempo seleccionado en el punto 8.
- Nota:** Tanto el recuadro de texto Máx. como el Mín. deben rellenarse al crear una alerta basada en el rango de volúmenes.
- **Volumen cero.** Seleccione Volumen cero para activar una alerta si no se recibe ningún tipo de documento en un margen de tiempo seleccionado en el punto 8.
8. Seleccione Diario o Rango para la trama de tiempo (Frecuencia) que el sistema utilizará para supervisar el volumen de flujo de documentos para la generación de alertas.
    - **Diario.** Seleccione Diario para supervisar el volumen de flujo de documentos uno o más días reales de la semana o el mes. Por ejemplo, seleccione Diario si va a supervisar el volumen de flujo de documentos sólo uno o más días de la semana (por ejemplo, los lunes, o los lunes y los jueves) o del mes (por ejemplo, el 1 y el 15).
    - **Rango.** Seleccione Rango para supervisar el volumen de flujo de documentos entre dos días de la semana o del mes. Por ejemplo, seleccione Rango para supervisar el volumen de flujo de documentos todos los días entre el lunes y el viernes, o todos los días entre el día 5 y el día 20 de cada mes.
  9. Seleccione la hora de inicio y de finalización (día de 24 horas) a las que el sistema supervisará el volumen de flujo de documentos para los días seleccionados en el siguiente paso. Tenga en cuenta que cuando se selecciona una frecuencia Rango, el volumen de flujo de documentos se supervisa desde la hora de inicio del primer día del rango hasta la hora de finalización del último día del rango.
  10. Seleccione los días adecuados de la semana o el mes en que se realizará la supervisión de dicha alerta. Si selecciona Diario como frecuencia, seleccione los días reales de la semana o los días del mes para la supervisión de alertas. Si selecciona Rango como frecuencia, seleccione los dos días de la semana o los dos días del mes entre los que desea que se produzca la supervisión de alertas.
  11. Seleccione el **Estado de alerta** de esta alerta como Habilitado o Inhabilitado.
  12. Pulse **Guardar**.
  13. Pulse la pestaña **Notificar**.
  14. Pulse el icono Editar.
  15. Seleccione un socio (sólo socio interno y administrador de concentrador).
  16. Si el contacto que desea añadir aparece en la lista del recuadro de texto Contactos, seleccione el contacto y pulse el botón **Suscribir**. Vaya al punto 21.

Si el contacto que desea añadir no aparece en la lista del recuadro de texto Contactos, pulse el botón **Añadir nueva entrada a contactos**. El sistema muestra la ventana emergente Crear nuevo contacto.

Tenga en cuenta que la opción Añadir nueva entrada a contactos sólo está presente en el Propietario de alertas para crear contactos asociados con éste. Esta función no permite al Propietario de alertas añadir contactos para los Socios de alertas.

17. Especifique el nombre, la dirección de correo electrónico, y los números de teléfono y de fax del contacto.
18. Seleccione el estado de alerta del contacto.
  - Seleccione **Habilitado** para iniciar el envío de mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
  - Seleccione **Inhabilitado** si no desea enviar mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
19. Seleccione la visibilidad del contacto.
  - Seleccione **Local** para hacer que el contacto sólo sea visible para su organización.
  - Seleccione **Global** para que el contacto sea visible al administrador de concentrador y al socio interno. Ambas partes pueden suscribir el contacto a alertas.
20. Pulse **Guardar** para guardar el contacto; pulse **Guardar & Suscribir** para añadir el contacto a la lista de contactos de esta alerta.
21. Pulse **Guardar**.

**Nota:** Los cambios realizados en alertas basadas en volumen después del periodo de supervisión original, se vuelven efectivos el día del siguiente periodo de supervisión. Por ejemplo, una alerta supervisa de 1-3 PM los miércoles y jueves. El miércoles a las 4 PM, la alerta se cambia para supervisar de 5-7 PM. La alerta no realizará la supervisión dos veces el miércoles; el cambio se volverá efectivo el jueves.

## Creación de una alerta basada en suceso

**Nota:** El servidor de mensajes de correo electrónico de alertas se tiene que configurar. Consulte la *Guía de administración* para configurar el servidor de mensajes de correo electrónico de alerta.

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Pulse el botón **Crear** de la esquina superior derecha de la pantalla. El sistema muestra la pestaña Definición de alertas.
3. Seleccione **Alerta de suceso** para **Tipo de alerta**. El sistema mostrará los recuadros de texto apropiados para una alerta basada en suceso.
4. Escriba un **Nombre de alerta** para la alerta. Será el identificador para esta alerta.
5. Seleccione un **Socio** que active la alerta (esta opción sólo está disponible para el socio interno y el administrador de concentrador).

Seleccione la opción **Cualquier socio** para asociar la alerta a todos los socios del sistema. Cuando realice la búsqueda de una alerta y seleccione **Cualquier socio** como **Socio de alerta**, el sistema mostrará todas las alertas que no estén asociadas a un socio específico.

6. Seleccione **Paquete**, **Protocolo**, y **Tipo de documento** en las listas desplegables.
7. Seleccione el tipo de suceso: **Depuración**, **Información**, **Aviso**, **Error**, **Crítico** o **Todos**. Cada uno actúa como filtro para limitar los sucesos que aparecen en la lista **Nombres de suceso**.
8. Seleccione el suceso que activará la alerta, por ejemplo, **BCG240601 Anomalía de reintento de AS** o **108001 No un certificado**. Para crear una alerta que le notifique cuándo un certificado está a punto de caducar, seleccione una de las siguientes opciones:
  - **BCG108005** Caducidad de certificado en 60 días
  - **BCG108006** Caducidad de certificado en 30 días
  - **BCG108007** Caducidad de certificado en 15 días
  - **BCG108008** Caducidad de certificado en 7 días
  - **BCG108009** Caducidad de certificado en 2 días
9. Seleccione el estado de esta alerta: **Habilitado** o **Inhabilitado**.
10. Pulse el botón **Guardar**.
11. Pulse la pestaña **Notificar**.
12. Pulse el icono **Editar**.
13. Seleccione un socio (sólo socio interno y administrador de concentrador).
14. Si el contacto que desea añadir aparece en la lista del recuadro de texto **Contactos**, seleccione el contacto y pulse el botón **Suscribir**. Vaya a 19.  
Si el contacto que desea añadir no aparece en la lista del recuadro de texto **Contactos**, pulse el botón **Añadir nueva entrada a contactos**. El sistema muestra la ventana emergente **Crear nuevo contacto**.  
Tenga en cuenta que la opción **Añadir nueva entrada a contactos** sólo está presente en el **Propietario de alertas** para crear contactos asociados con éste. Esta función no permite al **Propietario de alertas** añadir contactos para los **Socios de alertas**.
15. Especifique el nombre, la dirección de correo electrónico, y los números de teléfono y de fax del contacto. Sólo se utiliza la dirección de correo electrónico para enviar alertas. El resto de las entradas es únicamente para ofrecer información adicional.
16. Seleccione el estado de alerta del contacto.
  - Seleccione **Habilitado** para iniciar el envío de mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
  - Seleccione **Inhabilitado** si no desea enviar mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
17. Seleccione la visibilidad del contacto.
  - Seleccione **Local** para hacer que el contacto sólo sea visible para su organización.
  - Seleccione **Global** para que el contacto sea visible al administrador de concentrador y al socio interno. Ambas partes pueden suscribir el contacto a alertas.
18. Pulse el botón **Guardar** para guardar el contacto. Pulse el botón **Guardar y suscribir** para guardar el contacto y añadir el contacto a la lista de contactos de esta alerta.
19. Seleccione la modalidad de entrega:
  - **Enviar alertas inmediatamente**. Si selecciona esta opción, el sistema enviará notificaciones de alerta al contacto cuando se produzca la alerta. Utilice esta opción para alertas críticas.



- **Alertas de lote por.** Si selecciona esta opción, puede especificar cuándo desea que el contacto reciba las notificaciones de alerta. Utilice esta opción para alertas no críticas.

Las dos opciones de esta sección, Número y Tiempo, no son mutuamente excluyentes.

Si selecciona la opción Número, deberá seleccionar siempre la opción Tiempo.

- Si el número de alertas (Número) se alcanza durante el límite de tiempo que ha seleccionado (Tiempo), el sistema generará una notificación de alerta.
- Si se produce una alerta pero el número de alertas (Número) no se alcanza durante el límite de tiempo que ha seleccionado (Tiempo), el sistema generará una notificación de alerta al final del límite de tiempo.

La opción Tiempo se puede utilizar sin la opción Número, pero la opción Número debe siempre estar asociada con un límite de tiempo (Tiempo).

- **Número.** Debe también utilizar la opción Tiempo cuando seleccione esta opción. Especifique un número (n). Se trata del número de alertas que deben producirse durante el periodo de tiempo seleccionado (Tiempo), antes de que el sistema envíe una notificación de alerta al contacto de la alerta.

He aquí un ejemplo de cómo funcionan juntas estas dos opciones:

En nuestro ejemplo, las opciones de Alertas de lote por se establecen en 10 para Número (10 alertas) y en 2 para Tiempo (periodo de 2 horas). El sistema retiene todas las notificaciones para esta alerta hasta que se producen 10 en un periodo de dos horas o hasta que se alcanza el final del periodo de tiempo.

Cuando el número de alertas alcanza 10 en un periodo de 2 horas, el sistema envía todas las notificaciones de alerta para esta alerta al contacto.

Si se produce una alerta pero no se producen 10 alertas durante el límite de tiempo (dos horas), el sistema envía una notificación de alerta al contacto de la alerta al final del límite de tiempo.

- **Tiempo.** Seleccione el número de horas (n). El sistema retiene la notificación de alerta durante n horas. Cada n horas, el sistema envía todas las notificaciones de alerta retenidas al contacto.

Por ejemplo, si especifica 2, el sistema retendrá todas las notificaciones para esta alerta que se produzcan en cada intervalo de dos horas.

Cuando caduque el intervalo de dos horas, el sistema enviará todas las notificaciones de alerta para esta alerta al contacto.

20. Pulse el botón **Guardar**.

## Adición de un nuevo contacto a una alerta existente

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Especifique los criterios de búsqueda en las listas desplegables; escriba el nombre de alerta.
3. Pulse el botón **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.
4. Pulse el icono Ver detalles para ver detalles de la alerta.
5. Pulse el icono Editar para editar detalles de la alerta.
6. Pulse la pestaña **Notificar**.

7. Seleccione un socio (sólo socio interno y administrador de concentrador).
8. Si el contacto que desea añadir aparece en la lista del recuadro de texto Contactos, seleccione el contacto y pulse el botón **Suscribir**. Vaya al punto 13.  
Si el contacto que desea añadir no aparece en la lista del recuadro de texto Contactos, pulse el botón **Añadir nueva entrada a contactos**. El sistema muestra la ventana emergente Crear nuevo contacto.  
Tenga en cuenta que la opción Añadir nueva entrada a contactos sólo está presente en el Propietario de alertas para crear contactos asociados con éste. Esta función no permite al Propietario de alertas añadir contactos para los Socios de alertas.
9. Especifique el nombre, la dirección de correo electrónico, y los números de teléfono y de fax del contacto.
10. Seleccione el estado de alerta del contacto.
  - Seleccione **Habilitado** para iniciar el envío de mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
  - Seleccione **Inhabilitado** si no desea enviar mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
11. Seleccione la visibilidad del contacto.
  - Seleccione **Local** para hacer que el contacto sólo sea visible para su organización.
  - Seleccione **Global** para que el contacto sea visible al administrador de concentrador y al socio interno. Ambas partes pueden suscribir el contacto a alertas.
12. Pulse el botón **Guardar** para guardar el contacto. Pulse el botón **Guardar y suscribir** para guardar el contacto y añadir el contacto a la lista de contactos de esta alerta.
13. Pulse el botón **Guardar**.

---

## Creación de una dirección nueva

Utilice esta función para crear las direcciones en su perfil de socio. El sistema está configurado para dar soporte a varios tipos de dirección para ubicaciones Corporativas, Facturación y Técnicas.

Para crear una nueva dirección:

1. Pulse **Administración de cuentas > Perfiles > Direcciones**. El sistema mostrará la pantalla Direcciones.
2. Pulse el botón **Crear nueva dirección** en la esquina superior derecha de la pantalla. El sistema mostrará la pantalla Direcciones.
3. Seleccione el tipo de dirección en la lista desplegable (Facturación, Corporativa o Técnica).
4. Especifique la dirección en los recuadros de texto correspondientes.
5. Pulse el botón **Guardar**.

---

## Capítulo 3. Creación de destinos

Los destinos definen puntos de entrada en el sistema. Este capítulo incluye instrucciones para crear destinos y contiene los siguientes temas:

- “Visión general”
- “Configuración de un destino HTTP”
- “Configuración de un destino HTTPS” en la página 41
- “Configuración de un destino FTP” en la página 42
- “Configuración de un destino SMTP” en la página 43
- “Configuración de un destino JMS” en la página 44
- “Configuración de un destino de directorio de archivos” en la página 45
- “Configuración de un destino FTPS” en la página 47
- “Configuración de un destino de scripts FTP” en la página 48
- “Configuración de manejadores” en la página 51
- “Especificación de un destino predeterminado” en la página 51

---

### Visión general

WebSphere Partner Gateway utiliza destinos para direccionar los documentos a sus destinos. El receptor puede ser un socio externo o interno. El protocolo de transporte de salida determina la información que se utiliza durante la configuración del destino.

Los siguientes transportes están soportados (de manera predeterminada) para los destinos de socios:

- HTTP/1.1
- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

**Nota:** Puede definir un destino SMTP para socios externos únicamente (no para el socio interno).

- Directorio de archivos
- FTP Scripting

También puede especificar un transporte definido por el usuario, que va a subir durante la creación del destino.

---

### Configuración de un destino HTTP

Configure un destino HTTP para que se puedan enviar documentos del concentrador a la dirección IP del socio. Cuando configura un destino HTTP, también se especifica que los documentos se envíen a través de un servidor proxy configurado.

Para iniciar un proceso de creación de un destino HTTP, utilice el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

## Detalles del destino

En la página **Lista de destinos**, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario. Es el nombre que aparecerá en la lista de destinos.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

## Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Opcionalmente, seleccione el servidor proxy que se va a utilizar. La **Lista de proxy de avance** incluye los servidores proxy que ha creado, incluido el servidor proxy predeterminado. El valor predeterminado de este campo es **Utilizar proxy de avance predeterminado**. Si desea que el socio seleccionado utilice un servidor proxy distinto, seleccione ese servidor en la lista. Si no desea utilizar esta característica con el socio seleccionado, seleccione **No utilizar proxy de avance**.

2. Seleccione **HTTP/1.1** en la lista **Transporte**.

3. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.

El formato es: `http://<nombre servidor>:<puerto opcional>/<vía acceso>`

Un ejemplo de este formato sería:

`http://anotherserver.ibm.com:57080/bcgreceiver/Receiver`

Al configurar un destino que se va a utilizar con un servicio web, especifique el URL privado que proporciona el proveedor de servicio web. Ahí es donde WebSphere Partner Gateway invocará el servicio web cuando actúe como proxy para el proveedor de servicios web.

4. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor HTTP.
5. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
6. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
7. En el campo **Número de hebras**, escriba el número de documentos que se pueden procesar simultáneamente. El valor predeterminado es 3.
8. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
9. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la

entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.

10. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
11. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores” en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino HTTPS

Configure un destino HTTPS para que se puedan enviar documentos del concentrador a la dirección IP del socio. Cuando configura un destino HTTPS, también se especifica que los documentos se envíen a través de un servidor proxy configurado.

Para crear destinos HTTPS, utilice el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

### Detalles del destino

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

### Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **HTTPS/1.0** o **HTTPS/1.1** en la lista **Transporte**. La configuración del destino de HTTP/S no contiene la configuración de avance.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.

El formato es: `https://<nombre servidor>:<puerto opcional>/<vía acceso>`

Por ejemplo:

`https://anotherserver.ibm.com:57443/bcgreceiver/Receiver`

3. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor HTTP seguro.
4. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.

6. En el campo **Número de hebras**, escriba el número de documentos que se pueden procesar simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Validar certificado SSL de cliente**, seleccione **Sí** si desea que el certificado digital del socio remitente se valide comparándolo con el ID de empresa asociado con el documento. El valor predeterminado es **No**.
9. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.  
Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.
10. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
11. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino FTP

Para crear un destino FTP, siga el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

### Detalles del destino

En la página Detalles de destino, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

### Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **FTP** en la lista **Transporte**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.

El formato es: `ftp://<nombre servidor ftp>:<núm_puerto>`

Por ejemplo:

`ftp://ftpsrvr1.ibm.com:2115`

Si no especifica un número de puerto, se utiliza el puerto FTP estándar.

3. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor FTP.

4. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
6. En el campo **Número de hebras**, escriba el número de documentos que se pueden procesar simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.  
Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.
9. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
10. En el campo **Utilizar nombre de archivo exclusivo**, deje el recuadro seleccionado si lo desea. De lo contrario, pulse el recuadro para quitar la marca de selección. Si selecciona **Utilizar nombre de archivo exclusivo**, el nombre de archivo original se almacenará en la base de datos.
11. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores” en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino SMTP

Para crear un destino SMTP, utilice el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

### Detalles del destino

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

### Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **SMTP** en la lista **Transporte**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.

El formato es: `mailto:<usuario@nombre_servidor>`

Por ejemplo:

mailto:admin@anotherserver.ibm.com

3. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor SMTP.
4. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
6. En el campo **Número de hebras**, escriba el número de documentos que se pueden procesar simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.  
Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.
9. En el campo **Autenticación obligatoria**, indique si el documento proporciona un nombre de usuario y contraseña. El valor predeterminado es **No**.
10. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino JMS

Para crear destinos JMS, siga el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

### Detalles del destino

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

### Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **JMS** en la lista **Transporte**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.

Para WebSphere MQ JMS, el formato del URI de destino es el siguiente:

file:///<vía\_acceso\_enlaces\_MQ\_JNDI\_definidos\_por\_el\_usuario>



Por ejemplo:

```
file:///opt/JNDI-Directory
```

El directorio contiene el archivo “.bindings” para JNDI basado en archivo. Este archivo indica a WebSphere Partner Gateway cómo direccionar el documento al destino que desee. Este campo es necesario.

3. Si lo desea, especifique un nombre de usuario de y contraseña de JMS si son necesarios para acceder a la cola JMS.
4. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
6. En el campo **Número de hebras**, escriba el número de documentos que se pueden procesar simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.  
Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.
9. En el campo **Autenticación obligatoria**, indique si el documento proporciona un nombre de usuario y contraseña. El valor predeterminado es **No**.
10. En el campo **Nombre de fábrica JMS**, especifique el nombre de la clase Java que el proveedor JMS utiliza para conectarse a la cola JMS. Este campo es necesario.
11. En el campo **Clase de mensaje JMS**, especifique la clase de mensaje. Puede seleccionar cualquier clase de mensaje JMS válida, como mensajes de texto o mensajes de bytes. Este campo es necesario.
12. En el campo **Tipo de mensaje JMS**, especifique el tipo de mensaje. Este campo es opcional.
13. En el campo **Paquetes de URL del proveedor**, especifique el nombre de las clases (o archivo JAR) que utiliza Java para entender el URL del contexto de JMS. Este campo es opcional. Si no especifica un valor, se utiliza la vía de acceso del sistema de archivos al archivo de enlaces.
14. En el campo **Nombre de cola JMS**, especifique el nombre de la cola JMS a la que se enviarán los documentos. Este campo es necesario.
15. En el campo **Nombre de fábrica JMS JNDI**, especifique el nombre de fábrica utilizado para conectarse al servicio de nombres. Este campo es necesario.
16. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores” en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino de directorio de archivos

Para crear destinos de directorio de archivos, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

## Detalles del destino

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

## Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **Directorio de archivos** en la lista **Transporte**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.

El formato para sistemas UNIX y sistemas Windows en los que el directorio de archivos se encuentra en la misma unidad en que está instalado WebSphere Partner Gateway es: `file:/// <vía_acceso_directorio_destino>`

Por ejemplo:

```
file:///localfiledir
```

donde *localfiledir* es un directorio del directorio raíz.

Para los sistemas Windows en los que el directorio de archivos se encuentra en una unidad distinta a la de WebSphere Partner Gateway, el formato es:

```
file:/// <letra_unidad>:/ <vía_acceso>
```

3. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
4. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
5. En el campo **Número de hebras**, escriba el número de documentos que se deben procesar simultáneamente. El valor predeterminado es 3.
6. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
7. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.

8. En el campo **Utilizar nombre de archivo exclusivo**, deje el recuadro seleccionado si lo desea. De lo contrario, pulse el recuadro para quitar la marca de selección. Si selecciona **Utilizar nombre de archivo exclusivo**, el nombre de archivo original se almacenará en la base de datos.
9. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino FTPS

Para crear destinos FTPS, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

### Detalles del destino

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

### Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **FTPS** en la lista **Transporte**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Este campo es necesario.  
El formato es: `ftp://<nombre servidor ftp>:<núm_puerto>`  
Por ejemplo:  
`ftp://ftpserver1.ibm.com:2115`  
Si no especifica un número de puerto, se utiliza el puerto FTP estándar.
3. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor FTP seguro.
4. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
6. En el campo **Número de hebras**, escriba el número de documentos que se deben procesar simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí** si desea que la dirección IP del emisor se valide antes de que se procese el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si va a producirse una anomalía en la entrega porque se haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.  
Cuando selecciona **Cola automática**, todos los documentos siguen en cola hasta que el destino se coloca en línea manualmente.
9. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
10. En el campo **Utilizar nombre de archivo exclusivo**, deje el recuadro seleccionado si lo desea. De lo contrario, pulse el recuadro para quitar la

marca de selección. Si selecciona **Utilizar nombre de archivo exclusivo**, el nombre de archivo original se almacenará en la base de datos.

- Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores” en la página 51. De lo contrario, pulse **Guardar**.

---

## Configuración de un destino de scripts FTP

Un destino de scripts FTP se ejecuta de acuerdo con la planificación establecida. El comportamiento de un destino de scripts FTP se controla mediante un script de mandatos FTP.

### Creación de scripts FTP

Para utilizar un destino de scripts FTP, cree un archivo que incluya todos los mandatos FTP necesarios que puede aceptar el servidor FTP.

- Cree un script para los destinos, para indicar las acciones que desea llevar a cabo. En el siguiente script se muestra un ejemplo de cómo conectarse al servidor FTP especificado (con el nombre y la contraseña especificados), pasar al directorio especificado en el servidor FTP y enviar todos los archivos al directorio especificado en el servidor.

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
cd %BCGOPTIONx%
mput *
quit
```

Los indicadores de posición (por ejemplo, %BCGSERVERIP%) se sustituyen cuando el destino se pone en funcionamiento por los valores que se entran cuando se crea una instancia específica de un destino de scripts FTP, tal como se muestra en la tabla siguiente:

*Tabla 3. Cómo correlacionar los parámetros de script con las entradas de campo de destino de scripts FTP*

| Parámetro de script | Entrada de campo de pasarela de scripts FTP             |
|---------------------|---|
| %BCGSERVERIP%       | IP de servidor  |
| %BCGUSERID%         | ID de usuario   |
| %BCGPASSWORD%       | Contraseña  |
| %BCGOPTIONx%        | Opción <i>x</i> , en Atributos definidos por el usuario |

Puede haber hasta 10 opciones definidas por el usuario.

- Guarde el archivo.

### Mandatos de scripts FTP

Puede utilizar los siguientes mandatos al crear el script:

- ascii, binary, passive  
Estos mandatos no se envían al servidor FTP. Modifican la modalidad de transferencia (ascii, binary o passive) en el servidor FTP.
- cd  
Este mandato le lleva al directorio especificado.
- delete  
Este mandato suprime un archivo del servidor FTP.

- **mkdir**  
Este mandato crea un directorio en el servidor FTP.
- **mput**  
Este mandato acepta un solo argumento, que especifica los archivos que deben transferirse al sistema remoto. Este argumento puede contener los caracteres comodín estándar para identificar varios archivos ('\*' y '?').
- **open**  
Este mandato necesita 3 parámetros: dirección IP, nombre de usuario y contraseña del servidor ftp. Estos parámetros se correlacionan con las variables %BCGSERVERIP% %BCGUSERID% y %BCGPASSWORD%, respectivamente. La primera línea del script de destino de FTP Scripting debe ser:open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% .
- **quit, bye**  
Este mandato finaliza una conexión existente con un servidor FTP.
- **quote**  
Este mandato indica que todo lo que siga a QUOTE debe enviarse al sistema remoto como mandato. Esto permite enviar a un servidor FTP remoto mandatos que es posible que no estén definidos en el protocolo FTP estándar.
- **rmdir**  
Este mandato suprime un directorio del servidor FTP.
- **site**  
Este mandato puede utilizarse para emitir mandatos específicos del sitio al sistema remoto. El sistema remoto determina si el contenido de este mandato es válido.

## Destinos de scripts FTP

Si va a utilizar destinos de scripts FTP, realice las siguientes tareas:

Para crear destinos de scripts FTP, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

## Detalles del destino

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Este campo es necesario.
2. Indicar opcionalmente el estado del destino. El valor predeterminado es **Habilitada**. Un destino que está habilitado para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

## Configuración del destino

En el apartado **Configuración de destino** de la página, siga estos pasos:

1. Seleccione **Scripts FTP** en la lista **Transporte**.
2. Escriba la dirección IP del servidor FTP al que está enviando documentos. El valor aquí especificado sustituirá al valor %BCGSERVERIP% cuando se ejecute el script FTP.

3. Escriba el ID de usuario y la contraseña necesarios para acceder al servidor FTP. Los valores aquí especificados sustituirán a %BCGUSERID% y %BCGPASSWORD% cuando se ejecuta el script FTP.
4. Si el destino está en modalidad segura, utilice el valor predeterminado **Sí** para **Modalidad FTPS**. De lo contrario, pulse **No**.
5. Para subir el archivo de script, siga estos pasos:
  - a. Pulse **Subir archivo de script**.
  - b. Escriba el nombre del archivo que contiene el script para procesar documentos o utilice **Examinar** para desplazarse hasta el archivo.
  - c. Pulse **Cargar archivo** para cargar el archivo de script en el recuadro de texto de archivo **Archivo de script cargado actualmente**.
  - d. Si el archivo de script es el que desea utilizar, pulse **Guardar**.
  - e. Pulse **Cerrar ventana**.
6. En el campo **Recuento de reintentos**, escriba el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
7. En el campo **Intervalo de reintentos**, escriba la cantidad de tiempo que el destino debe esperar antes de intentar enviar el documento de nuevo. El valor predeterminado es 300 segundos.
8. En **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
9. En el campo **Bloquear usuario**, indique si el destino solicitará un bloqueo, para que ninguna otra instancia de un destino de scripts FTP pueda acceder al mismo directorio del servidor FTP a la vez.

## Atributos definidos por el usuario

Si desea especificar atributos adicionales, realice los pasos siguientes. El valor que especifique para la opción sustituirá al valor %BCGOPTIONx% cuando se ejecute el script FTP (donde *x* corresponde al número de la opción).

1. Pulse **Nuevo**.
2. Escriba un valor junto a la **Opción 1**.
3. Si va a especificar atributos adicionales, vuelva a pulsar **Nuevo** y escriba un valor.
4. Repita el paso 3 tantas veces como sea necesario para definir todos los atributos.

Por ejemplo, supongamos que el script FTP es parecido al siguiente:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  cd %BCGOPTION1%
  mput *
  quit
```

En este caso %BCGOPTION% sería un nombre de directorio.

## Planificación

En el apartado Planificación de la página, realice los siguientes pasos:

1. Indique si desea la planificación basada en intervalos o la planificación basada en agenda.

- Si elige **Planificación basada en intervalos**, seleccione el número de segundos que deben transcurrir antes de sondear el destino (o aceptar el valor predeterminado).
  - Si selecciona **Planificación basada en agenda**, elija el tipo de planificación (**Planificación diaria**, **Planificación semanal** o **Planificación personalizada**).
    - Si selecciona **Planificación diaria**, especifique la hora del día en que debe sondearse el destino.
    - Si elige **Planificación semanal**, seleccione uno o más días de la semana además de la hora del día.
    - Si elige **Planificación personalizada**, seleccione la hora del día y luego **Rango** o **Días selectivos** para la semana y el mes. Con **Rango**, indique la fecha de inicio y la fecha de finalización. (Por ejemplo, pulse **Lunes** y **Viernes** si desea que el servidor se sondee a una determinada hora únicamente los días laborables). Con **Días selectivos** puede elegir los días concretos de la semana y del mes.
2. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores”. De lo contrario, pulse **Guardar**.

---

## Configuración de manejadores

Puede modificar dos puntos de proceso para un destino: el preproceso y el postproceso.

No se proporciona ningún manejador predeterminado para el paso de preproceso o postproceso y, por lo tanto, no se lista ningún manejador predeterminado en la **Lista disponible**. Si ha subido un manejador, puede seleccionarlo y moverlo a la **Lista configurada**.

Para aplicar un manejador escrito por el usuario a estos puntos de configuración, antes debe subir el manejador. Consulte la *Guía de configuración del concentrador* para obtener información sobre cómo subir el manejador. A continuación, siga estos pasos:

1. Seleccione **preproceso** o **postproceso** en la lista **Manejadores de puntos de configuración**.
2. Seleccione el manejador en la **Lista disponible** y pulse **Añadir**.
3. Si desea cambiar los atributos del manejador, selecciónelo en la **Lista configurada** y pulse **Configurar**. Aparecerá una lista de atributos que pueden cambiarse. Haga los cambios necesarios y pulse **Establecer valores**.
4. Pulse el botón **Guardar**.

Puede modificar más la **Lista configurada** como se indica a continuación:

- Elimine un manejador seleccionándolo en la **Lista configurada** y pulsando **Eliminar**. El manejador pasa a la **Lista disponible**.
- Para cambiar el orden en que se procesa el manejador, seleccione el manejador y pulse **Mover arriba** o **Mover abajo**.

---

## Especificación de un destino predeterminado

Después de crear destinos para el socio interno o externo, seleccione uno de los destinos como destino predeterminado

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. Pulse **Crear**.

3. Pulse **Ver destinos predeterminados**.  
Aparece una lista de destinos definidos para el socio.
4. En la lista **Producción**, seleccione el destino que será el valor predeterminado para este socio. También puede establecer destinos predeterminadas para otros tipos de destinos, como **Prueba**.
5. Pulse el botón **Guardar**.



---

## Capítulo 4. Gestión de conexiones de comunidad y usuarios: Administración de cuentas

Las características del módulo Administración de cuentas controlan cómo y quién utiliza WebSphere Partner Gateway.

Por ejemplo, puede controlar el acceso a la Consola de comunidad y cada una de sus características. Puede controlar quién recibe alertas cuando se producen sucesos importantes. Los ejemplos de sucesos incluyen Conexión de socio no encontrada, Error de validación de RosettaNet y Error al entregar documento.

También utilizará este módulo para mantener el perfil de socio, los certificados, los destinos, los usuarios, los grupos, los contactos, las direcciones, las alertas y las posibilidades de B2B. (Las posibilidades de B2B definen los tipos de procesos empresariales que su sistema puede enviar y recibir). Si participó en el proceso de configuración, ya estará familiarizado con estas características.

*Tabla 4. Características de Administración de cuentas*

---

### ¿Qué característica desea utilizar?

“Gestión de destinos”  
“Gestión de certificados” en la página 55  
“Gestión de grupos” en la página 55  
“Gestión de usuarios” en la página 56  
“Gestión de contactos” en la página 58  
“Gestión de alertas” en la página 60  
“Gestión de direcciones” en la página 62

---

---

## Gestión de destinos

Utilice la característica Destinos para ver la información de destino utilizada para direccionar documentos a su destino correcto. Puede ver el URI de destino, el protocolo de transporte y el estado del destino desde esta característica.

**Atención:** Algunos valores de destino dependen del protocolo de transporte seleccionado. Las restricciones se anotan en los procedimientos y en las tablas de valores.

### Visualización de una lista de destinos

Pulse **Administración de cuentas > Perfiles > Destinos** para ver una lista de destinos del sistema.

### Visualización o edición de detalles de destino

**Importante:** Si inhabilita un destino, también inhabilitará la conexión de socio asociada con el destino. El destino no funcionará. Si establece el destino fuera de línea, los documentos permanecerán en cola hasta que el destino se vuelva a poner en línea.

1. Pulse **Administración de cuentas > Perfiles > Destinos**. El sistema mostrará la pantalla Lista de destinos.
2. Pulse el icono Ver detalles para ver detalles de los destinos.

3. Pulse el icono Editar para editar detalles de destino.
4. Edite la información según proceda. La siguiente tabla describe los valores de destino.

Tabla 5. Valores en la pantalla de destino

| Valor                     | Descripción  |
|---------------------------|--|
| Nombre de destino         | Nombre de destino.<br><br>Nota: Nombre de destino es un campo de libre formato definido por el usuario. Los usuarios deberían utilizar nombres diferentes para los destinos individuales a fin de evitar posibles confusiones. |
| Transporte                | Protocolo utilizado para direccionar documentos.   |
| URI de destino            | URI de destino.  |
| En línea o Fuera de línea | Si es fuera de línea, los documentos permanecerán en cola hasta que el destino se ponga en línea.  |
| Estado                    | Habilitado o Inhabilitado. Los documentos que se direccionen a través de un destino con estado Inhabilitado no podrán realizar el proceso.   |
| De forma predeterminada   | Identifica el destino predeterminada.  |

5. Pulse el botón **Guardar**.

## Ver, seleccionar o editar los destinos predeterminados

1. Pulse **Administración de cuentas > Perfiles > Destinos**. El sistema mostrará la pantalla Lista de destinos.
2. Pulse **Ver destinos predeterminadas** en la esquina superior derecha de la pantalla. El sistema mostrará la pantalla Lista de destinos predeterminados.
3. Utilice las listas desplegables para seleccionar o cambiar una o más destinos predeterminados.
4. Pulse el botón **Guardar**.

## Visualización del destino de Donde se utiliza

Para ver los detalles de dónde se emplea un destino determinado, utilice el siguiente procedimiento:

1. Pulse **Administración de cuentas > Perfiles > Destinos**
2. En la lista de destinos, pulse el icono **Donde se utiliza** del destino correspondiente. Se visualiza la lista de dónde se está utilizando el destino seleccionado.

**Nota:** Esta pantalla se proporciona con información de transferencia de páginas, ya que podrían haber muchos canales que utilicen el destino. Cada página soportará un máximo de 10 conexiones.

## Supresión de un destino

La función para suprimir un destino está disponible para todos los destinos excepto para el destino predeterminado. Para suprimir un destino, utilice el siguiente procedimiento:

1. Pulse **Administración de cuentas > Perfiles > Destinos**.
2. En la lista de destinos, pulse el icono **Suprimir** al lado del destino que desee suprimir.

**Nota:** El icono **Suprimir** no estará disponible para el destino predeterminado. Asimismo, la operación de supresión sólo está disponible si el destino seleccionado no se utiliza en las conexiones. En caso de que necesite información sobre la utilización del destino, consulte el apartado “Visualización del destino de Donde se utiliza” en la página 54.

3. Pulse **Aceptar** en la ventana de aviso para confirmar la supresión.

---

## Gestión de certificados

Esta sección proporciona los pasos para ver, editar y suprimir un certificado digital mediante la Consola de comunidad.

### Visualización y edición de detalles de certificados digitales

1. Pulse **Administración de cuentas > Perfiles > Certificados**. El sistema muestra una lista de los certificados digitales existentes.
2. Pulse el icono Ver detalles para ver detalles del certificado. El sistema mostrará la pantalla Detalles de certificado.
3. Pulse el icono Editar para editar el certificado.
4. Edite según sus necesidades.
5. Pulse el botón **Guardar**.

### Inhabilitación de un certificado digital

1. Pulse **Administración de cuentas > Perfiles > Certificados**. El sistema mostrará la pantalla Lista de certificados.
2. Pulse el icono Ver detalles para ver detalles del certificado. El sistema mostrará la pantalla Detalles de certificado.
3. Pulse el icono Editar para editar el certificado.
4. Pulse **Inhabilitado**.
5. Pulse el botón **Guardar**.

---

## Gestión de grupos

Puede ver, editar y suprimir grupos mediante la Consola de comunidad. Esta característica sólo está disponible para los usuarios del grupo de administradores de los socios internos/externos.

### Visualización de miembros de grupo y asignación de usuarios a grupos

1. Pulse **Administración de cuentas > Perfiles > Grupos**. El sistema mostrará la pantalla Lista de grupos.

*Tabla 6. Valores de la pantalla Lista de grupos*

| Valor         | Descripción                |
|---------------|----------------------------|
| Nombre        | Nombre del grupo.          |
| Descripción   | Descripción del grupo.     |
| Tipo de grupo | Tipo, por ejemplo Sistema. |

2. Pulse el icono Ver miembros para ver una lista de miembros de un grupo. Si este icono no aparece, no habrá miembros en el grupo. Pulse Miembros en el submenú.
3. Pulse el icono Editar para editar los usuarios de un grupo.

4. Pulse **Añadir a grupo** para asignar usuarios al grupo.
5. Pulse el icono Desactivar edición para guardar y salir.

## Visualización, edición o asignación de permisos de grupo

El permiso de grupo para los usuarios y grupos no lo puede establecer ni siquiera un usuario del grupo de administradores. Los permisos de otros grupos siempre serán inferiores o iguales a los permisos de administradores. Por ejemplo, si el administrador tiene permiso de sólo lectura a Dirección, el permiso de los otros grupos podrá ser "sin acceso" o "sólo lectura".

1. Pulse **Administración de cuentas > Perfiles > Grupos**. El sistema mostrará la pantalla Lista de grupos.
2. Pulse el icono Ver permisos para ver los permisos de un grupo. El sistema mostrará una lista de los permisos de grupo seleccionados.
3. Seleccione **Sin acceso, Sólo lectura** o **Lectura/Escritura** para cada característica.
4. Pulse el botón **Guardar**.

## Visualización o edición de detalles de grupo

1. Pulse **Administración de cuentas > Perfiles > Grupos**. El sistema mostrará la pantalla Lista de grupos.
2. Pulse el icono Ver detalles para ver los detalles del grupo (Nombre y descripción). El sistema mostrará la pantalla Detalles del grupo.
3. Pulse el icono Editar para editar los detalles del grupo (los grupos generados por el sistema no se pueden editar).
4. Edite según sus necesidades.
5. Pulse el botón **Guardar**.

**Restricciones:** El administrador y los grupos predeterminados son generados por el sistema y no se pueden editar ni suprimir. El Administrador de concentrador tiene un grupo adicional, Administración de concentrador.

## Supresión de un grupo

1. Pulse **Administración de cuentas > Perfiles > Grupos**. El sistema mostrará la pantalla Lista de grupos.
2. Pulse el icono Ver detalles para ver detalles del grupo. El sistema mostrará la pantalla Detalles de grupo.
3. Pulse el icono Editar para editar detalles del grupo.
4. Pulse el botón **Suprimir**. Confirme que desea suprimir.

**Aviso:** El administrador y los grupos predeterminados son generados por el sistema y no se pueden editar ni suprimir.

---

## Gestión de usuarios

Utilice esta característica para ver y editar perfiles de socio. Esta característica sólo está disponible para los usuarios del grupo de administradores de los socios internos/externos.

**Nota:** Puede utilizar esta característica para asignar o generar automáticamente una nueva contraseña para un usuario.

1. Pulse **Administración de cuentas > Perfiles > Usuarios**. El sistema mostrará la pantalla Lista de usuarios.

La siguiente tabla describe los valores de la pantalla Lista de usuarios.

*Tabla 7. Valores de la pantalla Lista de usuarios*

| Valor                      | Descripción   |
|----------------------------|---|
| Nombre de usuario          | Nombre de inicio de sesión de la consola.   |
| Nombre completo            | Nombre completo del usuario.  |
| Correo electrónico         | Dirección de correo electrónico utilizada para notificaciones de alertas.   |
| Subscrito                  | Si esta opción está activada, se asignarán una o más alertas al usuario. Si se elimina al usuario del sistema, se eliminarán igualmente todas las suscripciones de alerta para dicho usuario. |
| Estado de inicio de sesión | El estado habilitado permite al usuario iniciar la sesión en la consola.  |

2. Pulse el icono Ver detalles para ver los detalles de un usuario.
3. Pulse el icono Editar para editar los detalles de un usuario.
4. Edite la información según proceda. La siguiente tabla describe los valores de la pantalla Detalles de usuario.

*Tabla 8. Detalles de usuario*

| Valor                    | Descripción  |
|--------------------------|--|
| Nombre de usuario        | Nombre de inicio de sesión para el usuario de la consola.  |
| Habilitado               | Habilite o inhabilite acceso a la consola.   |
| Nombre de pila           | Nombre del usuario.  |
| Nombre de familia        | Apellido del usuario.  |
| Correo electrónico       | Dirección de correo electrónico utilizada para notificaciones de alertas.  |
| Teléfono                 | Número de teléfono del usuario.  |
| Número de fax            | Número de fax del usuario.   |
| Entorno local de idioma  | Seleccione el área geográfica del usuario. Se establecerá de forma predeterminada en el entorno local definido por el administrador de concentrador.             |
| Entorno local de formato | Seleccione el país del usuario. Se establecerá de forma predeterminada en el entorno local definido por el administrador de concentrador.                        |
| Huso horario             | Seleccione el huso horario del usuario. Se establecerá de forma predeterminada en el huso horario definido por el administrador de concentrador.                 |
| Estado de alerta         | Cuando esté habilitado, este usuario recibirá todas las alertas suscritas. Seleccione Inhabilitar para impedir que este usuario reciba todas las alertas.        |
| Subscrito                | Este valor lo rellena el sistema.  |
| Visibilidad              | Seleccione Local para tener al usuario visible sólo dentro de la organización. Seleccione Global para tener al usuario visible para la organización y el gestor. |

**Nota:** El entorno local y el huso horario predeterminados del sistema tras la instalación y el inicio es Inglés (Estados Unidos) y UTC. El sistema utiliza UTC para sus cálculos de huso horario. El valor predeterminado UTC no se puede cambiar en el nivel de sistema. No obstante, todos los usuarios pueden cambiar el huso horario que aparece dentro de la Consola de comunidad.

Una vez el usuario *Administrador de concentrador* inicia la sesión en el sistema por primera vez, detectará el entorno local del sistema y el huso horario (Inglés, UTC). Como el usuario Administrador de concentrador es el superusuario responsable de la configuración del sistema, el entorno local y el huso horario de la Consola de comunidad seleccionados por él se convertirán en los nuevos valores predeterminados de todos los usuarios de la Consola de comunidad. Los usuarios individuales también tienen la opción de cambiar su entorno local y su huso horario según sus necesidades.

5. Pulse el botón **Guardar**.

## Supresión de usuarios

Para suprimir usuarios, debe tener los permisos correspondientes. Mediante esta función, se pueden suprimir todos los usuarios excepto HUBADMIN.

Utilice esta característica para suprimir un usuario:

1. Pulse **Administración de cuentas > Perfiles > Usuarios**.
2. Pulse el icono **Suprimir** al lado del usuario que desee suprimir.
3. En la ventana de aviso, pulse **Aceptar** para confirmar la supresión. Si pulsa **Cancelar**, se anulará la supresión.

---

## Gestión de contactos

Utilice la característica Contactos para ver y editar información de contacto para el personal clave.

Dependiendo del tamaño de su organización, puede que desee enviar notificaciones a distintos contactos cuando se produzcan determinados tipos de suceso. Por ejemplo, cuando un documento no pueda validarse, debería notificárselo al personal de seguridad para que puedan evaluar el problema. Cuando las transmisiones del socio interno excedan los límites normales, debería notificárselo a su administrador de red para garantizar que el sistema está manejando el aumento de transmisiones eficazmente.

## Visualización o edición de detalles de contacto

1. Pulse **Administración de cuentas > Perfiles > Contactos**. El sistema mostrará una lista de contactos actuales.

La siguiente tabla identifica los valores que aparecen en la pantalla Contactos.

*Tabla 9. Valores de la pantalla Lista de contactos*

| Valor              | Descripción   |
|--------------------|---|
| Nombre completo    | Nombre completo de contacto.  |
| Tipo de contacto   | Describe el rol del contacto, por ejemplo, Jefe de B2B o Jefe de empresa.   |
| Correo electrónico | Dirección de correo electrónico utilizada para notificaciones de alertas.   |
| Visibilidad        | <ul style="list-style-type: none"> <li>Local: El contacto sólo está visible para la organización.</li> <li>Global: El contacto es visible para el administrador de concentrador y el socio interno. Ambas partes pueden suscribir el contacto a alertas.</li> </ul> |
| Subscrito          | Si esta opción está seleccionada, se asignarán una o más alertas a este contacto. Si el contacto se elimina del sistema, todas las suscripciones de alerta para este contacto se eliminarán del sistema.  |
| Estado de alerta   | Cuando el Estado de alerta está habilitado, este contacto recibirá todas las alertas suscritas.   |

2. Pulse el icono Ver detalles para ver detalles de contacto. El sistema mostrará la pantalla Detalles de contacto.
3. Pulse el icono Editar para editar detalles de contacto.
4. Edite la información según proceda. La siguiente tabla describe valores de contacto.

*Tabla 10. Detalles de contacto*

| Valor              | Descripción   |
|--------------------|---|
| Nombre de pila     | Nombre del contacto.  |
| Nombre de familia  | Apellido del contacto.  |
| Dirección          | Dirección del contacto. Incluye la calle, la ciudad, el estado y el código postal.  |
| Tipo de contacto   | Describe el rol del contacto, por ejemplo, Jefe de B2B o Jefe de empresa.   |
| Correo electrónico | Dirección de correo electrónico del contacto para notificaciones de alertas.  |
| Teléfono           | Número de teléfono del contacto.  |
| Número de fax      | Número de fax del contacto.   |
| Estado de alerta   | Cuando esta opción está habilitada, este contacto recibirá todas las alertas suscritas. Seleccione Inhabilitar para impedir que este contacto reciba todas las alertas.   |
| Subscrito          | Este valor lo rellena el sistema.   |
| Visibilidad        | <ul style="list-style-type: none"> <li>Local: El contacto sólo está visible para la organización.</li> <li>Global: El contacto es visible para el administrador de concentrador y el socio interno. Ambas partes pueden suscribir el contacto a alertas.</li> </ul> |

5. Pulse el botón **Guardar**.

## Eliminación de un contacto

1. Pulse **Administración de cuentas > Perfiles > Contactos**. El sistema mostrará una lista de contactos actuales.
2. Pulse el icono Suprimir para suprimir el contacto correspondiente.

---

## Gestión de alertas

Las alertas de WebSphere Partner Gateway se utilizan para notificar al personal clave sobre fluctuaciones poco corrientes en el volumen de transiciones recibidas, o cuando se producen errores en el proceso de los documentos de empresa.

Una opción complementaria del módulo Visor, Visor de sucesos, le ayuda a identificar mejor los errores y a resolver errores de procesos.

### Visualización o edición de contactos y detalles de alerta

El socio interno puede ver todas las alertas, independientemente de quién sea su propietario (el creador de la alerta).

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Seleccione los criterios de búsqueda en las listas desplegadas y especifique el nombre de alerta. También puede pulsar el botón **Buscar** sin seleccionar ningún criterio de búsqueda (el sistema mostrará todas las alertas).
3. Pulse el botón **Buscar**. El sistema mostrará la pantalla Resultados de la búsqueda de alertas.
4. Pulse el icono Ver detalles para ver los detalles de una alerta.
5. Pulse el icono Editar para editar detalles de la alerta.
6. Edite la información según proceda.
7. Pulse la pestaña **Notificar**.
8. Seleccione un socio (sólo socio interno o administrador de concentrador). El socio interno puede ver todas las alertas independientemente de su propietario.
9. Edite los contactos para esta alerta, si lo desea.
10. Pulse el botón **Guardar**.

### Búsqueda de alertas

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Seleccione los criterios de búsqueda en las listas desplegadas y especifique el nombre de alerta. También puede pulsar el botón **Buscar** sin seleccionar ningún criterio de búsqueda (el sistema mostrará todas las alertas).

*Tabla 11. Criterios de búsqueda de alertas para socios*

| Valor                 | Descripción   |
|-----------------------|---|
| Tipo de alerta        | Volumen, suceso o todos los tipos de alerta.  |
| Nombre de alerta      | Nombre de la alerta.  |
| Estado de alerta      | Alertas que están habilitadas, inhabilitadas o todas.   |
| Contactos suscritos   | Contactos con alertas asignadas. Las selecciones son Tiene suscriptores, Sin suscriptores o Todo. |
| Resultados por página | Controla la forma en que aparecen los resultados de la búsqueda.                                  |



Tabla 12. Los criterios de búsqueda de alertas para socios internos y administradores de concentrador

| Valor                 | Descripción   |
|-----------------------|---|
| Propietario de alerta | Creador de la alerta.   |
| Socio de alerta       | Socio al que se aplica la alerta.   |
| Tipo de alerta        | Volumen, suceso o todos los tipos de alerta.  |
| Nombre de alerta      | Nombre de la alerta.  |
| Estado de alerta      | Alertas que están habilitadas, inhabilitadas o todas.   |
| Contactos suscritos   | Contactos con alertas asignadas. Las selecciones son Tiene suscriptores, Sin suscriptores o Todo. |
| Resultados por página | Controla la forma en que aparecen los resultados de la búsqueda.                                  |

3. Pulse el botón **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.

## Inhabilitación o habilitación de una alerta

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Seleccione los criterios de búsqueda en las listas desplegables y especifique el nombre de alerta.
3. Pulse el botón **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.
4. Localice la alerta y pulse el botón **Inhabilitado** o **Habilitado** bajo Estado. Sólo el administrador de concentrador y el propietario de la alerta (creador de la alerta) tiene permiso para editar el estado de la alerta.

## Eliminación de una alerta

1. Pulse **Administración de cuentas > Alertas**. El sistema mostrará la pantalla Búsqueda de alertas.
2. Seleccione los criterios de búsqueda en las listas desplegables y especifique el nombre de alerta.
3. Pulse el botón **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.
4. Localice la alerta y pulse el icono Suprimir para suprimirla. Sólo el administrador de concentrador y el propietario de la alerta (el creador de la alerta) puede eliminarla.

## Notificación de sucesos

WebSphere Partner Gateway permite configurar una Alerta de suceso para que cuando se produzca el suceso, tanto el Socio de origen como el Socio de destino del suceso reciban una notificación. Ahora hay dos opciones disponibles para la Notificación de alertas. Dichas opciones son las siguientes:

- Notificar a todas las partes relacionadas
- Notificar sólo a los contactos suscritos

Cuando se selecciona la opción Notificar a todas las partes relacionadas, la alerta notifica el suceso a los contactos del Socio de origen y a los contactos del Socio de destino automáticamente, así como a los contactos del Propietario de las alertas. El usuario no necesita especificar los "Contactos suscritos" (y no tiene permiso para

ello) cuando esta modalidad está seleccionada. Cuando la modalidad Notificar sólo a los contactos suscritos está seleccionado, la alerta sólo se envía a los contactos suscritos.

Después de determinar las partes a las que se tiene que enviar una notificación, puede elegir si hará lo siguiente:

- Enviar alertas inmediatamente
- Agrupar por lotes las alertas (por horas o cuentas)

**Nota:** El servidor de mensajes de correo electrónico de alerta se debe configurar para utilizar esta funcionalidad adicional. Consulte la *Guía del administrador del sistema* para obtener instrucciones sobre cómo configurar este servidor.

---

## Gestión de direcciones

Utilice esta característica para gestionar las direcciones de su perfil de socio.

### Edición de una dirección

1. Pulse **Administración de cuentas > Perfiles > Direcciones**. El sistema mostrará la pantalla Direcciones.
2. Localice la dirección que desea editar y pulse el icono Editar.
3. Realice los cambios necesarios. La siguiente tabla describe los valores de dirección.

*Tabla 13. Valores de dirección*

| Valor             | Descripción  |
|-------------------|--|
| Tipo de dirección | Corporativa, Facturación y Técnica                               |
| Dirección         | Dirección, que incluye la calle, ciudad, estado y código postal. |

4. Pulse el botón **Guardar**.

### Supresión de una dirección

1. Pulse **Administración de cuentas > Perfiles > Direcciones**. El sistema mostrará la pantalla Direcciones.
2. Localice la dirección que desea suprimir y pulse el icono Suprimir.
3. Verifique que desea suprimir la dirección.

---

## Capítulo 5. Visualización de sucesos y documentos: Visores

Los Visores le ofrecen una visión global del buen funcionamiento del sistema. También son herramientas para la resolución de problemas relacionados con sucesos.

El módulo Visores incluye las siguientes características:

- “Visor de sucesos”
- “Visor AS” en la página 66
- “Visor ebMS” en la página 68
- “Visor de RosettaNet” en la página 70
- “Visor de documentos” en la página 72
- “Cola de destino” en la página 77

Los visores RosettaNet y AS incluyen criterios de búsqueda adicionales para el administrador de concentrador. Para obtener más información, consulte la *Guía del administrador*.

**Nota:** El término socios se utiliza en las pantallas del visor para identificar a un miembro de la comunidad de concentrador, incluido el socio interno.

---

### Visor de sucesos

El Visor de sucesos le permite buscar sucesos por hora, fecha, tipo de suceso, nombre de suceso y ubicación de suceso. La administración de concentrador también puede buscar por socio, IP de origen e ID de suceso.

Los datos que genera el Visor de sucesos identifican, entre otras cosas, el Nombre del suceso, la indicación de fecha y hora, el IP de origen y le permiten ver los detalles de sucesos y documentos para diagnosticar el problema. También puede ver el documento sin formato, que identifica el campo, el valor y el motivo del error.

Un suceso le hace saber que se ha producido algo inusual en el sistema. Un suceso puede permitirle saber que una operación o función del sistema es correcta (por ejemplo, un socio se ha añadido satisfactoriamente al sistema o que una conexión se ha creado satisfactoriamente entre el socio interno y el socio externo). Un suceso también puede identificar un problema (por ejemplo, que el sistema no haya podido procesar un documento o que el sistema haya detectado un error no crítico en un documento). La mayoría de los tipos de documento se reenvían varias veces, por lo tanto si un documento falla y genera una alerta, es algo que debería investigar y corregir para evitar anomalías similares en el futuro.

WebSphere Partner Gateway incluye sucesos predefinidos. Utilice la característica Alertas y el módulo Administrador de cuentas del producto para crear alertas basadas en sucesos. Este proceso identifica los sucesos que le afectan. A continuación, utilice la característica Contactos, también en el módulo Administrador de cuentas, para identificar a los miembros del personal a los que el sistema enviará notificaciones si se producen estos sucesos.

El Visor de sucesos muestra sucesos según criterios de búsqueda específicos. Puede localizar un suceso específico y, a continuación, buscar por qué ha ocurrido. El Visor de sucesos le permite buscar sucesos por hora, fecha, tipo de suceso (depuración, información, aviso, error y crítico), Nombre de suceso (por ejemplo, 210031), así como por ubicación de suceso.

Los datos disponibles a través del Visor de sucesos incluye el nombre del suceso, la indicación de fecha y hora, el usuario y la información del socio. Estos datos le ayudan a identificar el documento o proceso que creó el suceso. Si el suceso está relacionado con un documento, también puede ver el documento sin formato, que identifica el campo, el valor y el motivo del error.

## Tipos de suceso

WebSphere Partner Gateway incluye los siguientes tipos de suceso.

Tabla 14. Tipos de suceso

| Tipo de suceso | Descripción   |
|----------------|---|
| Depuración     | Los sucesos Depuración se utilizan en operaciones y soportes de bajo nivel del sistema. Su visibilidad y uso están sujetos al nivel de permiso del usuario. No todos los usuarios tienen acceso a los sucesos Depuración.   |
| Información    | Los sucesos de información se generan cuando una operación del sistema finaliza satisfactoriamente. Estos sucesos también se utilizan para proporcionar el estado de los documentos actualmente en proceso. Los sucesos de información no requieren acción por parte del usuario. |
| Aviso          | Los sucesos Aviso se producen debido a anomalías no críticas en el proceso del documento o las funciones del sistema que permiten que la operación continúe.  |
| Error          | Los sucesos Error se producen debido a anomalías en el proceso del documento que hacen que el proceso finalice.   |
| Crítico        | Los sucesos Críticos se generan cuando los servicios finalizan debido a una anomalía del sistema. Los sucesos Críticos requieren intervención por parte del personal de soporte.  |

## Realización de tareas del Visor de sucesos

Tabla 15. Tareas del Visor de sucesos

| ¿Qué desea hacer?                    | Consulte     |
|--------------------------------------|--------------|
| Búsqueda de sucesos.                 | la página 64 |
| Visualización de detalles de suceso. | la página 65 |

## Búsqueda de sucesos

### 1. Pulse **Visores > Visor de sucesos**.

Los sucesos están organizados por gravedad de izquierda a derecha en la pantalla Búsqueda del Visor de sucesos. Información, a la izquierda, es el tipo de suceso menos grave; Crítico, a la derecha, es el más grave. (Los sucesos Depuración no los pueden ver todos los usuarios). Para cualquier suceso seleccionado, dicho suceso y todos los sucesos de mayor gravedad aparecerán en el Visor de sucesos. Por ejemplo, si el tipo de suceso Aviso se selecciona en los criterios de búsqueda, aparecerán los sucesos Aviso, Error y Crítico. Si selecciona los sucesos Información, aparecerán todos los tipos de suceso.

2. Seleccione los criterios de búsqueda en las listas desplegables.

Tabla 16. Criterios de búsqueda de sucesos

| Valor                                | Descripción  |
|--------------------------------------|--|
| Fecha y hora de inicio               | Fecha y hora en que se produjo el primer suceso. El valor predeterminado es 10 minutos antes.  |
| Fecha y hora de finalización         | Fecha y hora en la que se produjo el último suceso.  |
| Socios                               | Seleccione todos los socios o un socio específico (sólo el socio interno).   |
| Tipo de suceso                       | Tipo de suceso: Depuración, Información, Aviso, Error o Crítico.   |
| Nombre de suceso                     | Búsqueda de nombres de suceso disponibles según el tipo de suceso seleccionado.  |
| Ubicación de sucesos                 | Ubicación en la que se generó el suceso: todos, desconocido, origen (desde), destino (hacia).  |
| Ordenar por Ascendente o Descendente | Valor utilizado para ordenar los resultados. Ordenar en orden ascendente o descendente.  |
| Resultados por página                | Número de registros mostrados por página.  |
| Renovar                              | El valor predeterminado es Desactivado. Cuando Renovar está activado, el Visor de sucesos realiza primero una nueva consulta y, a continuación, permanece en la modalidad Renovar. |
| Cadencia de renovación               | Controla la frecuencia de renovación de los resultados de la búsqueda (sólo el socio interno).   |

3. Pulse el botón **Buscar**. El sistema muestra una lista de sucesos.

**Consejo:** La lista de sucesos se puede volver a filtrar según el tipo de suceso seleccionado en la parte superior de la pantalla Visor de sucesos. La siguiente pantalla, Renovar, refleja el nuevo tipo de suceso seleccionado.

## Visualización de detalles de suceso

1. Pulse **Visores > Visor de sucesos**.
2. Seleccione los criterios de búsqueda en las listas desplegables.
3. Pulse el botón **Buscar**. El sistema muestra una lista de sucesos.
4. Pulse el icono Ver detalles al lado del suceso que desea visualizar. El sistema mostrará los detalles del suceso y los documentos asociados.
5. Pulse el icono Ver detalles al lado del documento que desea visualizar, si existe uno.
6. Pulse el icono de Mostrar documento sin formato para ver el documento sin formato, si lo hay.
7. Pulse el icono Ver errores de validación para ver los errores de validación.

Cuando aparece el mensaje de error No se ha encontrado ningún certificado de cifrado válido, ni el certificado primario ni el secundario son válidos. Puede que los certificados hayan caducado o se hayan revocado. Si los certificados han caducado o se han revocado, aparecerá el suceso correspondiente (Certificado caducado o revocado) en el Visor de sucesos.

**Consejo:** Si aparece un suceso de documento duplicado en Detalles del visor de sucesos, vea el documento original previamente enviado pulsando el icono Ver documento original en Detalles de documento.

---

## Visor AS

Utilice el Visor AS para buscar y ver información sobre transporte correspondiente a documentos que utilizan los protocolos de comunicación AS1, AS2 o AS3. Podrá ver ID de mensaje, URI de destino y estado de notificaciones de disposición de mensajes (Message Disposition Notification, MDN), y detalles de documentos (el documento y la envoltura).

El Visor AS también se puede utilizar para ver detalles de transacciones B2B y procesos B2B que utilicen el protocolo de comunicación AS1, AS2 o AS3 (Applicability Statement 1 o 2). Puede ver la coreografía del proceso B2B y de los documentos de empresa a él asociados, las señales de reconocimiento, el estado de proceso, las cabeceras HTTP y el contenido de los documentos transmitidos.

Como su predecesor AS1, que define un estándar para transmisiones de datos mediante SMTP, AS2 define un estándar para transmisiones de datos mediante HTTP.

AS2 identifica cómo conectar, entregar, validar y responder a datos; no está relacionado con el contenido del documento, sólo con el transporte. AS2 crea una envoltura sobre un documento para que se pueda transportar a través de Internet mediante HTTP o HTTPS. El documento y la envoltura se denominan en su conjunto mensaje. AS2 proporciona seguridad y cifrado a los paquetes HTTP. AS2 ofrece una base de cifrado con entrega garantizada. AS3 proporciona un estándar nuevo para transmitir documentos por FTP o FTPS de forma segura.

Un componente importante de AS2 es su mecanismo de recibo, que se denomina MDN (Message Disposition Notification, notificación de disposición de mensaje). Este componente garantiza al remitente del documento que el receptor ha recibido correctamente el documento. El remitente especifica cómo se debe devolver la MDN (síncrona o asíncronamente; firmada o sin firmar).

Puede utilizar el Visor AS para ver el ID del mensaje, las Indicaciones de fecha y hora, el Tipo de documento, el Tipo de destino, el estado Síncrono, así como los detalles del documento. Cuando se ven los detalles del documento se muestra información adicional sobre el proceso del documento.

## Realización de tareas del Visor AS

*Tabla 17. Tareas del Visor AS1/AS2*

| <b>¿Qué desea hacer?</b>                | <b>Consulte</b>  |
|---|--|
| Búsqueda de mensajes AS                 | la página "Búsqueda de mensajes"                                 |
| Visualización de documentos sin formato | la página "Visualización de detalles de mensaje" en la página 67 |

## Búsqueda de mensajes

1. Pulse **Visores > Visor AS**. El sistema mostrará la pantalla Visor AS.

2. Seleccione los criterios de búsqueda en las listas desplegables.

Tabla 18. Criterios de búsqueda del Visor AS

| Valor                               | Descripción  |
|-------------------------------------|--|
| Fecha y hora de inicio              | Fecha y hora en las que se inició el proceso.  |
| Fecha y hora de finalización        | Fecha y hora en las que finalizó el proceso.   |
| Socio de origen                     | Identifica al socio que realiza la transmisión (sólo socio interno).   |
| Socio de destino                    | Identifica al socio receptor   |
| Buscar en                           | Especifica si el documento que se va a buscar es un documento de origen o de destino.  |
| ID empresarial de origen de AS      | Número de identificación empresarial del socio de origen, por ejemplo, Duns.   |
| ID empresarial de origen de Payload | Número de identificación de origen de Payload.   |
| Modalidad de funcionamiento         | Producción, Prueba, Socio externo de simulador o Socio interno de simulador RN. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba.   |
| Paquete                             | Describe el formato, el empaquetado, el cifrado y la identificación content-type del documento.  |
| Protocolo                           | Formato de documento disponible para los socios, por ejemplo, RosettaNet de XML.   |
| Tipo de documento                   | El proceso empresarial específico.   |
| ID de mensaje                       | Número de ID asignado al documento empaquetado de AS1, AS2 o AS3. Los criterios de búsqueda pueden incluir el comodín asterisco (*). Longitud máxima, 255 caracteres.  |
| ID de documento Sinc./Asínc.        | Número de identificación exclusivo asignado al documento. Búsqueda de documentos recibidos en modalidad síncrona o asíncrona. La modalidad síncrona significa que la conexión entre el iniciador y el Gestor de documentos permanece abierta hasta que la transacción se haya completado, incluidas la solicitud y la notificación de disposición del mensaje (Message Disposition Notification, MDN). |
| Estado de la MDN                    | Este campo permite seleccionar el estado de la MDN en este mensaje.  |
| Ordenar por                         | Ordenar resultados según este valor.   |
| Descendiente o Ascendente           | Ascendente - Muestra primero la indicación de la hora más antigua o el final del alfabeto.<br><br>Descendiente - Muestra la indicación de la hora más reciente o el principio del alfabeto.  |
| Resultados por página               | Utilice esta opción para seleccionar el número de registros mostrados por página.  |

3. Pulse el botón **Buscar**. El sistema muestra una lista de mensajes.

## Visualización de detalles de mensaje

1. Pulse **Visores > Visor AS**. El sistema mostrará la pantalla Visor AS.
2. Seleccione los criterios de búsqueda en las listas desplegables.
3. Pulse el botón **Buscar**. El sistema muestra una lista de mensajes.
4. Pulse el icono Ver detalles al lado del mensaje que desea visualizar. El sistema mostrará el mensaje y los detalles de documentos asociados.

Tabla 19. Visor AS: Detalles del paquete

| Valor                           | Descripción  |
|---------------------------------|--|
| ID de mensaje                   | Número de ID asignado al documento empaquetado de AS1, AS2 o AS3. Este número identifica sólo al paquete. El documento tiene un número de ID de documento independiente que aparece al visualizar los detalles del documento. Longitud máxima, 255 caracteres.   |
| Socio de origen                 | Socio que inicia un proceso empresarial.   |
| Socio de destino                | Socio que recibe el proceso empresarial.   |
| Indicación de la hora de inicio | Fecha y hora en la que el documento inicia su proceso.   |
| Tipo de destino                 | Prueba o producción. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba.  |
| URI de MDN                      | Dirección de destino de la MDN. La dirección se puede especificar como URI HTTP o como dirección de correo electrónico.  |
| Texto de disposición de MDN     | Este texto proporciona el estado del mensaje original que se ha recibido (puede ser correcto o erróneo). Estos son algunos ejemplos: <ul style="list-style-type: none"> <li>• Automatic=action/MDN-sent-automatically; processed.</li> <li>• Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document.</li> <li>• Automatic-action/MDN-sent-automatically;processed/Error;description-failed.</li> <li>• Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.</li> </ul> |

5. (Opcional) Pulse el icono Mostrar documento sin formato para ver el documento sin formato.

## Visor ebMS

El mecanismo ebXML Message Service (ebMS) proporciona una forma estándar de intercambiar mensajes empresariales entre los socios comerciales de ebXML. Proporciona un medio fiable de intercambio de mensajes empresariales sin tener que depender de las soluciones y tecnologías de terceros. Un mensaje ebXML contiene estructuras para la cabecera de un mensaje (necesaria para su direccionamiento y entrega) y para una sección de carga. ebMS proporciona una forma estándar de intercambiar mensajes empresariales entre socios comerciales de ebXML. Un mensaje de ebXML es un sobre de mensaje MIME/Multipart independiente del protocolo de comunicaciones.

## Realización de tareas del visor ebMS

Tabla 20. Tareas del visor ebMS

| ¿Qué desea hacer?           | Consulte  |
|-----------------------------|---|
| Buscar procesos de ebMS     | “Búsqueda de procesos de ebMS” en la página 69                      |
| Ver procesos de ebMS        | “Visualización de los detalles del proceso de ebMS” en la página 69 |
| Ver documentos sin formato  | “Visualización de documentos sin formato” en la página 70           |
| Ver el estado del documento | “Visualización del estado del documento” en la página 70            |



## Búsqueda de procesos de ebMS

1. Haga clic en **Visores > Visor de ebMS**. El sistema visualiza la pantalla Búsqueda del visor de ebMS.
2. Seleccione los criterios de búsqueda en las listas desplegables.

| Valor                        | Descripción  |
|------------------------------|--|
| Fecha y hora de inicio       | La fecha y la hora en las que se inició el proceso.  |
| Fecha y hora de finalización | La fecha y la hora en las que finalizó el proceso.   |
| Socio de origen              | Identifica al socio emisor.  |
| Socio de destino             | Identifica al socio receptor.  |
| ID empresarial de origen     | Número de identificación empresarial de un socio iniciador, por ejemplo, DUNS.   |
| Modalidad de funcionamiento  | Producción, prueba, socio externo de simulador o socio interno de simulador RN. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba.                   |
| Protocolo                    | Protocolos disponibles para los socios.  |
| Tipo de documento            | Tipo de documento que se va a procesar.  |
| ID de conversación           | Información exclusiva de identificación asignada al proceso. Los criterios pueden incluir el comodín asterisco (*).  |
| Ordenar por                  | Ordenar resultados, por ejemplo, según la indicación de la hora de recepción.  |
| Descendente o Ascendente     | Ascendente - Muestra primero la indicación de la hora más antigua o el final del alfabeto.<br><br>Descendente - Muestra la indicación de la hora más reciente o el principio del alfabeto. |
| Resultados por página        | Muestra un número n de resultados por página.  |

3. Pulse el botón **Buscar**. El sistema muestra los procesos de ebMS que coinciden con su criterio de búsqueda.

## Visualización de los detalles del proceso de ebMS

1. Pulse en **Visores > Visor de ebMS**. El sistema visualiza la pantalla Visor de ebMS.
2. Seleccione los criterios de búsqueda en las listas desplegables.
3. Pulse el botón **Buscar**. El sistema muestra los resultados de la búsqueda.

Tabla 21. Valores de criterio de búsqueda del visor de ebMS

| Valor                                | Descripción   |
|--------------------------------------|---|
| Socios                               | Socios que participan en el proceso empresarial.                                    |
| Indicación de fecha y hora de inicio | Fecha y hora en la que se empezó a procesar el primer documento.                    |
| Tipo de documento                    | El proceso empresarial específico, por ejemplo: ebMS 2.0 : Producción de ALMSERVICE |
| Modalidad de funcionamiento          | Modalidad de funcionamiento, por ejemplo: Producción                                |
| ID de conversación                   | Número de identificación exclusivo asignado a este suceso                           |

## Visualización de documentos sin formato

Para ver el documento sin formato:

1. Pulse en **Visores > Visor de ebMS**.
  2. Seleccione el criterio de búsqueda de las listas desplegadas; consulte el apartado “Búsqueda de procesos de ebMS” en la página 69.
  3. Pulse el botón **Buscar**.
  4. Pulse el icono “**Pulsar para ver el documento sin formato**” que hay debajo de la sección **Descripción**.
- Para resolver problemas de documentos que no hayan podido realizar el proceso, consulte el apartado “Visualización de errores de validación de datos” en la página 76.
  - El visor de documentos sin formato muestra la cabecera HTTP con el documento sin formato.

## Visualización del estado del documento

1. Pulse en **Visores > Visor de ebMS**.
2. Seleccione el criterio de búsqueda de las listas desplegadas; consulte el apartado “Búsqueda de procesos de ebMS” en la página 69.
3. Pulse el botón **Buscar**.
4. Pulse **Solicitar estado**.
5. Pulse **Visualizar estado**.

---

## Visor de RosettaNet

Utilice el Visor de RosettaNet para localizar un proceso específico que haya generado un suceso. Cuando identifique el proceso de destino, podrá ver los detalles del proceso y el documento sin formato.

RosettaNet es un grupo de empresas que creó un estándar de la industria para transacciones de e-business. Los procesos de interfaz de socio (Partner Interface Processes ,PIP) definen procesos empresariales entre los miembros de la comunidad de concentrador. Cada PIP identifica un documento empresarial específico y la forma en que se procesa entre el socio interno y los socios externos.

El Visor de RosettaNet muestra la coreografía de los documentos que forman un proceso empresarial. Los valores visibles utilizando el Visor de RosettaNet son el estado de proceso, los detalles, los documentos sin formato y los sucesos de proceso asociados.

El Visor de RosettaNet muestra los procesos según los criterios específicos de búsqueda.

## Realización de tareas del Visor de RosettaNet

*Tabla 22. Tareas del Visor de RosettaNet*

| <b>¿Qué desea hacer?</b>                             | <b>Consulte</b> |
|--|-----------------|
| Búsqueda de procesos de RosettaNet.                  | la página 71    |
| Visualización de detalles de procesos de RosettaNet. | la página 71    |
| Visualización de documentos sin formato.             | la página 72    |

## Búsqueda de procesos de RosettaNet

1. Pulse **Visores > Visor de RosettaNet**. El sistema muestra la pantalla Búsqueda de Visor de RosettaNet.
2. Seleccione los criterios de búsqueda en las listas desplegables. EMPEZAR AQUÍ

Tabla 23. Criterios de búsqueda de RosettaNet

| Valor                        | Descripción  |
|------------------------------|--|
| Fecha y hora de inicio       | La fecha y la hora en las que se inició el proceso.  |
| Fecha y hora de finalización | La fecha y la hora en las que finalizó el proceso.   |
| Socio de origen              | Identifica al socio emisor.  |
| Socio de destino             | Identifica al socio receptor.  |
| ID empresarial de origen     | Número de identificación empresarial de un socio iniciador, por ejemplo, DUNS.   |
| Modalidad de funcionamiento  | Producción, prueba, socio externo de simulador o socio interno de simulador RN. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba.               |
| Protocolo                    | Protocolos disponibles para los socios.  |
| Tipo de documento            | Tipo de documento que se va a procesar.  |
| ID de instancia de proceso   | Número de identificación exclusivo asignado para el proceso. Los criterios pueden incluir el comodín asterisco (*).  |
| Ordenar por                  | Ordenar resultados, por ejemplo, según la indicación de la hora de recepción.  |
| Descendente o Ascendente     | Ascendente - Muestra primero la indicación de la hora más antigua o el final del alfabeto.<br>Descendente - Muestra la indicación de la hora más reciente o el principio del alfabeto. |
| Resultados por página        | Muestra un número n de resultados por página.  |

3. Pulse el botón **Buscar**. El sistema muestra los procesos de RosettaNet que coinciden con los criterios de búsqueda.
4. Pulse el icono Ver detalles al lado del proceso de ebMS que desea visualizar. El sistema muestra detalles y documentos asociados del proceso seleccionado.
5. Pulse el icono Ver detalles al lado del documento que desea visualizar. El sistema muestra el documento y los detalles de suceso asociados.

## Visualización de procesos de RosettaNet

1. Pulse **Visores > Visor de RosettaNet**. El sistema muestra la pantalla Búsqueda de Visor de RosettaNet.
2. Seleccione los criterios de búsqueda en las listas desplegables.

3. Pulse el botón **Buscar**. El sistema muestra los resultados de la búsqueda.

Tabla 24. Detalles de proceso de documentos

| Valor                      | Descripción  |
|----------------------------|--|
| Socios                     | Socios que participan en el proceso empresarial.   |
| Indicaciones de la hora    | Fecha y hora en la que se empezó a procesar el primer documento.   |
| Tipo de documento          | El proceso empresarial específico, por ejemplo, RosettaNet (1.1): 3A7.   |
| Tipo de destino            | Por ejemplo, Producción.   |
| ID de instancia de proceso | Número exclusivo asignado al proceso por el miembro de comunidad que lo inicie.  |
| ID de documento            | Identificador de documento de propiedad asignado por el socio emisor. El campo no está en una ubicación fija y varía según el tipo de documento. |
| Socio de origen            | Socio iniciador.   |
| Socio de destino           | Socio receptor.  |

4. Pulse el icono Ver detalles al lado del proceso de RosettaNet que desea visualizar. El sistema muestra detalles y documentos asociados del proceso seleccionado.
5. Pulse el icono Ver detalles al lado del documento que desea visualizar. El sistema muestra el documento y los detalles de suceso asociados.

## Visualización de documentos sin formato

1. Pulse **Visores > Visor de RosettaNet**. El sistema muestra la pantalla Búsqueda de Visor de RosettaNet.
2. Seleccione los criterios de búsqueda en las listas desplegables.
3. Pulse el botón **Buscar**. El sistema mostrará una lista de procesos.
4. Pulse el icono Ver detalles al lado del proceso que desea visualizar. El sistema mostrará los detalles de proceso y los documentos asociados al proceso seleccionado.
5. Pulse el icono Mostrar documento sin formato que hay junto a Tipo de documento para visualizar el documento sin formato.

**Restricciones:** Los documentos sin formato superiores a 100 K se truncan.

### Consejo:

- Para resolver problemas de documentos que no hayan podido realizar el proceso, consulte el apartado “Visualización de errores de validación de datos” en la página 76.
- El visor de documentos sin formato muestra la cabecera HTTP con el documento sin formato.

---

## Visor de documentos

El Visor de documentos se utiliza para localizar y ver un documento específico que desee investigar. Puede buscar documentos basados en la fecha, hora, tipo de proceso, (Proceso de origen o Proceso de destino), conexión del socio, tipo de destino, estado del documento, protocolo, tipo de documento y versión del proceso.

Algunos protocolos, como el protocolo personalizado de lenguaje de marcación extensible (Extensible Markup Language ,XML) que utiliza formatos XML, pueden

extraer información de los documentos y guardarla para poderla buscar mediante el Visor de documentos. Ése es el propósito de los atributos del campo de búsqueda del usuario en una definición de formato XML. En el caso de un documento direccionado mediante el uso de un formato XML que incluye campos de búsqueda, la información del documento obtenida gracias a los campos de búsqueda puede ser el objetivo de una búsqueda. Un documento XML personalizado que sea un pedido de compra es un ejemplo. Si utiliza sus conocimientos sobre la estructura de los documentos, puede definir un formato XML con un archivo de búsqueda que extraiga el número del pedido de compra. Cuando los documentos se direccionen utilizando este formato XML, podrá buscarlos mediante el número de la orden de compra, introduciendo dicho número en la búsqueda apropiada definida por el usuario archivada en la pantalla de búsqueda del Visor de documentos.

El direccionamiento de documentos de intercambio electrónico de datos (Electronic Data Interchange, EDI) que extrae información del documento también se puede definir. Esto se realiza codificando una correlación DIS, de manera que complete los valores de los campos de búsqueda definidos por el usuario.

También puede grabar una salida de usuario que extraiga información del documento para que pueda ser el objetivo de una búsqueda. Utilice el método de salida de usuario `BusinessDocumentInterface.setAttribute()` para completar los valores de los campos de búsqueda definidos por el usuario.

Los resultados de la búsqueda muestran todos los documentos que cumplen los criterios de la búsqueda e identifican las indicaciones de fecha y hora, procesos, conexiones de socio y tipos de destino. Localice el documento de destino y utilice las características del visor para ver el documento sin formato. También puede utilizar el Visor de documentos para volver a enviar los documentos erróneos o correctos.

## Búsqueda de documentos

1. Pulse **Visores > Visor de documentos**. El sistema mostrará la pantalla Búsqueda del Visor de documentos.

2. Seleccione los criterios de búsqueda en las listas desplegables.

*Tabla 25. Criterios de búsqueda del Visor de documentos*

| Valor                                       | Descripción  |
|---|--|
| Fecha y hora de inicio                      | Fecha y hora en las que se inició el proceso.  |
| Fecha y hora de finalización                | Fecha y hora en las que finalizó el proceso.   |
| Socio de origen                             | Identifica al socio emisor.  |
| Socio de destino                            | Identifica al socio receptor .   |
| Buscar en                                   | Buscar en el tipo de documento de origen o de destino.   |
| Modalidad de funcionamiento                 | Producción, prueba, socio externo de simulador o socio interno de simulador RN. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba.   |
| Estado de documento                         | Estado actual del documento en el sistema. Puede seleccionar En progreso, Satisfactorio o Error. El valor predeterminado es Todos.   |
| Paquete                                     | Describe el formato, el empaquetado, el cifrado y la identificación content-type del documento   |
| Protocolo                                   | Tipo de protocolo de proceso disponible para los socios.   |
| Tipo de documento                           | El proceso empresarial específico.   |
| ID de documento                             | Creado por el socio de origen. Los criterios pueden incluir el comodín asterisco (*).  |
| ID de referencia                            | Número de ID creado por el sistema para realizar el seguimiento del estado de documento.   |
| Dirección IP de origen                      | Dirección IP del socio de origen.  |
| Filtro                                      | Búsqueda de documentos recibidos en la modalidad síncrona. Esto significa que la conexión entre el iniciador y el Gestor de documentos permanece abierta hasta que la transacción finaliza, incluidas la solicitud y el acuse de recibo o la solicitud y su respuesta. |
| Ordenar por                                 | Valor utilizado para ordenar los resultados.   |
| Resultados por página                       | Número de registros mostrados por página.  |
| Descendente                                 | Ordenar resultados en orden descendente o ascendente.  |
| Campos de búsqueda definidos por el usuario | Realice la búsqueda según unos criterios definidos por el usuario.   |

**Nota:** Los sucesos de aviso aparecen de forma predeterminada. Para ver todos los sucesos, seleccione Depuración.

3. Pulse el botón **Buscar**. El sistema muestra una lista de documentos que cumplen con los criterios de búsqueda.

*Tabla 26. Información de documento disponible al utilizar el Visor de documentos*

| Valor                   | Descripción  |
|-------------------------|--|
| Socios                  | Socios de origen (Desde) y de destino (Hacia) que participan en el proceso empresarial.  |
| Indicaciones de la hora | Fecha y hora en las que empieza y finaliza el proceso.   |
| Tipo de documento       | Proceso empresarial que se está llevando a cabo.   |
| Tipo de destino         | Prueba o producción. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba.  |
| Síncrono                | Identifica que el documento se recibió en la modalidad síncrona. Esto significa que la conexión entre el iniciador y el Gestor de documentos permanece abierta hasta que la transacción finaliza, incluidas la solicitud y el acuse de recibo o la solicitud y su respuesta. |

## Visualización de detalles de documento, sucesos y documentos sin formato

1. Pulse **Visores > Visor de documentos**. El sistema mostrará la pantalla Búsqueda del Visor de documentos.
2. Seleccione los criterios de búsqueda en las listas desplegables.
3. Pulse el botón **Buscar**. El sistema mostrará una lista de los documentos.
  - Para ver los detalles y los sucesos de un documento, pulse el icono de carpeta abierta situado al lado del documento que aparece en la cabecera Documentos asociados. El sistema mostrará los detalles y sucesos de proceso correspondientes al documento seleccionado. En los documentos de intercambio EDI, si aparecen hijos de transacciones EDI después del desensobrado o el ensobrado, se pueden mostrar seleccionando el botón de selección de origen o destino **Hijo de documento**. Consulte la *Guía del administrador* para obtener más información sobre la visualización de documentos EDI.
  - Para ver el documento sin formato con cabecera HTTP, pulse el icono Mostrar documento sin formato junto al documento. El sistema mostrará el contenido del documento sin formato.

La siguiente información de proceso de documento aparece al visualizar los detalles del documento:

*Tabla 27. Valores de proceso de documento disponibles a través del Visor de documentos*

| Valor   | Descripción   |
|---|---|
| ID de referencia                                | Número de identificación exclusivo asignado al documento por el sistema.  |
| ID de documento                                 | Número de identificación exclusivo asignado al documento por el socio de origen.  |
| Indicación de la hora del documento             | Fecha y hora en que el socio creó el documento.   |
| Destino   | Destino a través del cual pasa el documento.  |
| Tipo de documento de conexión                   | Acciones realizadas en un documento por el sistema para garantizar su compatibilidad con los requisitos empresariales entre socios. |
| Origen y destino                                | Socios de origen y destino que participan en procesos empresariales.  |
| Indicación de la hora de inicio                 | Fecha y hora en las que el sistema recibió el documento del socio.  |
| Indicación de la hora de estado de finalización | Fecha y hora en las que el sistema direccionó el documento al socio de destino.   |
| ID de empresa de origen y de destino            | Número de identificación empresarial de los Socios de origen y de destino, por ejemplo, Duns.                                       |
| Tipo de documento de origen y de destino        | El proceso empresarial específico que tiene lugar entre los socios de origen y de destino.  |

**Restricciones:** Los documentos sin formato superiores a 100 K se truncan.

**Consejo:** Si el sistema muestra un suceso Documento duplicado, visualice el documento original enviado anteriormente seleccionando el icono de la flecha azul situado junto al suceso Documento duplicado y, a continuación, pulse el icono Ver documento original.

**Consejo:** Para resolver problemas de documentos que no hayan podido realizar el proceso, consulte el apartado “Visualización de errores de validación de datos” en la página 76.

## Visualización de errores de validación de datos

Puede buscar rápidamente documentos que no se hayan podido procesar utilizando el texto codificado en color de los campos XML que contengan errores de validación. Los campos que contienen errores de validación aparecen en rojo. Si se producen hasta tres errores de validación independientes dentro de los campos XML anidados, se utilizarán los siguientes colores para distinguir los campos de error:

Tabla 28. Errores de validación de documentos codificados en color

| Valor   | Descripción                 |
|---------|-----------------------------|
| Rojo    | Primer error de validación  |
| Naranja | Segundo error de validación |
| Verde   | Tercer error de validación  |

A continuación se muestra un ejemplo de errores de validación de XML anidados:

El elemento de datos *ContactInformation* es el primer error de validación porque este código está en la posición errónea. La posición correcta es directamente después de *PartnerRoleDescription*.

El elemento de datos *FreeFormText* es el segundo error de validación porque este código está duplicado.

El elemento de datos *John* es el tercer error de validación porque este campo requiere seis caracteres como mínimo.

```

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE Pip3 A7PurchaseOrderUpdateNotifion
SYSTEM "3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd">
<Pip3A7PurchaseOrderUpdateNotificafion>
  <fromRole>
    <PartnerRoleDescription>
      <GlobalPartnerRoleClassificationCode>Seller</GlobalPartnerRoleClassificationCode>
    <PartnerDescription>
      <ContactInformation>
        <ContactName>
          <FreeFormText>John</FreeFormText>
          <FreeFormText>John</FreeFormText>
        </contactName>
        <EmailAddress>John@example.com</EmailAddress>
        <telephoneNumber>
          <CommunicationsNumber>+1-234-567-8998-8</CommunicationsNumber>
        </telephoneNumber>
        <facsimileNumber>
          <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
        </facsimileNumber>
      </ContactInformation>
    <BusinessDescription>
      <GlobalBusinessIdentifier>123456789</GlobalBusinessIdentifier>
      <GlobalSupplyChainCode>InformationTechnology</GlobalSupplyChainCode>
    <BusinessDescription>
      <GlobalPartnerClassificationCode>Carrier</GlobalPartnerClassificationCode>
    </PartnerDescription>
  </PartnerRoleDescription>
  
```

Ejemplo de errores de validación de XML no anidados:



El elemento de datos *EmailAddress* es el primer error de validación no anidado porque este código está en la posición errónea. La posición correcta es directamente después de *ContactInformation*.

```

<billTo>
  <PartnerRoleDescription>
  <EmailAddress>frances@sample.com</EmailAddress>
  <ContactInformation>
    <contactName>
      <FreeFormText>String</FreeFormText>
    </contactName>
    <facsimileNumber>
      <CommunicationsNumber>String</CommunicationsNumber>
    </facsimileNumber>
    <telephoneNumber>
      <CommunicationsNumber>+888-999-0000</CommunicationsNumber>
    </telephoneNumber>
  </billTo>

```

El elemento de datos del número de teléfono es el segundo error de validación no anidado porque este campo requiere dos caracteres adicionales para el código de país.

Para ver errores de validación en un documento sin formato, consulte el apartado “Visualización de documentos sin formato” en la página 72.

**Restricciones:** La consola sólo muestra los primeros 100 KB de un documento sin formato. Los errores de validación por encima de los 100 KB no son visibles.

## Uso de la característica Detener proceso

Pulse **Detener proceso** para interrumpir un documento actualmente en progreso. Esta característica no está restringida al usuario hubadmin. Los permisos del grupo se deben configurar para aprovechar este recurso.

**Nota:** El sistema puede tardar hasta una hora en detener el documento. Durante este tiempo, el Visor de documentos seguirá mostrando el estado de documento En progreso.

## Cola de destino

La Cola de destino le permite ver documentos en cola pendientes de entrega desde cualquier destino del sistema. Asimismo, permite ver todos los destinos que tengan documentos en cola pendientes de entrega, visualizar y eliminar documentos en una cola, así como habilitar o inhabilitar destinos.

La cola de destino se puede utilizar para garantizar que los documentos de carácter urgente no se dejen en la cola. También se puede utilizar para asegurarse de que no se supere el número máximo de documentos que se pueden poner en cola. Mediante el uso de la cola de destino, puede:

- Ver una lista de todos los destinos que contengan documentos en cola pendientes de entrega
- Ver un documento que haya estado en una cola de destino durante un largo período de tiempo (30 segundos o más). Esto puede indicar un problema con el propio documento. También puede ver los detalles del documento para solucionar problemas con documentos de la cola.

**Nota:** Si implementa un destino de FTP Scripting con un intervalo o una planificación de calendario, los documentos pueden permanecer en esta cola durante un período hasta que se alcance dicho intervalo o fecha y hora. Este es un funcionamiento esperado, y los documentos no deben eliminarse de la cola.

- Ver los detalles de destino para garantizar un funcionamiento adecuado. La copia de seguridad de documentos en una cola puede significar que hay un error con el gestor de entrega o el destino.
- Conformar el estado del destino. Un destino fuera de línea provoca una recopilación de documentos en la cola hasta que el destino vuelva a estar en línea. El estado del destino no afecta a la funcionalidad de conexión, y los documentos se continúan procesando y colocándose en la cola para ser entregados.
- Limitar el tamaño de la lista de colas de destino mediante los campos **Nombre del socio** y **Destino**.

## Visualización de la lista de destinos

Para ver una lista de documentos residentes en el destino, utilice el siguiente procedimiento:

1. Seleccione **Visores > Cola de destino**. La consola mostrará la ventana Cola de destino.

2. Especifique los parámetros que se muestran en la Tabla 29.

Tabla 29. Ventana Cola de destino

| Criterio               | Descripción  |
|------------------------|--|
| Nombre de socio        | Para completar este campo, puede: <ol style="list-style-type: none"> <li>1. Especificar el nombre de socio.</li> <li>2. Especificar parte del nombre de socio en este campo y pulsar <b>Mostrar socios</b>. Seleccione el socio en la lista de socios.</li> <li>3. Especificar el comodín * y pulsar <b>Mostrar socios</b>. Seleccione el socio en la lista de socios.</li> </ol> <p>Al pulsar <b>Mostrar socios</b> se muestra un campo Socio en la página. El campo <b>Socio</b> lista todos los socios disponibles en orden alfabético.</p> |
| Destino                | El primer elemento de esta lista es Todo, que está seleccionado de forma predeterminada. El resto de la lista es una lista ordenada de transportes de destino. En esta lista, puede seleccionar un único destino. El valor predeterminado es Todo. <p><b>Nota:</b> La lista Destino se rellena automáticamente con los destinos del socio seleccionado, y la lista se presenta en orden alfabético.</p>  |
| En cola al menos       | Número mín. de minutos que un documento ha estado esperando en la cola de destino. Por ejemplo, si se seleccionan 6 minutos, todos los destinos que contengan documentos que hayan estado 6 minutos o más a la espera de ser entregados, se mostrarán. El valor predeterminado es 0.   |
| Ordenar por            | Ordena los resultados de búsqueda por Socio (valor predeterminado) o por Nombre de destino.  |
| Renovar                | Activa o desactiva (valor predeterminado) la renovación.   |
| Mínimo en cola         | Número mínimo de documentos en una cola de destino. El valor predeterminado es 1.  |
| Dirección              | Pulse <b>Ascendente</b> para mostrar los documentos empezando por la última indicación de la hora o el final del abecedario, o <b>Descendente</b> para mostrar los documentos empezando por la indicación de la hora más reciente o el principio del abecedario.   |
| Cadencia de renovación | Número de segundos que espera la consola antes de actualizar los datos visualizados.   |

3. Pulse el botón **Buscar**. El sistema encuentra todos los documentos en el destino que coinciden con los criterios de búsqueda. En la **Tabla 30** se muestra la información devuelta de la búsqueda.

Tabla 30. Resultados de la búsqueda de cola de destino

| Criterio     | Descripción  |
|--------------|--|
| Socio        | Socio comercial asociado al destino  |
| Destino      | Nombre del destino   |
| En cola      | Número de documentos en la cola de destino pendientes de entrega. Enlace a los detalles de destino |
| Estado       | Muestra si el destino está en línea o fuera de línea   |
| Último envío | Fecha y hora de la última vez que se envió un documento al destino satisfactoriamente              |

**Nota:** Para que la consola muestre un destino, éste debe cumplir todos los requisitos de los criterios de búsqueda utilizando la lógica AND.

## Visualización de documentos en cola

Para ver los documentos en cola para un socio determinado:

1. Pulse **Visores > Cola de destino**.
2. En la ventana Búsqueda de cola de destino, pulse **Búsqueda de documentos**.
3. En la ventana Búsqueda de documentos en cola, especifique los criterios de búsqueda (consulte la Tabla 31 en la página 80).

Tabla 31. Ventana Búsqueda de documentos en cola

| Criterio  | Descripción   |
|---|---|
| Nombre de socio   | Para completar este campo, puede: <ol style="list-style-type: none"><li>1. Especificar el nombre de socio en el campo.</li><li>2. Especificar parte del nombre de socio en este campo y pulsar <b>Mostrar socios</b>. Seleccione el socio en la lista.</li><li>3. Especificar el comodín * y pulsar <b>Mostrar socios</b>. Seleccione el socio en la lista de socios.</li></ol> <p><b>Nota:</b> Al pulsar <b>Mostrar socios</b> se muestra un campo Socio en la página. El campo <b>Socio</b> lista todos los socios disponibles en orden alfabético.</p> |
| Destino   | El primer elemento de esta lista es Todo, que está seleccionado de forma predeterminada. El resto de la lista es una lista ordenada de transportes de destino. En esta lista, puede seleccionar un único destino. El valor predeterminado es Todo. <p><b>Nota:</b> La lista Destino se rellena automáticamente con los destinos del socio seleccionado, y la lista se presenta en orden alfabético.</p>   |
| Ordenar por   | Seleccione si la lista se debe ordenar por Socios (valor predeterminado), por Destinos, ID de referencia o por Fecha y hora en cola (hora en que el documento se envió por última vez).   |
| ID de referencia  | Escriba el número de identificación exclusivo asignado al documento por el sistema.   |
| Dirección   | Pulse <b>Ascendente</b> para mostrar los documentos empezando por la última indicación de la hora o el final del abecedario, o <b>Descendente</b> para mostrar los documentos empezando por la indicación de la hora más reciente o el principio del abecedario.  |
| ID de documento   | Escriba el número de identificación exclusivo asignado al documento por el socio de origen.   |
| Resultados por página<br>Nº máximo de<br>documentos<br>permitidos | Especifica el número de documentos mostrados en una página.<br>Especifica el número de registros que se deben mostrar.  |

4. Pulse el botón **Buscar**. Se muestra el resultado de la búsqueda de colas.

## Eliminación de documentos de la cola de entrega

En el siguiente procedimiento se describe cómo eliminar documentos de la cola de entrega. Debe haber iniciado sesión como administrador de concentrador para eliminar documentos de la cola.

1. Pulse **Visores > Cola de destino**.
2. En la ventana Cola de destino, pulse **Buscar**.
3. Complete los parámetros en la ventana (consulte la Tabla 30 en la página 79).
4. Pulse el icono Suprimir para suprimir el documento.

## Visualización de los detalles de destino

Para ver información acerca de un destino en concreto, incluida una lista de documentos en la cola, utilice el siguiente procedimiento:

1. Pulse **Visores > Cola de destino**.
2. En la ventana Cola de destino, escriba los criterios de búsqueda (consulte la Tabla 29 en la página 79).
3. Pulse el botón **Buscar**.
4. En la lista de destinos, pulse el enlace del recuento de documentos de la columna **En cola**. Aparecerán los detalles de destino y una lista de documentos en cola.

## Cambio del estado de destino

Para colocar un destino en línea o fuera de línea, utilice el procedimiento siguiente:

1. Pulse **Visores > Cola de destino**.
2. En la ventana Cola de destino, escriba los criterios de búsqueda (consulte la Tabla 29 en la página 79).
3. Pulse el botón **Buscar**.
4. En la lista de destinos, pulse el enlace del recuento de documentos de la columna **En cola**. Aparecerán los detalles de destino y una lista de documentos en cola.
5. Pulse **En línea** en **Información de destino** para colocar un destino fuera de línea, o pulse **Fuera de línea** para colocar un destino fuera de línea. (Debe haber iniciado sesión como administrador de concentrador para cambiar el estado del destino).



---

## Capítulo 6. Análisis de tipo de documento: Herramientas

Utilice la herramienta Análisis de documento para obtener una visión general detallada del número de documentos en el sistema, por estado (Recibido, En progreso, Error y Satisfactorio). Los criterios de búsqueda incluyen fecha, hora, tipo de proceso (Hacia o Desde), tipo de destino, protocolo, tipo de documento y versión del proceso. Utilice los resultados de la búsqueda para localizar y visualizar los documentos con anomalías y para investigar el motivo de las mismas.

El Informe de volumen de documentos es una herramienta valiosa para gestionar, realizar el seguimiento y resolver problemas relacionados con el flujo de los documentos de empresa. El informe muestra el volumen de los documentos procesados por el sistema dentro de un periodo de tiempo específico. Este informe se puede ver, imprimir y guardar (exportado) para enviárselo a otros miembros de personal. Puede personalizar este informe para ver información basada en criterios de búsqueda específicos.

La herramienta Probar conexión de socio se utiliza para probar el destino o el servidor web.

*Tabla 32. Herramientas*

| <b>¿Qué característica desea utilizar?</b> | <b>Consulte</b> |
|--|-----------------|
| Análisis de documentos                     | la página 83    |
| Informe de volumen de documentos           | la página 86    |
| Probar conexión de socio                   | la página 87    |
| Informes de EDI                            | la página 90    |
| Informes de FTP                            | la página 94    |

---

### Análisis de documentos

Utilice la herramienta Análisis de documento para obtener una visión general detallada del número de documentos en el sistema, por estado, dentro de un periodo de tiempo específico.

Utilice los criterios de búsqueda para localizar los documentos con anomalías e investigar el motivo de las mismas.

La pantalla Análisis de documentos incluye una alarma. Si se ha producido un error en un proceso, la fila que contiene el proceso erróneo parpadea en rojo.

## Estados de documento

La siguiente tabla describe los distintos estados de documento.

Tabla 33. Estados de documento

| Estado        | Descripción  |
|---------------|--|
| Recibido      | El sistema ha recibido el documento y espera para procesarlo.  |
| En progreso   | El documento está actualmente en uno de los siguientes pasos de proceso: <ul style="list-style-type: none"><li>• <b>Incompleto.</b> Por ejemplo, el sistema está esperando otros documentos.</li><li>• <b>Validación de datos.</b> Por ejemplo, el sistema está comprobando el contenido del documento.</li><li>• <b>Traducción.</b> Por ejemplo, el sistema está convirtiendo el documento a otro protocolo.</li><li>• <b>Cola.</b> Por ejemplo, el documento está esperando a ser direccionado al socio externo o interno.</li></ul> |
| Error         | El proceso de documento se ha interrumpido debido a errores en el sistema, validación de datos o duplicados.   |
| Satisfactorio | El mensaje final que completa el proceso de documentos se ha transmitido desde el sistema hasta el socio de destino.   |

## Visualización de documentos en el sistema

1. Pulse **Herramientas > Análisis de documentos**. El sistema muestra la pantalla Búsqueda de análisis de documentos.
2. Seleccione los criterios de búsqueda en las listas desplegadas.

Tabla 34. Criterios de búsqueda de documentos

| Valor                        | Descripción  |
|------------------------------|--|
| Fecha y hora de inicio       | La fecha y la hora en las que se inició el proceso.  |
| Fecha y hora de finalización | La fecha y la hora en las que finalizó el proceso.   |
| Socio de origen              | El socio que ha iniciado el proceso empresarial (sólo socio interno).  |
| Socio de destino             | El socio que ha recibido el proceso empresarial (sólo socio interno).  |
| Buscar en                    | Buscar en el tipo de documento de origen o en el tipo de documento de destino.   |
| Tipo de destino              | Por ejemplo, producción o prueba. La prueba sólo está disponible en sistemas que dan soporte al tipo de destino de prueba. |
| Paquete                      | Describe el formato, el empaquetado, el cifrado y la identificación content-type del documento.                            |
| Protocolo                    | Protocolo de documento disponible para los socios.   |
| Tipo de documento            | Proceso empresarial específico.  |
| Ordenar por                  | Ordenar resultados por Nombre de socio de origen o Nombre de socio de destino.   |
| Renovar                      | Controla si los resultados de la búsqueda se renuevan periódicamente (sólo socio interno).                                 |
| Cadencia de renovación       | Controla la frecuencia de renovación de los resultados de la búsqueda (sólo el socio interno).                             |

3. Pulse el botón **Buscar**. El sistema muestra el Resumen de análisis de documentos.



## Visualización de detalles de procesos y sucesos

1. Pulse **Herramientas > Análisis de documentos**. El sistema muestra la pantalla Búsqueda de análisis de documentos.
2. Seleccione los criterios de búsqueda en las listas desplegables.
3. Pulse el botón **Buscar**. El sistema muestra el Resumen de análisis de documentos.
4. Pulse el icono Ver detalles al lado de los socios de origen y de destino que desea visualizar. El sistema muestra una lista de todos los documentos correspondientes a los socios seleccionados. La cantidad de documentos se ordena en columnas según el estado de proceso de documento.
5. Seleccione el enlace de cantidad en las columnas Recibido, En progreso, Error o Satisfactorio. El sistema presenta detalles de procesos de documentos en el Informe de análisis de documentos. Si selecciona Error, el informe también incluirá un Resumen de sucesos de documento.

---

## Proceso de archivos XML personalizados

WebSphere Partner Gateway V6.0 y versiones anteriores proporcionaban soporte al proceso personalizado XML (Extensible Markup Language) utilizando formatos XML. WebSphere Partner Gateway V6.0 y los formatos XML anteriores no permiten utilizar todo el lenguaje de expresión de XPath para extraer la información del proceso de los documentos. Éste es el motivo por el cual WebSphere Partner Gateway V6.1 ha vuelto a diseñar la forma en que funcionan los formatos XML. En WebSphere Partner Gateway V6.1, las expresiones de la versión 1.0 de XPath se pueden utilizar en los formatos. La potencia añadida de proceso del soporte completo de XPath limita el tamaño de los archivos que se pueden utilizar con los formatos XML completos de XPath. Para permitir que se procesen archivos grandes se proporciona una opción que se establece cuando se define una familia de documentos. Los formatos de una familia con la opción de proceso de archivos grandes tienen la misma potencia de proceso limitada de XPath que la que proporcionaba WebSphere Partner Gateway V6.0 y las versiones anteriores, pero se pueden procesar archivos grandes. Cuando se utiliza la opción de archivos grandes en una familia de documentos, estas limitaciones se colocan en las expresiones utilizadas en los formatos XML que se almacenan en la familia:

1. Sólo se pueden utilizar las vías de acceso de elementos simples que empiezan en la raíz del documento.
2. Las vías de acceso de elementos no deben incluir prefijos de espacio de nombres aunque es posible que aparezcan en los documentos.

La ventana Gestionar formatos XML incluye una lista desplegable con la etiqueta Opciones de archivos grandes. La lista incluye las opciones: *Ninguno*, *Utilizar procesador de archivos grandes* y *Utilizar procesador de archivos grandes con reconocimiento de espacio de nombres*. El usuario selecciona un opción de archivo grandes si está grabando formatos XML que coincidirán con los documentos grandes que no se puedan manejar con el procesador completo de XPath. La opción de reconocimiento de espacio de nombres significa que las vías de acceso de los elementos incluyen prefijos de espacio de nombres cuando aparecen en un documento.

**Nota:** Esta opción no se puede cambiar una vez creada la familia. El motivo es que es posible que la familia de documentos ya incluya formatos XML que no serán válidos si se cambia el tipo de familia. El proceso de archivos XML personalizados no está disponible para los socios.

---

## Informe de volumen de documentos

El Informe de volumen de documentos es una herramienta valiosa para gestionar, realizar el seguimiento y resolver problemas relacionados con el flujo de los documentos de empresa. El informe muestra el volumen de los documentos procesados por el sistema dentro de un periodo de tiempo específico. Este informe se puede ver, imprimir y guardar (exportado) para enviárselo a otros miembros de personal.

Puede personalizar este informe para ver información basada en criterios de búsqueda específicos.

El Informe de volumen de documentos muestra el número de documentos actualmente en proceso según su estado:

*Tabla 35. Estados de documento*

| Valor           | Descripción  |
|-----------------|--|
| Total recibidos | Número total de documentos recibidos por el sistema.   |
| En progreso     | Los documentos que están en progreso están siendo probados y validados. No se ha detectado ningún error pero el proceso no ha concluido todavía. |
| Error           | El proceso de documento se interrumpió debido a un error.  |
| Satisfactorio   | El mensaje final que completa el proceso de documentos se ha transmitido desde el sistema hasta el socio de destino.                             |

Utilice este informe para realizar las siguientes tareas:

- Determinar si los procesos empresariales clave se han completado.
- Realizar un seguimiento de las tendencias en volumen de proceso para el control de costes.
- Gestionar la calidad de los procesos: satisfactoria o errónea.
- Si usted es el socio interno, ayude a los socios a realizar el seguimiento de la eficacia del proceso.

## Creación de un informe de volumen de documentos

1. Pulse **Herramientas > Informe del volumen de documentos**. El sistema mostrará la pantalla Búsqueda de informes de volumen de documentos.

2. Seleccione los criterios de búsqueda en las listas desplegadas.

Tabla 36. Criterios de búsqueda de informes de volumen de documentos

| Valor                        | Descripción   |
|------------------------------|---|
| Fecha y hora de inicio       | La fecha y la hora en las que se inició el proceso.   |
| Fecha y hora de finalización | La fecha y la hora en las que finalizó el proceso.  |
| Socio de origen              | El socio que ha iniciado el proceso empresarial (sólo socio interno).                                 |
| Socio de destino             | El socio que ha recibido el proceso empresarial (sólo socio interno).                                 |
| Buscar en                    | Buscar en el tipo de documento de origen o en el tipo de documento de destino.                        |
| Tipo de destino              | Producción o prueba. Prueba sólo disponible en sistemas que dan soporte al tipo de destino de prueba. |
| Paquete                      | Describe el formato, el empaquetado, el cifrado y la identificación content-type del documento.       |
| Protocolo                    | Tipo de protocolo de proceso, por ejemplo, XML, EDI, archivo sin formato.                             |
| Tipo de documento            | Proceso empresarial específico.   |
| Ordenar por                  | Ordenar resultados por este criterio (tipo de documento o tipo de documento de destino).              |
| Resultados por página        | Número de registros mostrados por página.   |

3. Pulse el botón **Buscar**. El sistema muestra el informe.

## Exportación del informe de volumen de documentos

1. Pulse **Herramientas > Informe del volumen de documentos**. El sistema mostrará la pantalla Búsqueda de informes de volumen de documentos.
2. Seleccione los criterios de búsqueda en las listas desplegadas.
3. Pulse el botón **Buscar**. El sistema muestra el informe.
4. Pulse el icono Exportar informe para exportar el informe. Navegue hasta la ubicación deseada para guardar el archivo.

**Nota:** Los informes se guardan como archivos de valores separados por comas (.CSV). El nombre de archivo tiene un sufijo “.csv”.

## Impresión de informes

1. Pulse **Herramientas > Informe del volumen de documentos**. El sistema mostrará la pantalla Búsqueda de informes de volumen de documentos.
2. Seleccione los criterios de búsqueda en las listas desplegadas.
3. Pulse el botón **Buscar**. El sistema muestra el informe.
4. Pulse el icono Imprimir para imprimir el informe.

---

## Probar conexión de socio

La función Probar conexión de socio permite probar el destino o el servidor web. Si usted es el socio interno, también puede seleccionar a un socio específico. La prueba consiste en enviar una solicitud de autoprueba de encendido en blanco a un destino o URL. La solicitud es similar a introducir el URL de Yahoo (www.yahoo.com) en el campo de dirección del navegador. Nada se envía; es una solicitud vacía. La respuesta recibida del destino o servidor web indicará su estado:

- Si se devuelve una respuesta, el servidor estará activado.

- Si no se devuelve nada, el servidor estará inactivo.

**Importante:** La función Probar conexión de socio funciona con el protocolo HTTP, que no requiere ningún parámetro de conexión.

**Para probar una conexión de socio:**

1. Haga clic en **Herramientas > Probar conexión de socio**. El sistema muestra la pantalla Probar conexión de socio.
2. Seleccione los criterios de prueba de las listas desplegables.

*Tabla 37. Probar valores de la conexión de socio*

| Valor   | Descripción   |
|---------|---|
| Socio   | Socio que hay que probar (sólo socio interno).                                    |
| Destino | Muestra los destinos disponibles en función del socio seleccionado anteriormente. |
| URL     | Rellenado dinámicamente en función del destino seleccionado anteriormente.        |
| Mandato | Post o Get.   |

3. Pulse el botón **Probar URL**. El sistema mostrará los resultados de la prueba. Para obtener información sobre el código de estado devuelto, consulte los siguientes apartados.

## Códigos de resultado de servidor web

### Serie 200:

- 200 - Correcto - Transmisión satisfactoria. No es un error. Aquí está el archivo solicitado.
- 201 - Creado - La solicitud se ha llevado a cabo y dado como resultado la creación de un nuevo recurso. El recurso recientemente creado se puede referenciar mediante los URL devueltos en el campo cabecera de URL de la respuesta, con el URL más específico para el recurso determinado mediante un campo de cabecera Ubicación.
- 202 - Aceptado - La solicitud ha sido aceptada para ser procesada, pero el proceso todavía no se ha completado.
- 203 - Información no autoritativa - La información META devuelta en la cabecera de entidad no es el conjunto definitivo disponible del servidor de origen, pero se reúne a partir de una copia local o de terceros.
- 204 - Sin contenido - El servidor ha completado satisfactoriamente la solicitud, pero no hay información nueva que volver a enviar.
- 206 - Contenido parcial - Ha solicitado un rango de bytes en el archivo y aquí están. Esto es nuevo en HTTP 1.1

### Serie 300:

- 301 - Movido permanentemente - El recurso solicitado se ha asignado a un URL nuevo permanente y cualquier referencia futura a este recurso debería llevarse a cabo usando uno de los URL devueltos.
- 302 - Movido temporalmente - El recurso solicitado reside temporalmente bajo un nuevo URL. Redirigiéndolo a un nuevo URL. La página original se ha movido. No es un error; la mayoría de los navegadores encuentran invisible la nueva página cuando ven este resultado.

### **Serie 400:**

- 400 - Solicitud errónea - La solicitud podría no haber sido entendida por el servidor debido a una sintaxis que no está bien formada. La solicitud errónea fue realizada por el cliente.
- 401 - No autorizada - La solicitud requiere autenticación del usuario. La respuesta debe incluir un campo de cabecera WWW-Authenticate que contiene una pregunta aplicable al origen solicitado. El usuario pidió un documento pero no proporcionó un nombre de usuario o una contraseña válidos.
- 402 - Pago necesario - Este código no está actualmente soportado, pero se reserva para futuro uso.
- 403 - Prohibido - El servidor entendió la solicitud pero está rechazando realizarla por un motivo no especificado. Se niega explícitamente el acceso a este documento. (Esto podría producirse porque el servidor no tiene permiso de lectura para el archivo que esté solicitando). El servidor rechaza enviarle este archivo. Puede que el permiso se haya desactivado explícitamente.
- 404 - No encontrado - El servidor no ha encontrado nada que coincida con el URL solicitado. Este archivo no existe. Lo obtiene si proporciona un URL erróneo al navegador. También se puede enviar si el servidor ha recibido instrucciones de proteger el documento comunicando a las personas no autorizadas que no existe. Los errores 404 son el resultado de solicitudes de páginas que no existen, y pueden deberse a un URL escrito incorrectamente, a un marcador que señala a un archivo que ya no está, a motores de búsqueda que buscan un robots.txt (que se utiliza para marcar páginas que no desea que los motores de búsqueda indexen), a personas que adivinan nombres de archivo, a enlaces erróneos del sitio o de otros sitios, etc.
- 405 - Método no permitido - El método especificado en la línea de solicitud no está permitido para el recurso identificado por el URL de solicitud.
- 406 - Ninguno aceptable - El servidor ha encontrado un recurso que coincide con el URL de solicitud, pero no uno que satisfaga las condiciones identificadas por las cabeceras Aceptar y Aceptar-Codificando solicitud.
- 407 - Autenticación de proxy necesaria - Este código se reserva para uso futuro. Es parecido al 401 (No autorizado) pero indica que el cliente debe primero autenticarse con un proxy. HTTP 1.0 no proporciona ningún medio para la autenticación de proxy.
- 408 - Tiempo de espera de solicitud - El cliente no produjo una solicitud dentro del tiempo de espera del servidor.
- 409 - Conflicto - La solicitud no se ha podido completar debido a un conflicto con el estado actual del recurso.
- 410 - Eliminado - El recurso solicitado no se encuentra ya disponible en el servidor y no se conoce ninguna dirección de reenvío.
- 411 - Autorización rechazada - Las credenciales de solicitud proporcionadas por el cliente fueron rechazadas por el servidor o no eran suficientes para otorgar una autorización de acceso al recurso.
- 412 - Error de precondition
- 413 - Solicitud de entidad demasiado grande
- 414 - Solicitud de URI demasiado grande
- 415 - Tipo de medio no soportado

### **Serie 500:**

- 500 - Error interno del servidor - El servidor ha encontrado una condición no esperada que le ha impedido completar la solicitud. Algo no funcionaba en el servidor web y no se le ha podido ofrecer una respuesta significativa.

Normalmente, no se puede hacer nada desde el extremo del navegador para arreglar este error; probablemente, el administrador del servidor tendrá que comprobar el registro cronológico de errores del servidor para ver qué ha ocurrido. Se trata a menudo del mensaje de error para un script de CGI que no se ha codificado correctamente.

- 501 - Método no implementado - El servidor no soporta la funcionalidad necesaria para completar la solicitud. El método de aplicación (GET o POST) no se ha implementado.
- 502 - Destino erróneo - El servidor recibió una respuesta no válida del destino o servidor ascendente al que accedió intentando completar la solicitud.
- 503 - Servicio temporalmente no disponible - El servidor no puede actualmente manejar la solicitud debido a una sobrecarga o un mantenimiento temporal del servidor. El servidor se ha quedado sin recursos.
- 504 - Tiempo de espera de destino - El servidor no recibió una respuesta a tiempo del destino o servidor ascendente al que accedió intentando completar la solicitud.
- 505 - Versión de HTTP no soportada

---

## Informes de EDI

Utilice Informes de EDI para buscar reconocimientos funcionales (FA) retrasados de intercambio de datos electrónicos (EDI). También puede buscar transacciones de intercambio de datos electrónicos (EDI) rechazados. En las secciones siguientes se detalla el procedimiento para utilizar Informes de EDI.

### Búsqueda de FA retrasados de EDI

La página Búsqueda de FA retrasados de EDI proporciona criterios de búsqueda para realizar una búsqueda de reconocimientos funcionales (FA) retrasados de intercambio de datos electrónicos (EDI).

**Nota:** Los registros devueltos por búsquedas de FA retrasados de EDI y que se eliminaron de los informes resultantes se pasarán por alto en búsquedas posteriores. Por consiguiente, los registros eliminados no se visualizan en informes posteriores. Los registros pueden eliminarse de un informe si se selecciona **Ignorar registros seleccionados** en la página Informe de FA de EDI retrasados. Sólo el administrador de concentradores puede eliminar registros de un informe.

Para buscar registros de FA de EDI retrasados, realice lo siguiente:

1. Pulse **Herramientas > Informes de EDI**. Se muestra la pantalla Búsqueda de FA retrasados de EDI.

2. Seleccione uno o varios criterios de búsqueda en la lista desplegable:

*Tabla 38. Criterios de búsqueda de FA retrasados de EDI*

| Valor                        | Descripción   |
|------------------------------|---|
| Fecha y hora de inicio       | La fecha y la hora en las que se inició la transacción.   |
| Fecha y hora de finalización | La fecha y la hora en las que finalizó la transacción.  |
| Socio de origen              | El socio que inició la transacción.   |
| Socio de destino             | El socio que recibió la transacción.  |
| Buscar en                    | Buscar en Tipo de documento de origen o en Tipo de documento de destino.  |
| Paquete                      | Describe el formato, el empaquetado, el cifrado y la identificación content-type del documento.   |
| Protocolo                    | Tipo de protocolo de proceso, por ejemplo, XML, EDI, archivo sin formato. Los protocolos visualizados varían en función del valor que seleccione en el campo Paquete.   |
| Tipo de documento            | Especifique el tipo de documento. Los tipos visualizados varían en función del valor que seleccione en el campo Paquete.  |
| ID de referencia             | Especifica un ID de transacción.  |
| Ordenar por                  | Especifica los criterios para ordenar los resultados de la búsqueda. Los valores predeterminados son Tiempo de retraso y Descendente. Utilice Descendente para visualizar primero los FA más retrasados. Seleccione Ascendente para visualizar primero los FA menos retrasados. |
| Resultados por página        | Especifica el número de resultados de búsqueda de transacciones que se visualizan en cada página.   |

3. Pulse **Buscar** para visualizar el informe de Búsqueda de FA retrasados de EDI.

### **Visualización de informes de retraso de FA de EDI**

En función de los criterios de búsqueda seleccionados en la página Búsqueda de FA retrasados de EDI, el resultado de la búsqueda se muestra en la página Informe de retraso de FA de EDI.

Los datos siguientes, cuando son aplicables, se muestran en el informe de retraso de FA de EDI.

Tabla 39. Informe de retraso de FA de EDI

| Valor                           | Descripción   |
|---------------------------------|---|
| Fecha                           | La fecha en que se envió el EDI desde el socio de origen al socio de destino.   |
| Hora                            | La hora (GMT) en que se envió el EDI desde el socio de origen al socio de destino.  |
| ID de actividad                 | El ID virtualmente exclusivo (VUID) de la transacción.  |
| Socio comercial de origen       | El socio que envió la transacción.  |
| Paquete de origen               | El paquete de origen de la transacción.   |
| Protocolo de origen             | El protocolo de origen de la transacción.   |
| Tipo de documento de origen     | El tipo de documento de origen de la transacción.   |
| Socio comercial de destino      | El socio que envió la transacción.  |
| Paquete de destino              | El paquete de destino de la transacción.  |
| Protocolo de destino            | El protocolo de destino de la transacción.  |
| Tipo de documento de destino    | El tipo de documento de destino de la transacción.  |
| Número de intercambio           | El número de intercambio de la transacción.   |
| Número de grupo                 | El número de grupo de la transacción.   |
| Número de transacción           | El número de identificación de la transacción.  |
| FA vence el                     | La fecha en que vence el FA de la transacción.  |
| Vencido                         | Período de tiempo que el FA está retrasado.   |
| Ignorar registros seleccionados | Cuando se selecciona esta opción para un registro, dicho registro se elimina del informe. Una vez eliminado un registro de un informe, posteriores búsquedas de retrasos de FA de EDI lo pasarán por alto y, por lo tanto, no se visualizará en los informes resultantes. Sólo el administrador de concentradores puede eliminar registros de un informe. |

## Búsqueda de transacciones rechazadas de EDI

La página Búsqueda de transacciones rechazadas de EDI contiene criterios para realizar búsquedas para transacciones de intercambio de datos electrónicos (EDI) que tienen un reconocimiento funcional (FA) que contiene un código de error. Una búsqueda de transacciones rechazadas de EDI no devuelve los registros de transacciones sin FA.

Para buscar registros rechazados de EDI, realice lo siguiente:

1. Pulse **Herramientas > Informes de EDI > Informe de rechazo de EDI**.



2. Seleccione uno o varios criterios de búsqueda en la lista desplegable:

*Tabla 40. Criterios de búsqueda de transacciones rechazadas de EDI*

| Valor                        | Descripción   |
|------------------------------|---|
| Fecha y hora de inicio       | La fecha y la hora en las que se inició la transacción.   |
| Fecha y hora de finalización | La fecha y la hora en las que finalizó la transacción.  |
| Socio de origen              | El socio que inició la transacción.   |
| Socio de destino             | El socio que recibió la transacción.  |
| Buscar en                    | Buscar en Tipo de documento de origen o en Tipo de documento de destino.  |
| Paquete                      | Describe el formato, el empaquetado, el cifrado y la identificación content-type del documento.   |
| Protocolo                    | Tipo de protocolo de proceso, por ejemplo, XML, EDI, archivo sin formato. Los protocolos visualizados varían en función del valor que seleccione en el campo Paquete.   |
| Tipo de documento            | Especifique el tipo de documento. Los tipos visualizados varían en función del valor que seleccione en el campo Paquete.  |
| ID de referencia             | Especifica un ID de transacción.  |
| Ordenar por                  | Especifica los criterios para ordenar los resultados de la búsqueda. Los valores predeterminados son Tiempo de retraso y Descendente. Utilice Descendente para visualizar primero los FA más retrasados. Seleccione Ascendente para visualizar primero los FA menos retrasados. |
| Resultados por página        | Especifica el número de resultados de búsqueda de transacciones que se visualizan en cada página.   |

3. Pulse **Buscar** para ver el informe de transacciones rechazadas de EDI.

### **Visualización de informes de transacciones rechazadas de EDI**

En función de los criterios de búsqueda seleccionados en la página Búsqueda de transacciones rechazadas de EDI, el resultado de la búsqueda se muestra en la página Informe de transacciones rechazadas de EDI.

Los datos siguientes, cuando son aplicables, se muestran en el informe de transacciones rechazadas de EDI.

Tabla 41. Informe de transacciones rechazadas de EDI

| Valor                        | Descripción   |
|------------------------------|---|
| Fecha                        | La fecha en que se recibió el EDI.  |
| Hora                         | La hora (GMT) en que se envió la transacción de EDI desde el socio de origen al socio de destino. |
| ID de actividad              | El ID virtualmente exclusivo (VUID) de la transacción.  |
| Socio comercial de origen    | El socio que envió la transacción.  |
| Paquete de origen            | El paquete de origen de la transacción.   |
| Protocolo de origen          | El protocolo de origen de la transacción.   |
| Tipo de documento de origen  | El tipo de documento de origen de la transacción.   |
| Socio comercial de destino   | El socio que recibió la transacción.  |
| Paquete de destino           | El paquete de destino de la transacción.  |
| Protocolo de destino         | El protocolo de destino de la transacción.  |
| Tipo de documento de destino | El tipo de documento de destino de la transacción.  |
| Número de intercambio        | El número de intercambio de la transacción.   |
| Número de grupo              | El número de grupo de la transacción.   |
| Número de transacción        | El número de identificación de la transacción.  |
| Código de estado             | El código de estado de FA.  |
| Texto de estado              | El texto de estado de FA.   |

---

## Informes de FTP

Informes de FTP proporciona detalles sobre estadísticas de FTP y conexiones FTP.

### Estadísticas de FTP

La página Estadísticas de FTP mostrará el estado de servidor FTP en modalidad de sólo lectura.

**Nota:** Las estadísticas no se visualizarán si el servidor FTP o el servidor de gestión de FTP no está disponible.

Para ver el estado del servidor FTP, realice lo siguiente:

1. Pulse **Herramientas > Informes de FTP**. Se muestra la página Estadísticas de FTP.

2. Se muestra la siguiente información sobre el estado de los servidores:

*Tabla 42. Estadísticas de FTP*

| Valor                               | Descripción  |
|-------------------------------------|--|
| Hora de inicio del servidor         | Hora de inicio del Servidor FTP.   |
| Número de directorios creados       | Número de directorios creados por usuarios mediante mkdir.                       |
| Número de directorios eliminados    | Número de directorios eliminados por usuarios mediante rmdir.                    |
| Número de archivos cargados         | Número de archivos cargados por todos los usuarios.                              |
| Número de archivos descargados      | Número de archivos descargados por todos los usuarios.                           |
| Número de archivos suprimidos       | Número de archivos suprimidos por todos los usuarios mediante el mandato delete. |
| Bytes cargados                      | Número total de bytes cargados.  |
| Bytes descargados                   | Número total de bytes descargados.   |
| Inicios de sesión actuales          | Visualiza los inicios de sesión existentes.                                      |
| Total de inicios de sesión          | Total de inicios de sesión desde el último restablecimiento.                     |
| Total de inicios de sesión erróneos | Número total de inicios de sesión erróneos.                                      |
| Conexiones actuales                 | Conexiones actuales desde el último restablecimiento.                            |
| Conexiones totales                  | Conexiones totales desde el último restablecimiento.                             |

3. Pulse **Recargar** para renovar los inicios de sesión actuales.

4. Pulse **Restablecer** para restablecer los valores.

## Conexiones FTP

Vea las conexiones FTP siguiendo los pasos indicados a continuación:

1. Pulse **Herramientas > Informes de FTP > Conexiones FTP**.

2. En el informe se muestra la siguiente información sobre conexiones:

*Tabla 43. Conexiones FTP*

| Valor                      | Descripción  |
|----------------------------|--|
| Nombre de inicio de sesión | El ID de usuario de inicio de sesión correspondiente a esta conexión. Si está en blanco, quiere decir que el usuario sólo ha establecido una conexión pero no ha iniciado la sesión. |
| Hora de inicio de sesión   | La hora en que el usuario inició la sesión. Si está en blanco, quiere decir que el usuario sólo ha establecido una conexión.   |
| Última hora de acceso      | La hora en que el usuario accedió por última vez a esta conexión. Si está en blanco, quiere decir que el usuario sólo ha iniciado la sesión pero no ha emitido ningún mandato aún.   |
| Dirección de cliente       | La IP del cliente desde la que el usuario ha iniciado la sesión.   |



---

## Glosario

### A

**Administración de cuentas.** El módulo Administración de cuentas le permite ver y editar la información que identifica la empresa en la red. Esta pantalla también se utiliza para gestionar los privilegios de acceso a la consola de otro personal de su empresa.

**Acción.** (1) Acciones realizadas en un documento por el sistema para garantizar su compatibilidad con los requisitos empresariales entre socios. (2) Una serie de pasos de proceso como, por ejemplo, validación y transformación de documentos.

**ID de instancia de acción.** Identifica documentos con contenido de naturaleza comercial, como una orden de compra o RFQ.

**Activación.** Conexión de un socio al sistema.

**Alerta.** Las alertas proporcionan una notificación y una resolución rápidas cuando se infringen los límites operativos preestablecidos. Una alerta se compone de un mensaje de correo electrónico basado en texto enviado a personas o a una lista de distribución de personal clave dentro o fuera de la red. Las alertas se pueden basar en la aparición de un suceso de sistema o en un volumen de proceso esperado.

**Recuento de intentos.** Indica si la transacción es un primer intento o un reintento. 1 es un primer intento. 2 o más son el número de reintentos.

### B

**Proceso empresarial.** Un conjunto predefinido de transacciones que representan el método de realizar el trabajo necesario para lograr un objetivo empresarial.

**Realización de pruebas de normas empresariales.** Proceso de realización de pruebas y reparación de errores de contenido de documentos entre socios.

**Código de señal empresarial.** Identifica el tipo de señal (documento) enviado en respuesta a una acción. Algunos ejemplos son el recibo, el acuse de recibo, o la excepción normal.

### C

**Conexión de los socios.** Una conexión de socio define la conexión entre dos entornos de miembro de comunidad específicos a través de los cuales se ejecuta un proceso único.

**Conjunto de certificados.** Un conjunto de certificados primarios y secundarios que pueden asociarse a una conexión participante.

**Coreografía.** Orden necesario de documentos para completar correctamente un proceso empresarial.

**Clasificación.** Identifica el rol de socio en un proceso empresarial.

**Cerrado.** Fecha y hora en las que se transaccionó el último documento de un proceso o en las que se canceló un proceso.

**Consola de comunidad.** La Consola de comunidad es una herramienta basada en web que se utiliza para supervisar el flujo de los documentos comerciales de la empresa hacia y desde el socio interno o los socios externos.

**Hijo de Socio interno.** Hijo de socio interno es un tipo de socio especial que actúa como socio en la consola pero como socio interno cuando hay direccionamiento.

**Socio externo.** Miembro de comunidad de concentrador que intercambia transacciones empresariales con el socio interno.

### D

**Mitigación de datos.** El proceso de probar y reparar errores en la estructura y el formato del documento según estándares de proceso empresarial.

**Firma digital.** Una firma digital es una firma electrónica que se utiliza para autenticar la identidad de los socios, y para asegurar que el contenido original de un documento que se ha enviado no se cambia.

**Desensobrar .** Extraer un documento de un sobre EDI.

**Destino.** Punto de red B2B que actúa como entrada de otra red. Los problemas de compatibilidad y transacción de datos se pueden resolver mediante un destino que garantice la transferencia de datos.

**Documento.** Colección de información que cumple con a un convenio organizativo. La información puede ser texto, imágenes y sonido.

**Definición de documentos.** Ofrece al sistema toda la información necesaria para recibir, procesar y direccionar documentos entre miembros de comunidad. Los tipos de definición de documentos son paquete, protocolo, tipo de documento, actividad y acción.

**Protocolo de documento.** Conjunto de normas e instrucciones (protocolo) para el formateo y la transmisión de información por una red de sistemas. Algunos ejemplos son RosettaNet, XML, archivo sin formato y EDI.

**DUNS.** El número D-U-N-S de D&B es una secuencia de identificación única de nueve dígitos que proporciona identificadores exclusivos de entidades empresariales mientras enlaza estructuras de familias corporativas. D&B enlaza los números D-U-N-S de D&B de padres, subsidiarios, sedes y ramas de más de 64 millones de miembros de familias corporativas de todo el mundo. Utilizado por las organizaciones más influyentes, es reconocido, recomendado y, a menudo, requerido por más de 50 asociaciones comerciales e industriales del mundo, que incluyen las Naciones Unidas, el Gobierno Federal de EE.UU., el Gobierno australiano y la Comisión Europea. En la economía global de nuestros días, el número D-U-N-S de D&B se ha convertido en el estándar para realizar el seguimiento de las empresas del mundo.

## E

**EDI.** Transferencia de sistema a sistema de información en un formato estructurado y predeterminado. Normalmente, el principal objetivo de la actividad de EDI ha sido la sustitución de formatos de empresa predefinidos como, por ejemplo, los órdenes de compra y las facturas, con formatos electrónicos definidos de manera similar.

**Suceso.** Mensaje generado por el sistema asociado con el proceso de documentos.

## F

**Filtro.** Eliminar datos dentro de una subtransacción según parámetros predefinidos.

**FTP.** El protocolo de transferencia de archivos (File Transfer Protocol, FTP), un protocolo de Internet estándar, es la forma más sencilla de intercambiar archivos entre sistemas en Internet.

## G

**Modalidad de funcionamiento.** Identifica los documentos que se dirigen a una pasarela determinada durante la realización de pruebas o para la producción en directo.

**Global.** El socio y el socio interno pueden asignar alertas a la persona de contacto.

**Grupo.** Una colección de usuarios a los que se otorga privilegio de acceso para la consola y que pueden realizar funciones seleccionadas.

## H

**HTTP.** El Protocolo de transferencia de hipertexto (Hypertext Transfer Protocol, HTTP) es el conjunto de normas (protocolo) para intercambiar archivos (texto, imágenes de gráfico, sonido, vídeo y otros archivos multimedia) en la web.

**HTTPS.** HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) es un protocolo web que cifra y descifra solicitudes de páginas de usuario, así como páginas que sean devueltas por el servidor web.

## I

**Acción de empresa en respuesta.** Identifica el tipo de documento de empresa enviado en respuesta a una acción en el mismo proceso.

**ID en respuesta.** Número de ID de la acción de empresa en respuesta

**Gestor entrante.** Recupera documentos del NAS y los prepara para la tarea de acción adecuada mediante el motor de proceso empresarial.

## L

**Directo.** El estado en el que un socio ha completado correctamente la realización de pruebas de normas empresariales, y en el que el socio interno ha emitido una incidencia para moverlas a un estado en directo.

## P

**Paquetes.** Identifique formatos de paquetes de documento que se puedan recibir por el servidor del sistema. Por ejemplo, AS1 y AS2.

**PIP (Partner Interface Process).** Defina procesos empresariales entre socios internos y socios (en WebSphere Partner Gateway, los socios son participantes). Cada PIP identifica un documento de empresa específico y la forma en que se procesa.

**ID de instancia de proceso.** Número de identificación exclusivo para un proceso empresarial determinado.

**Producción.** Pasarela de destino utilizada para direccionar documentos en directo.

**Perfil.** El módulo Perfil le permite ver y editar la información que identifica su empresa en el sistema.

**Protocolos.** Identifique tipos específicos de formatos de documento para una gran variedad de procesos empresariales. Por ejemplo, RosettaNet y XML.

**Abastecimiento.** El abastecimiento (o en embarque) consiste en completar una secuencia de pasos

necesarios para conectar una pasarela B2B de usuario con la infraestructura del sistema.

## R

**Informes.** El módulo Informes permite a los usuarios crear informes detallados sobre el volumen de los documentos procesados, así como de los sucesos generados por el sistema.

**RNIF.** La infraestructura RosettaNet Implementation Framework (RNIF) es una directriz para crear un contenedor-sobre estándar para todos los procesos de interfaz de socio (Partner Interface Processes, PIP).

**RTF.** Rich Text Format (RTF) es un formato de archivo que le permite intercambiar archivos de texto entre distintos procesadores de texto en distintos sistemas operativos. Por ejemplo, puede crear un archivo utilizando Microsoft Word en Windows 98, guardarlo como archivo RTF (tendrá un sufijo de nombre de archivo .rtf) y enviárselo a alguien que utilice WordPerfect 6.0 en Windows 3.1.

## S

**Servicio.** Identifica si el mensaje está basado en RosettaNet.

**Servlet.** Pequeño programa que se ejecuta en el servidor web que graba el documento entrante en el NAS.

**Señal.** El documento enviado en respuesta a una acción.

**ID de instancia de señal.** Identifica documentos que son acuses de recibo positivos o negativos enviados en respuesta a acciones.

**Versión de señal.** Versión de proceso empresarial enviado como señal.

**SMTP.** Simple Mail Transfer Protocol es un protocolo utilizado en el envío y la recepción de correo electrónico.

**SR.** Solicitud de servicio

**SSL.** Secure Sockets Layer es un método seguro de enviar datos mediante el protocolo HTTP.

**Estado.** (1) Los documentos procesados por el sistema están en uno de cuatro estados (2) recibido, en progreso, erróneo o correcto.

**Contrato suscrito.** Un contacto suscrito es una persona a la que se ha designado para que reciba alertas de correo electrónico.

**Sustituto.** Sustituir datos dentro de una subtransacción por otros datos basados en parámetros predefinidos.

## T

**Prueba.** El estado en el que un socio se somete a la mitigación de datos o a la realización de pruebas de normas empresariales durante el proceso de abastecimiento.

**Herramientas.** El módulo Herramientas le permite solucionar problemas relacionados con anomalías de proceso permitiéndole ver documentos erróneos, campos de datos y sus sucesos asociados.

**Transacción.** Secuencia de intercambio de información y trabajo relacionado que se trata como unidad con el propósito de realizar negocios entre los socios.

**ID de transacción.** Número de ID de proceso empresarial.

**Transformar.** Sustituir el contenido de un documento por los datos de una tabla de referencia cruzada.

**Conversión.** Cuando un documento se convierte de un protocolo a otro.

**Protocolo de transporte.** Conjunto de normas (protocolo) utilizado para enviar datos en forma de unidades de mensaje entre sistemas a través de Internet. Algunos ejemplos son HTTP, HTTPS, SMTP y FTP.

## U

**URL.** Un URL (Uniform Resource Locator) es la dirección de un documento o proceso (recurso) accesible en Internet.

## V

**Validación.** La validación es el acto de comparar una subtransacción de proceso con los requisitos especificados para determinar su validez o no validez. La secuencia de transacción y el contenido son parámetros normales.

**Versión.** Release particular de un protocolo de documento.

**Visibilidad.** La visibilidad define si una persona de contacto puede haber sido asignada a una alerta a través de un socio (local) o, también, a través del socio interno (global).

## W

**Comodín.** Los criterios para búsquedas con comodín incluyen el asterisco (\*).



---

## Avisos

Puede que IBM no ofrezca los productos, los servicios o las características tratadas en este documento en todos los países. Consulte con el representante local de IBM para obtener información sobre los productos y servicios actualmente disponibles en su área. Cualquier referencia a un producto, programa o servicio de IBM no establece ni implica que sólo se pueda utilizar dicho producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de los productos, programas o servicios que no sean de IBM.

IBM puede tener patentes o aplicaciones de patente pendientes que cubran los temas descritos en este documento. El suministro de este documento no le ofrece ninguna licencia para estas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
EE.UU.

El siguiente párrafo no se aplica al Reino Unido ni a ningún otro país donde tales disposiciones no sean coherentes con las leyes locales:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INCUMPLIMIENTO, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no permiten declaración de limitación de responsabilidad de garantías explícitas o implícitas en determinadas transacciones, por lo que puede que no se aplique esta declaración.

Esta información podría incluir inexactitudes técnicas o errores tipográficos. A la información de este documento se le hacen cambios periódicamente; estos cambios se incorporarán a las nuevas ediciones de la publicación. IBM puede realizar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Toda referencia en esta información a sitios web que no sean de IBM se suministra sólo por comodidad y no sirve de ninguna manera como promoción de dichos sitios web. El material de dichos sitios web no forma parte del material de este producto de IBM y su uso es responsabilidad del usuario.

IBM puede utilizar o distribuir cualquier información suministrada por usted de la forma que crea conveniente sin que ello suponga ninguna obligación para usted.

Las personas con licencia de este programa que deseen obtener información sobre él con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deberían ponerse en contacto con:

IBM Burlingame Laboratory Director

IBM Burlingame Laboratory  
577 Airport Blvd., Suite 800  
Burlingame, CA 94010  
EE.UU.

Dicha información puede estar disponible, sujeta a los términos y las condiciones correspondientes, incluido en algunos casos el pago de una tarifa.

El programa bajo licencia descrito en este documento, y todo el material con licencia del que dispone, es suministrado por IBM bajo los términos del Contrato de licencia de IBM, el Contrato de licencia de programas internacional de IBM o cualquier acuerdo equivalente entre nosotros.

Cualquier dato de rendimiento aquí contenido se determinó en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar de manera significativa. Algunas medidas pueden haberse llevado a cabo en sistemas de nivel de desarrollo y no existe garantía de que dichas medidas sean las mismas en sistemas disponibles de manera normal. Además, algunas medidas pueden haberse calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deberían verificar los datos aplicables para su entorno específico.

La información relativa a productos que no sean de IBM se obtuvo de los proveedores de dichos productos, sus anuncios publicados u otras fuentes disponibles públicamente. IBM no ha probado necesariamente tales productos y no puede confirmar su exactitud de rendimiento, compatibilidad o cualquier otras cuestiones relacionadas con productos que no sean de IBM: Las preguntas sobre posibilidades de productos que no sean de IBM deberían dirigirse a los proveedores de tales productos.

Esta información puede contener ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlos de la mejor manera posible, los ejemplos pueden incluir nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones utilizados por una empresa real es totalmente casual.

Todas las declaraciones relativas a futuras directrices o intenciones de IBM están sujetas a cambios o reembolsos sin previo aviso, y representan sólo objetivos.

#### LICENCIA DE COPYRIGHT

Esta información puede contener programas de aplicación de ejemplo en el idioma de origen, que ilustran las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma, sin pago a IBM, con el fin de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programación de aplicación de la plataforma operativa para la que se graban los programas de ejemplo. Estos ejemplos no se han probado a fondo en todas las condiciones. Por lo tanto, IBM no puede garantizar ni asegurar la fiabilidad, la facilidad ni el funcionamiento de estos programas.

WebSphere Partner Gateway contiene código denominado ICU4J, cuya licencia le otorga IBM bajo los términos del Contrato de licencias de programa internacional, sujeto a sus términos de Componentes excluidos. No obstante, es necesario que IBM le ofrezca el siguiente párrafo como aviso:

## COPYRIGHT Y AVISO DE PERMISO

Copyright (c) 1995-2008 International Business Machines Corporation y otros.

Reservados todos los derechos.

El permiso se otorga por el presente, libre de cargo, a cualquier persona que obtenga una copia de este software y de los archivos de documentación asociados (el "Software"), para utilizar el software sin restricción, incluidos pero sin limitarse a, los derechos de utilización, copia, modificación, fusión, publicación, distribución o venta de copias del Software, y para permitir a aquellas personas a las que se suministre el Software a así hacerlo, dado que los avisos de copyright anteriores y este aviso de permiso aparecen en todas las copias del Software y ambos aparecen en la documentación de soporte.

EL SOFTWARE SE PROPORCIONA "TAL CUAL", SIN GARANTÍA DE NINGÚN TIPO, EXPLÍCITA O IMPLÍCITA, INCLUIDAS PERO SIN LIMITARSE A LAS GARANTÍAS DE COMERCIALIZACIÓN, IDONEIDAD PARA UN FIN DETERMINADO Y NO INCUMPLIMIENTO DE DERECHOS DE TERCEROS. EN NINGÚN CASO EL TITULAR O LOS TITULARES DEL COPYRIGHT INCLUIDOS EN ESTE AVISO SERÁN RESPONSABLES DE NINGUNA QUEJA O DAÑO INDIRECTO O CONSECUCIONAL, ASÍ COMO TAMPOCO DE LOS POSIBLES DAÑOS RESULTANTES DE LA PÉRDIDA DE FUNCIONAMIENTO, DATOS O BENEFICIOS, YA SEA EN UNA ACCIÓN DE CONTRATO, NEGLIGENCIA U OTRA ACCIÓN DE RESPONSABILIDAD EXTRA CONTRACTUAL, QUE SURJA O ESTE EN CONEXIÓN CON EL USO O RENDIMIENTO DE ESTE SOFTWARE.

Salvo si así consta en este aviso, el nombre de un titular de copyright no se utilizará en anuncios, etc. para promocionar la venta, el uso u otras funciones de este Software sin previa autorización escrita del titular del copyright.

---

## Información de la interfaz de programación

La información de la interfaz de programación, si se proporciona, sirve para ayudar a crear software de aplicación con este programa.

Las interfaces de programación de uso general le permiten grabar el software de aplicación que obtiene los servicios de las herramientas de este programa.

No obstante, esta información también puede contener información de diagnóstico, modificación y ajuste. La información de diagnóstico, modificación y ajuste sirve para ayudarle a depurar el software de aplicación.

**Aviso:** No utilice esta información de diagnóstico, modificación y ajuste como interfaz de programación porque está sujeta a cambios.

---

## Marcas registradas y marcas de servicio

Los siguientes términos son marcas comerciales o marcas registradas de International Business Machines Corporation en Estados Unidos o en otros países:

IBM el logotipo de IBM AIX CICS DB2 DB2 Universal Database IBMLink IMS MQSeries MVS OS/390 WebSphere z/OS

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

MMX, Pentium y ProShare son marcas comerciales o marcas registradas de Intel Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas registradas basadas en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicio de otros.



WebSphere Partner Gateway Enterprise Edition y Advanced Edition, versión 6.1.

---

# Índice

## A

- Acción, definición 8
- Actividad, definición 8
- administrador del concentrador
  - descripción 1
- Alertas
  - añadir contacto a alerta existente 37
  - búsqueda de alertas 60
  - crear alerta basada en suceso 35
  - crear alerta basada en volumen 33
  - criterios de búsqueda 61
  - criterios de búsqueda, Socios 60
  - descripción 32, 60
  - eliminar alerta 61
  - inhabilitar alerta 61
  - ver o editar contactos y detalles de alerta 60
- Análisis de documentos
  - criterios de búsqueda 84
  - descripción 83
  - visualización de detalles de procesos y sucesos 85
  - visualización de documentos 84
- Añadir contacto a alerta existente 37
- Asignar
  - miembro de grupo 55
  - permisos de grupo 56
  - usuarios a grupos 30
- atributo AS cifrado 24
- atributo AS firmado 28
- atributos AS
  - AS cifrado 24
  - AS firmado 28
- autenticación de cliente
  - configurar 14
  - SSL entrante 14
  - SSL saliente 18
- autenticación de servidor
  - SSL entrante 13
  - SSL saliente 17

## B

- Buscar
  - alertas 60
  - de mensajes, Visor AS1/AS2 66
  - para procesos de RosettaNet 71
  - sucesos 64

## C

- Cambiar
  - estado de destino 81
- Campos de error
  - errores de validación 76
- Características de Administración de cuentas 53
- Certificado de cliente SSL, definición 11
- Certificado de firma digital, definición 12
- Certificado digital VTP
  - definición 12
- Certificado X.509, definición 11

- certificados
  - firma 24, 27
  - formato, conversión 17
- Certificados
  - alerta de caducidad, crear 36
  - tipos y formatos soportados 11
- certificados de firma
  - entrantes 27
  - salientes 24
- certificados de firma entrantes 27
- certificados de firma salientes 24
- certificados primarios
  - cifrado saliente 21
  - firma digital saliente 24
  - SSL saliente 18
- certificados secundarios
  - cifrado saliente 21
  - firma digital saliente 24
  - SSL saliente 18
- certificados SSL
  - autenticación de cliente, entrante 14
  - autenticación de cliente, saliente 18
  - autenticación de servidor, entrante 13
  - autenticación de servidor, saliente 17
  - entrantes 13
- cifrado
  - habilitar 24
- Cifrado
  - definición 11
- Clave, definición 11
- Clave con firma personal, definición 11
- Clave privada, definición 11
- Clave pública, definición 11
- Códigos de resultado
  - Servidor web 88
- Códigos de resultado de servidor web 88
- Cola, eliminar documentos de 80
- Comunidad de concentrador
  - descripción 1
- Conexiones FTP
  - informe 95
- Consola de comunidad
  - uso 3
  - usuarios 1
  - visualización 5
- Contactos
  - descripción 31, 58
  - detalles 59
  - eliminar contacto 59
  - valores 55, 59
  - ver o editar detalles de contacto 58
- Crear
  - alerta basada en suceso 35
  - alerta basada en volumen 33
  - alerta de caducidad de certificado 36
  - Informe de volumen de documentos 86
  - nuevo grupo 28
  - nuevo usuario 29
  - pasarelas 7
- Criterios de búsqueda
  - alertas 60, 61

Criterios de búsqueda (*continuación*)  
Análisis de documentos 84  
FA retrasados de EDI 91  
Informe de volumen de documentos 87  
Transacción rechazada de EDI 93  
Visor AS1/AS2 67  
Visor de documentos 74  
Visor de RosettaNet 71  
Visor de sucesos 65

## D

depuración, sucesos 3  
Depurar sucesos 64  
Descifrado  
definición 11  
destino  
cambiar el estado 81  
eliminar 80  
ver detalles 81  
ver documentos en cola 80  
ver la lista 78  
destino predeterminado  
ejemplo de establecimiento 51  
Destino predeterminado  
editar 54  
seleccionar 54  
ver 54  
destinos  
directorio de archivos 45  
FTP 42  
FTP Scripting 48, 49  
FTPS 47  
HTTP 40  
HTTPS 41  
JMS 44  
predeterminados 51  
SMTP 43  
transportes soportados 39  
valores 54  
ver lista 53  
ver o editar detalles de destino 53  
destinos FTP 42  
destinos JMS 44  
destinos SMTP 43  
Detalles, ver destino 81  
Detalles de paquete  
Visor AS1/AS2 68  
Direcciones  
descripción 38, 62  
editar 62  
suprimir 62  
valores 62  
Documento  
detalles, Visor de documentos 74  
valores de proceso, Visor de documentos 75  
Documentos  
eliminar de la cola 80  
ver en cola 80  
Documentos en cola, ver 80  
Documentos sin formato  
ver 72  
DUNS+4 7

## E

Editar  
contactos y detalles de alerta 60  
detalles de contacto 58  
detalles de destino 53  
detalles de grupo 56  
dirección 62  
Eliminación de documentos de la cola 80  
Eliminar  
alerta 61  
contacto 59  
Errores de validación  
ver 76  
Estadísticas de FTP  
informe 95  
Estado, cambiar destino 81  
Estados de documento  
definiciones 83  
Informe de volumen de documentos 86  
Exportar  
Informe de volumen de documentos 87

## F

FA retrasados de EDI  
criterios de búsqueda 91  
informe 92  
firma digital  
habilitar 28  
Firma digital, definición 11

## G

Grupos 55  
asignación de usuarios a 30  
crear 28  
descripción 55  
permisos, ver editar asignar 56  
suprimir 56  
valores 55  
ver miembros de grupo 55  
ver o editar detalles de grupo 56

## H

Habilitar alerta 61  
Herramientas  
Análisis de documentos 83  
descripción 83  
Informe de volumen de documentos 86  
Probar conexión de socio 87

## I

Iconos 2  
Impresión de informes  
Informe de volumen de documentos 87  
Informe  
Conexiones FTP 95  
Estadísticas de FTP 95  
FA retrasados de EDI 92  
Transacción rechazada de EDI 94  
Informe de volumen de documentos  
crear 86  
criterios de búsqueda 87

Informe de volumen de documentos (*continuación*)

- descripción 86
- estados de documento 86
- exportar 87
- impresión 87

Inhabilitar alerta 61

Iniciar sesión en la consola 5

## M

mandatos

- FTP 48

mandatos FTP 48

mensaje Certificado revocado o caducado 24

mensaje No se ha encontrado ningún certificado de cifrado  
válido 24

## N

números de ID de formato libre 7

números DUNS 7

## O

opción Validar certificados SSL de cliente 15

## P

Paquete, definición 8

Pasarelas

- crear 7

- descripción 53

Perfil del socio

- descripción 6

- editar 6

- valores 7

- ver 6

planificación basada en agenda

- destino de scripts FTP 50

planificación basada en intervalos

- destino de scripts FTP 50

posibilidades B2B, descripción 7

Probar conexión de socio

- Códigos de resultado de servidor web 88

- descripción 87

- valores 88

Protocolo, definición 8

puntos de configuración

- destinos 51

## S

script bcgClientAuth.jacl

- configuración de la autenticación de cliente 14

scripts FTP

- destinos 48

- mandatos permitidos en 48

Sin repudio, definición 11

socio

- descripción 1

socio externo

- descripción 1

socio interno

- descripción 1

SSL entrante

- autenticación de cliente 14

- autenticación de servidor 13

SSL saliente

- autenticación de cliente 18

- autenticación de servidor 17

Sucesos

- búsqueda de 64

- criterios de búsqueda 65

Suprimir

- dirección 62

- grupo 56

## T

Terminar sesión en la consola 5

tipo de documento, definición 8

Tipo de suceso Aviso 64

Tipo de suceso Crítico 64

Tipo de suceso Error 64

Tipo de suceso Información 64

Tipos de suceso 64

- descripciones 64

Transacción rechazada de EDI

- criterios de búsqueda 93

- informe 94

transportes

- destino, proporcionado por el sistema 39

## U

Usuarios

- asignar a grupos 30

- crear nuevo usuario 29

- descripción 29, 56

- valores 57

## V

Valores

- Contactos 55, 59

- destinos 54

- Direcciones 62

- Perfil del socio 7

- Probar conexión de socio 88

- Visor de documentos 67, 68, 74, 75

Ver

- contactos y detalles de alerta 60

- detalles de contacto 58

- detalles de destino 53

- detalles de grupo 56

- lista de destinos 53

- permisos de grupo 56

Visor AS1/AS2 72

- búsqueda de mensajes 66

- criterios de búsqueda 67

- descripción 66

- detalles de paquete 68

- visualización de detalles de mensaje 67

Visor de documentos

- criterios de búsqueda 74

- descripción 72

- detalles de documento 74

- valores 67, 68, 74, 75

- valores de proceso de documento 75

- Visor de RosettaNet
  - búsqueda de procesos 71
  - criterios de búsqueda 71
  - descripción 70
  - proceso de documentos, detalles 72
  - visualización de detalles de procesos 71
- Visor de sucesos 24
  - criterios de búsqueda 65
  - descripción 63
  - visualización de detalles de suceso 65
- Visores
  - descripción 63
  - Visor AS1/AS2 66
  - Visor de documentos 72
  - Visor de RosettaNet 70
  - Visor de sucesos 63
- Visualización
  - detalles de destino 81
  - detalles de documento 75
  - detalles de mensaje, Visor AS1/AS2 67
  - detalles de proceso de documentos, Visor de RosettaNet 72
  - Detalles de procesos de RosettaNet 71
  - detalles de procesos y sucesos, Análisis de documentos 85
  - detalles de suceso, Visor de sucesos 65
  - documentos
    - Análisis de documentos 84
  - documentos en cola 80
  - documentos sin formato 75
  - Documentos sin formato 72
  - errores de validación 76
  - lista de destinos 78
  - sucesos 75
- Visualizar consola 5







Impreso en España