IBM WebSphere Partner Gateway Enterprise e Advanced Editions

Guia do Parceiro

Versão 6.1.1

IBM WebSphere Partner Gateway Enterprise e Advanced Editions

Guia do Parceiro

Versão 6.1.1

Nota!
Antes de utilizar estas informações e o produto suportado por elas, leia as informações em "Avisos" na página 101.

27 de Março de 2008

Esta edição aplica-se à Versão 6.1.1, Release 1, Modificação 1, do IBM(TM) WebSphere(TM) Partner Gateway Advanced Edition (5724-L68) e Enterprise Edition (5724-L69), e a todos os releases e modificações subseqüentes, até que seja indicado de outra forma em novas edições.

Para enviar seus comentários sobre este documento, envie um e-mail para doc-comments@us.ibm.com. Esperamos receber os seus comentários.

Quando o Cliente envia seus comentários, concede direitos não-exclusivos à IBM para usá-los ou distribuí-los da maneira que achar conveniente, sem que isso implique em qualquer compromisso ou obrigação para com o Cliente.

Índice

Sobre este Manual

O IBM WebSphere Partner Gateway é um sistema de processamento de documento eletrônico utilizado para gerenciar uma comunidade comercial B2B (Business-to-Business). O B2B foi desenvolvido nos últimos anos para ajudar as empresas a conduzir diversos tipos de transações automáticas (por exemplo, ordens de compra e faturas) de forma rápida, conveniente e econômica.

Este guia fornece aos parceiros da comunidade todas as informações que são necessárias para configurar o console e para executar as tarefas diárias.

Público-Alvo

As partes envolvidas em uma comunidade de hub ou negócio do IBM WebSphere Partner Gateway são o parceiro interno, o administrador do hub e os parceiros externos. Cada uma dessas partes possui usuários administrativos com diferentes níveis de privilégios. Além disso, os usuários administrativos incluem usuários comuns com privilégios específicos de acesso ao console.

Convenções Tipográficas

Este documento utiliza as seguintes convenções tipográficas:

Convenção	Descrição
`Fonte Monoespaçada`	O texto nesta fonte indica o texto que você digita, valores para argumentos ou opções de comando, exemplos e códigos de exemplo ou informações que o sistema imprime na tela (texto de mensagem ou avisos).
Negrito	O texto em negrito indica controles da interface gráfica com o usuário (por exemplo, nomes de botões on-line, nomes de menus e opções de menu) e títulos das colunas em tabelas e texto.
Itálico	O texto em itálico indica ênfase, títulos de manuais, novos termos e termos definidos no texto, nomes de variáveis ou letras do alfabeto utilizadas como letras.
`Fonte Monoespaçada em Itálico`	O texto em fonte monoespaçada em itálico indica nomes de variáveis dentro do texto de fonte monoespaçada.
Texto Colorido Sublinhado	O texto colorido sublinhado indica uma referência cruzada. Clique no texto para ir para o objeto da referência.
Texto em um Contorno Azul	(Apenas em arquivos PDF) Um contorno azul em torno do texto indica uma referência cruzada. Clique no texto contornado para ir para o objeto da referência. Essa convenção é o equivalente para arquivos PDF da convenção "Texto colorido sublinhado" incluída nesta tabela.
{INSTALL DIR}	Representa o diretório onde o produto está instalado.
UNIX:/Windows:	Os parágrafos que iniciam com um desses termos indicam notas listando diferenças do sistema operacional.
" "(Aspas)	(Apenas em arquivos PDF) As aspas circundam referências cruzadas para outras seções do documento.
{ }	Em uma linha de sintaxe, as chaves circundam um conjunto de opções a partir das quais é necessário escolher uma e apenas uma.

`[ ]`	Em uma linha de sintaxe, os colchetes circundam parâmetros opcionais.
`...`	Em uma linha de sintaxe, as reticências indicam uma repetição do parâmetro anterior. Por exemplo, `option[,...]` significa que é possível inserir várias opções separadas por vírgulas.
`< >`	Os colchetes angulares circundam elementos variáveis de um nome para distingui-los um do outro. Por exemplo, <*server_name* ><*connector_name*>tmp.log.
`\, /`	As barras invertidas (\) são utilizadas como separadores de componentes nos caminhos de diretório em instalações do Windows. Para instalações UNIX, substitua barras (/) por barras invertidas.

Documentos Relacionados

O conjunto completo de documentação disponível com este produto inclui informações abrangentes sobre como instalar, configurar, administrar e utilizar o WebSphere Partner Gateway Enterprise e Advanced Editions.

É possível fazer download da documentação ou lê-la on-line diretamente no seguinte site:

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

Nota: Informações importantes sobre este produto podem estar disponíveis nos Technotes e Flashes de Suporte Técnico emitidos após a publicação deste documento. Elas podem ser localizadas no Web site de Suporte do WebSphere Partner Gateway:

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

Selecione a área de componentes de interesse e procure a seção Technotes e Flashes.

Novidades neste Release

Esta seção descreve os novos recursos do IBM WebSphere Partner Gateway.

Novidades no Release 6.1.1

O WebSphere Partner Gateway 6.1.1 suporta os seguintes novos recursos:

- Nos releases anteriores, o suporte de autenticação básica estava disponível apenas para mensagens de serviços da Web. Este recurso agora está estendido a todos os protocolos. A recomendação para a autenticação básica é o uso da conexão HTTP segura, isto é, HTTPS em vez de HTTP.
- Além de assinar e criptografar, o suporte para compactação e descompactação é fornecido para mensagens RNIF.
- O suporte é fornecido para a validação do SOAP Body e SOAP Envelope. Além disso, é possível desenvelopar um SOAP Envelope.
- O tempo limite máximo síncrono e as conexões máximas síncronas podem ser controlados localmente para todos os receptores HTTP.
- O Servidor FTP é integrado ao WebSphere Partner Gateway para suportar o protocolo AS3, o Destino de Script FTP, o Receptor de Script FTP, o receptor e o destino FTP / FTPS.
- O documento de erro pode ser enviado ao parceiro inicial, parceiro de recepção ou ambos. O fluxo de documentos de erro pode ser configurado no console do WebSphere Partner Gateway e pode ser enviado no formato do WebSphere Partner Gateway ou no formato de serviços da Web.
- O desempenho do arquivador foi melhorado.
- O suporte é fornecido para vários parceiros internos.
- É possível reenviar vários documentos de entrada e saída simultaneamente.
- O suporte para o modo FIPS é fornecido. O produto pode ser configurado para executar no modo FIPS ou modo padrão.
- As funcionalidades Excluir e Whereused são fornecidas para Destino, Mapas de Validação, Definições de Documentos, Interações e Usuários.
- O suporte à compressão de arquivos grandes é fornecido para documentos AS2 e AS3.
- O suporte é fornecido para a criptografia e assinatura.
- As dependências dos tipos de configuração para a migração também incluem os códigos de eventos e as notificações de alertas. Além disso, a funcionalidade de migração de parceiros foi aprimorada para fornecer suporte para as definições de importação/exportação dos eventos alertáveis.
- O suporte é fornecido para fazer upload de vários certificados. O novo assistente está incluído no console, para fazer upload e configurar certificados.
- O produto agora suporta o AIX 6.1, RHEL 5 (32 e 64 bits), SLES 10 (64 bits) e o Windows Server 2003 64 bits.

Novidades no Release 6.1

O WebSphere Partner Gateway V6.1 suporta os seguintes recursos novos:

- Novos protocolos comerciais: suporte para AS3, SOAP com anexos, CIDX, e ebXML Message Service (ebMS) 2.0

- O suporte aprimorado para documentos XML customizados inclui melhor organização, suporte completo de expressão XPath, campos de procura, atributos definidos pelo usuário e suporte síncrono.
- Novo suporte IPv6 e Script de FTP avançado para suportar AS3
- Reorganização dos atributos de Definição de Documento.
- Novos atributos de Definição de Documento para uso com Saídas de Usuário.
- Irrecusabilidade configurável por tipo de documento e nível do parceiro de negócio.
- O visualizador de documento possui campos de procura adicionais definidos pelo usuário.
- Melhor suporte de Visualizador AS com base em status de retorno MDN
- Assistente de Configuração do EDI e Assistente de Importação do EIF (anteriormente entregue no pacote de Suporte do GA02)
- Novo nó de notificação de alerta para enviar notificações para todos os parceiros relacionados (parceiros de origem e de destino) ou todos os contatos inscritos, o que reduz a configuração de alertas.
- Permissões de reenvio e gateway agora disponíveis a outros usuários além do administrador hubadmin
- Novo grupo de usuários para permitir que vários usuários tenham a capacidade de ser administradores do hub.
- Suporte LDAP para autenticação de logon.
- Uso do WebSphere Application Server para efetuar login e rastrear componentes do WebSphere Partner Gateway
- Os dados de configuração do arquivo de propriedades agora são localizados centralmente e gerenciados pelo WebSphere Partner Gateway Console
- O WebSphere MQ não é mais um produto pré-requisito; O suporte do WebSphere Platform Messaging agora é utilizado para comunicações internas
- Arquivo seletivo baseado no parceiro e/ou tipo de documento
- Migração da configuração do WebSphere Partner Gateway exportando e importando definições de uma instância do WebSphere Partner Gateway para outra instância.
- Uma opção de instalação simplificada da máquina única (modo simples).
- Implementação de rede do WebSphere Application Server agora utilizada para várias implementações de máquina ativando o armazenamento em cluster e gerenciamento de infra-estrutura central.
- Suporte para uso do WebSphere Process Server, Versão 6.1 como um sistema de integração de backend

Notas:

1. A API administrativa com base em XML está reprovada na versão 6.1.
2. O WebSphere Partner Gateway, Versão 6.1 não suporta o algoritmo RC5.

Capítulo 1. Introdução

Comunidade de hub

A comunidade de hub do IBM WebSphere Partner Gateway consiste em três entidades conectadas a um hub central para a troca de documentos comerciais em tempo real: administrador do hub e parceiros interno e externo.

Administrador do hub

O administrador do hub é uma empresa responsável por gerenciar a operação diária da comunidade de hub. O administrador do hub mantém a infra-estrutura de hardware e software da comunidade de hub em uma base 24 x 7. As responsabilidades incluem:

- Resolver problemas e reparar erros.
- Assegurar que a comunidade de hub seja configurada apropriadamente para todos os parceiros.
- Auxiliar na configuração de novos parceiros para a comunidade de hub.
- Planejar estrategicamente o crescimento futuro, assegurando a máxima eficiência da operação da comunidade de hub.

A função do administrador do hub pode ser contratada em uma outra empresa dentro da comunidade de hub ou o parceiro interno que adquiriu o WebSphere Partner Gateway pode ser escolhido para desempenhar a função do administrador do hub.

Parceiro Interno

O parceiro interno é a empresa primária que controla os trabalhos dentro da comunidade de hub. Essa empresa é responsável pela aquisição e construção da comunidade de hub, incluindo a definição de processos comerciais eletrônicos transacionados entre eles e os parceiros externos.

O parceiro interno também pode escolher se deseja ser o administrador do hub.

Parceiros Externos

Os parceiros externos são as empresas que efetuam negócios com o parceiro interno por meio da comunidade de hub. Os parceiros devem concluir um processo de configuração para se conectarem à comunidade de hub. Depois de conectados, eles podem trocar documentos comerciais eletrônicos com o parceiro interno.

Ícones do Community Console

Os ícones na tabela a seguir são exclusivos do WebSphere Partner Gateway Community Console

Tabela 1. Ícones do Community Console

Ícone	Nome do Ícone
	Reduzir

Tabela 1. Ícones do Community Console (continuação)

Ícone	Nome do Ícone
	Copiar
	Criar função. A função não está ativa
	Os dados estão contidos
	Ativar
	Excluir
	Exibir documento não-processado
	Documento em progresso
	O processamento do documento falhou
	Processamento do documento bem-sucedido
	Fazer download do mapa
	Editar
	Editar valores de atributos
	Desativar edição
	Editar valores de atributos de RosettaNet
	Expandir
	Exportar informações
	Exportar relatório
	Destino desativado
	Ocultar critérios de procura
	Modificar
	Não há dados contidos
	Abrir calendário
	Ativar/desativar a classificação de documentos
	Pausar
	Imprimir
	Entrada requerida
	Iniciar

Tabela 1. Ícones do Community Console (continuação)

Ícone	Nome do Ícone
	Parar processamento; o documento está em progresso, opção do usuário para pedir que o servidor pare o processamento do documento.
	Fluxo de dados síncrono; nenhum ícone é exibido para transações assíncronas.
	Fazer upload do mapa
	Visualizar detalhes
	Visualizar configuração de atributo de uma Definição de Documentos
	Visualizar sistema de Ajuda
	Visualizar membros
	Visualizar documento original
	Visualizar permissões
	Visualizar as associações de grupo
	Visualizar erros de validação
	Utilizado onde

Utilizando o Community Console

Depois de configurar o WebSphere Partner Gateway, você utilizará duas ferramentas de console regularmente: o Visualizador de Eventos e a Análise de Documento.

Utilize o Visualizador de Eventos, no módulo Visualizadores, para pesquisar eventos. A maioria dos documentos é reenviada várias vezes, portanto, quando um documento falha e gera um alerta, trata-se de algo que é necessário investigar e corrigir para evitar que falhas semelhantes ocorram futuramente.

É possível localizar um evento específico e, em seguida, pesquisar por que ele ocorreu. O Visualizador de Eventos permite procurar eventos por hora, data, tipo, nome e local. A administração do hub também pode procurar parceiro, IP de origem e IP de evento.

Nota: Nem todos os usuários terão acesso aos eventos de depuração.

Os dados que o Visualizador de Eventos gera ajuda você a identificar o evento e o documento que o criou. É possível, também, visualizar o documento não processado, que identifica o campo, o valor e o motivo do erro.

A segunda ferramenta mais usada é a Análise de Documentos, um recurso no módulo Ferramentas. Ela é utilizada para descobrir quantos documentos foram recebidos, quantos estão em andamento, quantos foram concluídos, quantos

obtiveram falhas e os que foram bem-sucedidos. Utilize essa ferramenta para fazer drill down em documentos específicos, que falharam ao descobrir por que obtiveram falha.

O módulo Administrador de Conta do console é utilizado principalmente quando você está configurando o WebSphere Partner Gateway e, por conseguinte, para manutenção.

Capítulo 2. Configurando o Ambiente do WebSphere Partner Gateway

Esta seção descreve as tarefas que o Parceiro Externo deve executar para preparar o WebSphere Partner Gateway para os usuários e ambiente do Parceiro Externo.

Para configurar o WebSphere Partner Gateway para a sua empresa, é necessário executar as atividades a seguir a partir do Community Console, na ordem mostrada.

1. "Efetuando Login no Community Console"
2. "Verificando o Perfil do Parceiro" na página 6
3. "Criando um Destino" na página 7
4. "Revisando os Recursos B2B" na página 7
5. "Fazendo o Upload de Certificados Digitais" na página 9
6. "Criando Grupos de Console" na página 28
7. "Criando Usuários" na página 29
8. "Configurando o Usuário do FTP" na página 30
9. "Criando Informações de Contato" na página 31
10. "Criando Alertas e Incluindo Contatos" na página 31
11. "Criando um Novo Endereço" na página 38

Efetuando Login no Community Console

Esta seção fornece as etapas para exibir e efetuar login no Community Console. A resolução de tela recomendada é 1024 x 768.

Nota: O WebSphere Partner Gateway Community Console requer que o suporte a cookies esteja ativado para manter informações sobre a sessão. Nenhuma informação pessoal é armazenada no cookie, que expira quando o navegador é fechado.

1. Abra um navegador da Web e digite a seguinte URL para exibir o console:

   http://<*nome_do_host*>.<*domínio*>:58080/console (não-seguro)

   https://<*nome_do_host*>.<*domínio*>:58443/console (seguro)

   Onde <*nome_do_host*> e <*domínio* são o nome e o local do computador que hospeda o componente Community Console.

   Nota: Essas URLs assumem que são utilizados os números de portas padrão. Se você alterou os números de portas padrão, substitua os números padrão pelos valores especificados.

Na maioria dos casos, o administrador do hub enviou a você o nome do usuário, a senha inicial e o nome de login da empresa que será utilizado para efetuar login no Community Console. Você precisará dessas informações para o procedimento a seguir. Caso não as tenha recebido, entre em contato com o administrador do hub.

Para efetuar login no Community Console (estas instruções são tanto para Parceiros Internos quanto para Parceiros Externos):

1. Digite o **Nome do Usuário** da sua empresa.

2. Digite a **Senha** da sua empresa.
3. Digite o **Nome de Login da Empresa**, por exemplo, IBM.
4. Clique em **Login**. Ao efetuar login pela primeira vez, será necessário criar uma nova senha.
5. Digite uma nova senha e, em seguida, digite-a novamente na caixa de texto Confirmar.
6. Clique em **Salvar**. O sistema exibe a tela de entrada inicial do console.

Nota: Se o WebSphere Partner Gateway estiver configurado utilizando LDAP, então, é necessário inserir o Nome do Usuário e a Senha do LDAP. O Nome de Login da Empresa não é relevante neste cenário, então você não será solicitado a inserir esta informação. Além disso, o sistema não solicitará a alteração da senha.

Verificando o Perfil do Parceiro

Utilize o recurso Parceiros Administradores de Conta para visualizar e editar as informações que identificam a empresa para o sistema.

Os parceiros podem editar todos os atributos em seus perfis, exceto o Nome de Login da Empresa. Os parceiros também podem inserir e remover IDs Comerciais, ID de E-mail relacionado a todo ID Comercial e os endereços IP. Os endereços IP ou nomes de hosts podem ser digitados para os seguintes Modos de Operação: Produção, Teste, Gerenciador do CPS e Parceiro do CPS.

Este recurso também inclui uma opção para a reconfiguração de todas as senhas de usuários. Se você achar que as senhas dos usuários estão comprometidas, utilize esse recurso.

Visualizando e Editando o Perfil do Parceiro

1. Clique em **Administrador de Conta** >**Perfis** > **Parceiro**.
2. Clique no ícone Meu Perfil para editar. O sistema exibe a tela Detalhe do Parceiro.
3. Edite o seu perfil, como requerido (alguns valores não podem ser editados). Para obter uma explicação dos valores, consulte a Tabela 2 na página 7.

Tabela 2. Valores nas Telas dos Parceiros

Valor	Descrição
Nome de Login da Empresa	Identifica o parceiro para o sistema. Máximo de 15 caracteres. Os seguintes caracteres especiais não podem ser incluídos:, . ! # ; : \ / & ?. Os parceiros não podem editar esse valor.
Nome de Exibição do Parceiro	O nome que o parceiro quer que seja exibido para a comunidade do hub. Máximo de 30 caracteres.
Tipo de Parceiro	Tipo de Parceiro - parceiro externo ou parceiro interno. Os parceiros podem editar este valor apenas se a propriedade bcg.allow.partner.type.edit estiver configurada como True. Por padrão, este valor é configurado como False.
Status	Ativado ou Desativado. Se o status estiver desativado, o Parceiro não estará visível no critério de procura e nas listas drop-down.
Tipo de Fornecedor	Identifica a função do parceiro, por exemplo, Fabricante ou Distribuidor do Contrato.
Web Site	Identifica o Web site do parceiro.
ID de Negócio	Número DUNS, DUNS+4 ou Freeform que o sistema utiliza para o roteamento. É possível incluir números de IDs comerciais adicionais. • Os números DUNS devem devem ter nove dígitos. • Os números DUNS+4 devem ter treze dígitos. • Os números de IDs Freeform aceitam até 60 caracteres alfanuméricos, numéricos e especiais. **Nota:** Os IDs comerciais de EDI precisam ser prefixados com quaisquer qualificadores utilizados no documento EDI. O formato é o Qualificador de EDI mais ″-″ e o ID. Por exemplo, um EDI X12 utilizando DUNS será 01-123456789.
ID de E-mail	O ID de E-mail válido de cada ID Comercial. É possível incluir números de IDs de E-mail adicionais para cada ID Comercial. Este campo não é visível se não houver IDs Comerciais.
Endereço IP ou Nome do Host	• Modo de Operação, por exemplo, Parceiro do CPS. • Endereço IP ou nome do host do parceiro.

4. Clique em **Salvar**.

Criando um Destino

Você deve criar e manter um destino padrão. Se não fizer isso, você não poderá criar conexões. Consulte o Capítulo 3, “Criando Destinos”, na página 39 para obter detalhes sobre como criar destinos.

Revisando os Recursos B2B

Nota: Em instalações menores, este processo pode ser executado pela administração de hub.

Utilize este recurso para visualizar e editar os recursos B2B predefinidos que abrangem o hub e para ativar os recursos B2B locais adicionais, se necessário.

Um recurso B2B identifica um tipo específico de processo de negócios que pode ser trocado entre você e outros membros da comunidade. O recurso B2B ou os recursos de processamento de documentos são definidos com as definições de tipo

de documento. Uma definição de tipo de documento fornece ao sistema todas as informações necessárias para receber, processar e rotear documentos entre os membros da comunidade.

Cada recurso consiste de até cinco diferentes definições de tipo de documento:

Pacote. Identifique os formatos de pacotes de documentos utilizados para transmitir documentos pela Internet. Por exemplo, RNIF, AS1, AS2 e AS3.

Protocolo. Identifica a estrutura e a localização das informações no documento. O sistema precisa dessas informações para processar e rotear o documento.

Tipo de Documento. Identifica o processo comercial que será processado entre o parceiro interno e seus parceiros externos.

Atividade. A função comercial que o processo executa.

Ação. Os documentos individuais que constituem um processo de negócios completo. Os documentos são processados entre o parceiro interno e o parceiro externo.

Cada definição de tipo de documento contém atributos (ou seja, informações) que definem a funcionalidade das definições. Um atributo é uma parte das informações associada a um tipo de documento específico. O sistema utiliza essas informações para várias funções, como, por exemplo, para a validação de documentos ou para a verificação de criptografia.

Revisando e Editando os Recursos B2B:

1. Clique em **Administrador de Conta** > **Perfis** >**Recursos B2B**. O sistema exibe a tela Recursos B2B.
   - Se uma pasta aparecer ao lado de um pacote e o status Ativado aparecer na coluna Ativado, a administração de hub terá ativado este recurso para você.
   - Uma marca de seleção abaixo de Definir Origem ou Definir Destino significa que você poderá utilizar este recurso naquela função (ou seja, como a origem, o destino ou ambos).
   - O ícone de rolagem Criar, abaixo de Definir Origem ou Definir Destino, indica que o recurso não está ativado nessa função (ou seja, como a origem, o destino ou ambos).
   - A coluna Ativado exibe o status do pacote: Ativado ou Desativado.

   Nota: O recurso de destino, de origem ou ambos deve ser definido antes de ser ativado.
2. Defina o recurso para iniciar (**Definir Origem**), receber (**Definir Destino**) ou iniciar e receber o contexto do tipo de documentos. Em um PIP 2-way, Definir Origem e Definir Destino são iguais para todas as ações, não importando se o pedido origina-se de um parceiro e a confirmação correspondente origina-se de outro.
3. Defina o recurso para iniciar (**Definir Origem**), receber (**Definir Destino**) ou iniciar e receber para cada definição de tipo de documentos de nível inferior.
4. Clique no ícone Editar para visualizar, e se desejar, alterar as definições de tipo de documentos de nível inferior (por exemplo, Protocolo ou Tipo de Documentos). Pode-se, também, alterar os atributos das definições de tipo de documento (por exemplo, Hora de Execução ou Contagem de Novas Tentativas). Ao utilizar esta tela pela primeira vez, os atributos serão definidos

no nível global. Entretanto, você poderá redefini-los no nível local, se desejado. A definição de um atributo no nível local substituirá a definição global em seu ambiente, mas não a alterará.

- Se você fizer uma alteração em qualquer nível, ela será propagada para todos os níveis inferiores.
- É possível selecionar e editar uma pasta individual abaixo de um pacote, se desejado. Esse tipo de alteração não será propagado para os níveis inferiores.
- É possível substituir a opção incorporada “selecionar tudo” desmarcando-a de baixo para cima.
- Os sinais, por exemplo, as confirmações de recebimento, são específicos do RosettaNet. Há três sinais em cada ação: Confirmação de Recebimento, Exceção Geral e Exceção de Confirmação de Recebimento. É possível definir atributos para os sinais.
- Irrecusabilidade obrigatória
- ID Comercial do AS

Se você tiver alterado um atributo, clique em **Salvar**.

Fazendo o Upload de Certificados Digitais

Um certificado digital é uma credencial de identificação on-line, similar à licença ou ao passaporte de um driver. Um certificado digital pode ser utilizado para identificar um indivíduo ou uma organização.

Assinaturas digitais são cálculos baseados em um documento eletrônico que utiliza criptografia de chave pública. Através deste processo, a assinatura digital é vinculada ao documento que está sendo assinado, bem como ao assinante, e não pode ser reproduzida. Com a passagem da conta de assinatura digital federal, as transações eletrônicas assinadas digitalmente têm o mesmo valor legal que as transações assinadas à mão.

O WebSphere Partner Gateway utiliza certificados digitais para verificar a autenticidade das transações de documentos comerciais entre o parceiro interno e os parceiros externos. Eles também são utilizados para a criptografia e para a decriptografia.

É possível especificar um certificado primário e um secundário para documentos de saída para assegurar que a troca de documentos não seja interrompida. O primário é utilizado em todas as transações. O secundário é utilizado se o primário estiver expirado ou revogado.

Os certificados digitais são transferidos por upload e identificados durante o processo de configuração.

Se for detectado que um certificado expirará ou será anulado, ele será desativado e refletivo como tal no console. Se o certificado primário expirar ou for anulado, ele será desativado e o certificado secundário será definido como o primário. Um evento será gerado quando for detectado que um certificado expirará ou será anulado.

A opção Uso de Certificado está disponível com base no tipo de certificado selecionado. No perfil Operador de Hub, a opção Uso de Certificado pode ser definida para Assinatura Digital ou certificado Cliente SSL. No perfil do parceiro, a opção Uso de Certificado pode ser definida para certificado Criptografia. Se o mesmo certificado deve ser utilizado para finalidades diferentes, para Assinatura

Digital e Criptografia no perfil Operador de Hub, ele precisa ser carregado duas vezes, uma para a Assinatura Digital e, novamente, para o certificado Criptografia. No entanto, se o certificado for utilizado para Assinatura Digital e Cliente SSL, as caixas de opções correspondentes podem ser definidas na mesma entrada de certificado.

Esses certificados também podem ser carregados duas vezes, uma para Assinatura Digital e, novamente, para Cliente SSL. Se forem, o mesmo padrão deve ser seguido para os certificados secundários. Por exemplo, se os certificados primários foram carregados como certificados diferentes para Assinatura Digital ou Cliente SSL, os certificados secundários também deverão ser carregados como entradas de certificado diferentes (embora o certificado possa ser o mesmo).

Para construção e validação completas de certpath, é solicitado que você faça o upload de todos os certificados contidos na cadeia de certificados. Por exemplo, se a cadeia de certificados contiver certificados A -> B -> C -> D, em que A -> B significa que A é o emissor de B e, em seguida, os certificados A, B e C deverão ser transferidos por upload como certificados raízes. Se um dos certificados não estiver disponível, o certpath não será construído e a transação não será bem-sucedida. Os certificados CA podem ser obtidos nos Repositórios de Certificados mantidos pelas Autoridade de Certificação ou no parceiro que forneceu o certificado. Certificados raízes e intermediários podem ser transferidos por upload apenas no perfil Operador de Hub.

Nota: Antes de você poder utilizar os procedimentos nas seções a seguir, os certificados devem ser carregados para o sistema. Para obter mais informações sobre como carregar os certificados, consulte o *Hub Configuration Guide*.

É possível criar alertas de expiração de certificados que informam a data em que o certificado está prestes a expirar. Para obter informações adicionais, consulte "Criando Alertas e Incluindo Contatos" na página 31. Os certificados expirados são salvos no banco de dados do IBM WebSphere Partner Gateway; eles não podem ser excluídos do sistema.

Termos do Certificado

CA (Autoridade de Certificação). Uma autoridade que emite e gerencia credenciais de segurança e chaves públicas para a criptografia de mensagens. Quando um indivíduo ou empresa solicita um certificado digital, uma CA solicita a uma RA (Autoridade de Registro) a verificação das informações fornecidas. Se a RA verificar as informações enviadas, a CA emitirá um certificado.

Exemplos de uma CA incluem VeriSign e Thawte.

Certificado Digital. Um certificado digital é a versão eletrônica de uma carteira de identidade. Ele estabelece sua identificação quando você executa transações B2B pela Internet. Os certificados digitais são obtidos de uma CA (Autoridade de Certificação) e consistem de:

- A chave pública do seu par de chaves pública e privada.
- Informações que o identificam.
- A assinatura digital de uma entidade confiável (CA) que atesta a validade do certificado.

Assinatura Digital. Um código digital criado com uma chave privada. As assinaturas digitais permitem que os membros da comunidade de hub autentiquem

as transmissões por meio da verificação de assinatura. Quando você assina um arquivo, um código digital, exclusivo para os conteúdos do arquivo e para a sua chave privada, é criado. Sua chave pública é utilizada para verificar sua assinatura.

Criptografia. Um método de mesclar informações para torná-las ilegíveis para qualquer pessoa, exceto para o destinatário, que deverá decriptografar as informações para lê-las.

Decriptografia. Um método de decriptografar informações para que elas se tornem legíveis novamente. A chave privada do destinatário é utilizada para a decriptografia.

Chave. Um código digital usado para criptografar, assinar, decriptografar e verificar arquivos. As chaves podem ser pares de chaves, uma chave pública e uma chave privada.

Não-recusa. Para evitar a negação de compromissos ou ações anteriores. Para transações eletrônicas B2B, as assinaturas digitais são utilizadas para validar o remetente e a data e a hora da transação. Isso impede que as partes envolvidas aleguem que a transação não foi autorizada ou não era válida.

Chave privada. A parte secreta de um par de chaves. Essa chave é utilizada para assinar e para decriptografar informações. Somente você terá acesso à sua chave privada. A sua chave privada também é usada para gerar uma assinatura digital exclusiva, com base no conteúdo do documento.

Chave pública. A parte pública de um par de chaves. Essa chave é usada para criptografar informações e verificar assinaturas. Uma chave pública pode ser distribuída para outros membros da comunidade de hub. Conhecer a chave pública de um indivíduo não significa descobrir a chave privada correspondente.

Chave auto-assinada. Uma chave pública que foi assinada pela chave privada correspondente para testar a propriedade.

Certificado X.509. Um certificado digital usado para provar a identidade e a propriedade da chave pública em uma rede de comunicação. Ele contém o nome do remetente (ou seja, a CA), as informações de identificação do usuário e a assinatura digital do remetente.

O seu certificado identifica sua organização e o período de tempo pelo qual o certificado é válido.

Tipos de Certificados e Formatos Suportados

Todos os certificados devem estar no formato DER ou ASCII PEM (Privacy Enhanced Mail). Os certificados podem ser convertidos de um formato a outro.

Há vários tipos de certificados:

- **Certificado Cliente SSL (parceiros externos e parceiro interno)**. Um certificado de transporte. Se o seu transporte de saída for HTTPS, você precisará de um certificado Cliente SSL. Na maioria dos casos, o certificado Cliente SSL deve ser assinado por uma CA. Se o certificado for usado em um ambiente de teste, ele poderá ser auto-assinado.

  É necessário fazer upload do certificado no WebSphere Partner Gateway por meio do console e enviar uma cópia do certificado ao Operador de Hub.

- **Certificado de Servidor SSL.** Ativa a autenticação do servidor SSL. A CA do certificado de servidor SSL precisa ser trocada entre os parceiros.
- **Certificado de criptografia (parceiros externos e parceiro interno)**. Se os membros da comunidade de hub criptografarem arquivos, a parte de chave pública do certificado de criptografia terá que ser enviada para os membros da comunidade de hub. A parte de chave privada correspondente do certificado de criptografia deve ser transferida por upload, por meio do console, para o nível do operador de hub. É necessário fazer upload da parte pública do certificado do parceiro no WebSphere Partner Gateway por meio do console e enviar uma cópia dele para o Operador de Hub.
- **Certificado de assinatura digital (parceiros externos e parceiro interno)**. Se os membros da comunidade de hub assinarem os documentos, a parte pública do certificado de assinatura deverá ser transferida por upload para o hub no nível do parceiro como um certificado de assinatura. Se o gerenciador de hub precisar assinar os documentos que ele está enviando para os membros da comunidade de hub, você deverá enviar a parte pública do certificado do gerenciador de hub para os membros da comunidade de hub. O certificado de assinatura do hub precisa ser transferido por upload por meio do console para o Operador de Hub.
- **Certificado VTP (parceiro interno)**. Este certificado é utilizado pelo Gerenciador de Documentos do WebSphere Partner Gateway para o recurso Simulador de Parceiro Externo. Esse certificado é copiado para o sistema de arquivos em vez de ser transferido por upload através do console.

  Os certificados VTP copiados para o sistema de arquivos estão ativos para todos os parceiros criados por meio do console. Eles são usados para validar documentos assinados recebidos a partir do Simulador de Parceiro Externo. Além disso, os certificados copiados para o sistema de arquivos não são visíveis através do console.

Autenticação de Servidor e de Cliente SSL

Se a autenticação do cliente não for requerida, deverá ocorrer o seguinte:

- Se o certificado do servidor Web da comunidade de hub for um certificado auto-assinado, os parceiros deverão ter uma cópia desse certificado.
- Se o certificado do servidor da Web da comunidade de hub for de uma Autoridade de Certificação, os parceiros deverão ter uma cópia do certificado raiz e intermediário da CA.

Se a autenticação do cliente for requerida, deverá ocorrer o seguinte:

- Se o certificado do servidor Web da comunidade de hub for um certificado auto-assinado, os parceiros deverão ter uma cópia desse certificado.
- Se o certificado do servidor da Web da comunidade de hub for de uma Autoridade de Certificação, os parceiros deverão ter uma cópia do certificado raiz e intermediário da CA.
- O servidor de destino deve ter uma cópia do certificado do parceiro se ele for auto-assinado e carregado no armazenamento de chaves confiável.
- O servidor de destino deve ter uma cópia do certificado das autoridades de certificação se o certificado for autenticado por uma CA e carregado no armazenamento de chaves confiável.

Nota: Versões anteriores do WebSphere Partner Gateway não suportavam o formato de endereço do IPv6. O WebSphere Partner Gateway 6.1 não suporta esse formato. Certifique-se de que, pelo menos, um dos seus servidores esteja configurado para dar suporte ao formato de endereço do IPv6. A configuração do formato do IPv6 é necessária apenas no servidor.

Configurando Certificados SSL de Entrada

Esta seção descreve como configurar a autenticação de servidor e a autenticação de cliente para os pedidos de conexão de entrada dos parceiros.

Um pedido de entrada é quando o parceiro está enviando um documento ao WebSphere Partner Gateway. Se sua comunidade não estiver utilizando o SSL, não é necessário um certificado SSL de entrada ou de saída.

Nota: Para o FTPS de entrada, o WebSphere Partner Gateway utiliza um Servidor FTP fornecido pelo cliente, então qualquer configuração SSL de entrada é direcionada a este produto de Servidor FTP específico que o cliente está utilizando.

Etapa 1: Obter um Certificado SSL: O WebSphere Application Server utiliza o certificado SSL ao receber os pedidos de conexão dos parceiros através do SSL. Esse é o certificado que o Receptor apresenta para identificar o hub ao parceiro. Este certificado do servidor pode ser auto-assinado ou pode ser assinado por um CA. Na maioria dos casos, será utilizado um certificado de CA para aumentar a segurança. É possível utilizar um certificado auto-assinado em um ambiente de teste. Utilize o iKeyman ou o console administrativo do WebSphere Application Server para gerar um certificado ou um par de chaves. Consulte a documentação disponível da IBM para obter mais informações sobre o uso do iKeyman ou o console administrativo do WebSphere Application Server.

Após gerar o certificado e o par de chaves, utilize o certificado para o tráfego de SSL de entrada para todos os parceiros. Se você possuir vários Receptores ou Consoles, copie o armazenamento de chaves resultante para cada instância. Se o certificado for gerado utilizando o console administrativo do WebSphere Application Server, a chave e o certificado podem ser importados em outro armazenamento de chaves em outro servidor, utilizando o console administrativo do WebSphere Application Server. Se o certificado for auto-assinado, forneça este certificado aos parceiros. Para obter este certificado, utilize o iKeyman para extrair o certificado público para um arquivo.

Gerando um Certificado Auto-assinado: Se você irá utilizar certificados de servidor auto-assinados, utilize o seguinte procedimento.

1. Inicie o utilitário iKeyman, que está localizado em */<dir_de_Instalação_do_WAS>*/bin. Se esta é sua primeira vez utilizando o iKeyman, exclua o certificado "fictício" que reside no armazenamento de chaves.
2. Abra o armazenamento de chaves do Receptor ou do Console utilizando o iKeyman, e utilize o iKeyman para gerar um certificado auto-assinado e um par de chaves para o armazenamento de chaves do Receptor ou do Console.
3. Utilize iKeyman para extrair o certificado a um arquivo, contendo a chave pública.

   Salve o armazenamento de chaves em um arquivo JKS, PKCS12 ou JCEKS.
4. Distribua o certificado aos parceiros. O método preferencial para a distribuição é enviar o certificado em um arquivo compactado protegido por senha, por e-mail. Seus parceiros devem chamar e solicitar a senha para o arquivo compactado.
5. Utilizando o console administrativo do WebSphere Application Server, configure o novo certificado na Configuração do SSL e nas configurações para o

receptor e o console. É possível fazer isso selecionando o alias do novo certificado no armazenamento de chaves na Configuração para cada nó ou servidor.

Obtendo um Certificado Gerado por CA: Se você irá utilizar um certificado assinado por um CA, utilize o seguinte procedimento.

1. Inicie o utilitário iKeyman, localizado no diretório */<dir_de_instalação_do_WAS>*/bin.
2. Utilize iKeyman para gerar um pedido de certificado e um par de chaves para o Receptor.
3. Submeta um CSR (Certificate Signing Request) a um CA.
4. Ao receber o certificado assinado do CA, utilize iKeyman para colocar o certificado assinado no armazenamento de chaves.
5. Distribua o certificado de CA a todos os parceiros, se necessário.
6. Utilizando o console administrativo do WebSphere Application Server, configure o novo certificado na Configuração do SSL e nas configurações para o receptor e o console. É possível fazer isso selecionando o alias do novo certificado no armazenamento de chaves na Configuração para cada nó ou servidor.

   Nota: O console administrativo do WebSphere Application Server também pode ser utilizado para concluir as etapas anteriores.

Etapa 2: Autenticar os Clientes: Se desejar autenticar os parceiros que enviaram documentos, desempenhe as etapas nesta seção.

Instalando o Certificado Cliente: Para a autenticação de cliente, utilize o seguinte procedimento:

1. Obtenha o certificado do parceiro.
2. Se o certificado for auto-assinado, instale o certificado no armazenamento de confiança, utilizando o iKeyman ou o console administrativo do WebSphere Application Server.
3. Se o certificado for emitido por CA, inclua os certificados de CA relacionados no armazenamento de confiança relacionado, utilizando o iKeyman ou o console administrativo do WebSphere Application Server.

Nota: Ao incluir mais parceiros à comunidade de hub, é possível utilizar o iKeyman ou o console administrativo do WebSphere Application Server, para incluir os certificados ao armazenamento de confiança. Se um parceiro deixar a comunidade, é possível utilizar o iKeyman ou o console administrativo do WebSphere Application Server para remover os certificados do parceiro do armazenamento de confiança.

Configurando a Autenticação de Cliente: Após instalar os certificados, configure o WebSphere Application Server para utilizar a autenticação de cliente, executando o script do utilitário bcgClientAuth.jacl.

1. Navegue ao seguinte diretório: */<Dir_do_Produto>*/bin
2. Para ativar a autenticação de cliente, chame o script da seguinte maneira:

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

   Nota: Para desligar a autenticação de cliente, chame o script da seguinte maneira:

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

O servidor bcgreceiver precisa ser reiniciado para que estas alterações sejam efetivadas A autenticação de cliente também pode ser ativada utilizando o console administrativo do WebSphere Application Server. Um valor ″Suportado″ indica que o servidor solicitará o certificado cliente, mas, se o certificado cliente não estiver disponível, a autenticação inicial SSL ainda pode ser estabelecida. Um valor ″Necessário″ indica que o certificado cliente deve ser enviado. Caso contrário, a autenticação inicial SSL falhará.

Validando o Certificado do Cliente: Há um recurso adicional que pode ser utilizado com a autenticação de cliente SSL. Este recurso é ativado através do Console da Comunidade. Para HTTPS, o WebSphere Partner Gateway verifica os certificados em oposição aos IDs Comerciais nos documentos de entrada. Para utilizar este recurso, crie o perfil do parceiro, importe o certificado cliente e sinalize-o como SSL.

1. Importe o certificado cliente.
   a. Clique em **Admin da Conta > Perfis > Parceiro** e procure o perfil do parceiro.
   b. Clique em **Certificados**.
   c. Clique em **Carregar Certificado**.
   d. Clique em **Procurar** e navegue ao diretório no qual o certificado foi salvo.
   e. Selecione **Cliente SSL** como o tipo de certificado.
   f. Digite uma descrição do certificado (que é necessário).
   g. Altere o status para **Ativado**.
   h. Se desejar selecionar um modo de operação diferente de **Produção** (o padrão), selecione-o na lista.
   i. Clique em **Concluir**.
2. Atualize o destino do cliente.
   a. Clique em **Admin da Conta > Perfis > Parceiro** e procure o perfil do parceiro.
   b. Clique em **Destinos**.
   c. Selecione o destino HTTPS criado anteriormente. Se você ainda não criou o destino HTTPS, consulte “Configurando um Destino HTTPS” na página 41.
   d. Clique no ícone **Editar** para editar o destino.
   e. Selecione **Sim** for **Validar o Certificado Cliente SSL**.
   f. Clique em **Salvar**.

Configurando o Armazenamento de Chaves e o Truststore Separados para o Receptor e o Console: Por padrão, o WebSphere Partner Gateway versão 6.1 utiliza o armazenamento de chaves e o truststore comum para o Receptor e o Console. No entanto, é possível configurar o armazenamento de chaves e o truststore separados para o receptor e o console no modo de instalação distribuído.

Para configurar o armazenamento de chaves e o truststore, crie e configure um armazenamento de chaves e um truststore separados para o Receptor e o Console. Além disso, crie configurações SSL separadas. As configurações SSL podem ser definidas no nível do Cluster ou do Servidor. A definição da configuração SSL no nível do cluster é mais fácil, visto que a configuração é, então, aplicável a todos os servidores no cluster e não é necessário configurar cada servidor separadamente.

Definindo a Configuração SSL no Nível do Cluster: Ao definir a configuração SSL com o novo armazenamento de chaves e truststore no nível do cluster, não deve haver nenhuma configuração SSL definida no nível do servidor. Se houver uma configuração SSL definida no nível do servidor, então, a configuração SSL no nível do cluster não será utilizada; em vez disso, o configurado para o servidor será utilizado.

Siga estas etapas para configurar a configuração SSL para bcgconsoleCluster:

1. Crie um armazenamento de chaves para o cluster do console. O armazenamento de chaves deve ser criado no escopo do cluster bcgconsole, navegando para **Segurança > Certificado SSL e Gerenciamento de Chaves > Armazenamentos de Chaves e Certificados**.
2. Crie um truststore para o cluster do Console. O truststore deve ser criado no escopo do cluster bcgconsole, navegando para **Segurança > Certificado SSL e Gerenciamento de Chaves > Armazenamentos de Chaves e Certificados**.
3. Crie uma configuração SSL para o cluster do console no escopo do cluster do console, navegando para **Segurança > Certificado SSL e Gerenciamento de Chaves > Configurações SSL**. Configure o armazenamento de chaves e o truststore criados nas etapas anteriores. Atualize os alias de certificados na lista de alias de certificados, clicando em **Obter Alias de Certificados** e selecione o alias necessário a ser utilizado para a autenticação de servidor. Configure o gerenciador de confiança como **IbmPKIX**.
4. Defina esta configuração SSL em bcgconsoleCluster, substituindo a configuração SSL herdada. Atualize os alias de certificados clicando em **Atualizar Alias de Certificados** e configure o alias a ser utilizado para a autenticação de servidor.
5. Reinicie o bcgconsoleCluster.

Siga estas etapas para configurar a configuração SSL para bcgreceiverCluster:

1. Crie um armazenamento de chaves para o cluster do receptor. O armazenamento de chaves deve ser criado no escopo do cluster bcgreceiver, navegando para **Segurança > Certificado SSL e Gerenciamento de Chaves > Armazenamentos de Chaves e Certificados**.
2. Crie um truststore para o cluster do Receptor. O truststore deve ser criado no escopo do cluster bcgconsole, navegando para **Segurança > Certificado SSL e Gerenciamento de Chaves > Armazenamentos de Chaves e Certificados**.
3. Crie uma configuração SSL para o cluster do receptor no escopo do cluster do receptor, navegando para **Segurança > Certificado SSL e Gerenciamento de Chaves > Configurações SSL** e configure o armazenamento de chaves e o truststore criados nas etapas anteriores. Obtenha os alias de certificados clicando em **Obter Alias de Certificados** e selecionando o alias necessário a ser utilizado para a autenticação de servidor. Configure o gerenciador de confiança como **IbmPKIX**.
4. Defina esta configuração SSL em bcgreceiverCluster, substituindo a configuração SSL herdada. Atualize os alias de certificados clicando em **Atualizar Alias de Certificados** e configure o alias a ser utilizado para a autenticação de servidor.
5. Reinicie o bcgreceiverCluster.

Para obter mais informações sobre o trabalho com os armazenamentos de chaves, a configuração SSL e as configurações de terminais, consulte a seção *Protegendo os Aplicativos e seu Ambiente da Documentação do WebSphere Application Server.*

Nota:

Configurando o NodeDefaultTrustStore no NodeDefaultSSLSetting no Modo Distribuído: Esta configuração deve ser feita para o modo distribuído simples. Mas, isso também é aplicável ao modo totalmente distribuído, se o armazenamento de chaves e o truststore comuns devem ser utilizados para o Receptor e o Console. Se um nó estiver federado em uma célula, os certificados do signatário do nó são incluídos ao CellDefaultTrustStore. Por padrão, NodeDefaultSSLSetting refere-se ao CellDefaultTrustStore como o truststore. Para o Receptor e o Console do WebSphere Partner Gateway, utilizar certificados de signatário de outros nós pode não ser desejado. Para utilizar um truststore dedicado para os nós nos quais o WebSphere Partner Gateway está instalado, NodeDefaultTrustStore pode ser configurado no NodeDefaultSSLSettings como o truststore.

As etapas para fazer esta alteração são as seguintes:

1. No console administrativo do WebSphere Application Server, navegue para **Segurança > Certificado SSL e Gerenciamento de Chaves > Gerenciar as Configurações de Segurança dos Terminais > <nome_do_nó> > Configurações SSL > NodeDefaultSSLSettings**.
2. No campo Nome do Armazenamento de Confiança, selecione **NodeDefaultTrustStore**.

   Nota: Assegure-se de que NodeDefaultTrustStore está configurado para o truststore que deseja utilizar; por exemplo, bcgSecurityTrust.jks.
3. Clique em **Aplicar**.
4. Na página seguinte do Console, clique em **Salvar** para atualizar as alterações na configuração principal.
5. Reinicie os servidores neste nó.

Nota: Para o modo totalmente distribuído, as alterações acima devem ser feitas para todos os nós contendo os servidores bcgreceiver e bcgconsole. Para o modo distribuído simples, essas alterações devem ser feitas a todos os nós contendo bcgserver.

Incluindo Certificados do Signatário para trust.p12 se NodeDefaultTrustStore Estiver Configurado para o Nó Contendo os Servidores WebSphere Partner Gateway: Atualmente, NodeDefaultTrustStore refere-se ao trust.p12. Se o NodeDefaultTrustStore estiver configurado para o nó contendo os servidores WebSphere Partner Gateway, bcgSecurityTrust.jks não será utilizado. Os certificados do signatário do bcgSecurityTrust.jks precisam ser incluídos ao trust.p12, conforme necessário.

Configurando os Certificados SSL de Saída

Um pedido de saída é quando o WebSphere Partner Gateway está enviando um documento a um parceiro. Se sua comunidade não estiver utilizando o SSL, não é necessário um certificado SSL de entrada ou de saída.

Etapa 1: Autenticar o Servidor: Quando o SSL está sendo utilizado para enviar documentos de saída aos parceiros, o WebSphere Partner Gateway solicita um certificado do lado do servidor dos parceiros. O mesmo certificado CA pode ser utilizado para vários parceiros. O certificado deve estar no formato X.509 DER.

Nota: É possível converter o formato com o utilitário iKeyman. Siga estas etapas para utilizar o iKeyman para converter o formato:

1. Inicie o iKeyman.

2. Crie um novo armazenamento de chaves em branco ou abra um armazenamento de chaves existente.
3. No Conteúdo do Banco de Dados de Chaves, selecione **Certificados do Signatário**.
4. Inclua o certificado ARM utilizando a opção **Incluir**.
5. Extraia o mesmo certificado como os dados DER binários utilizando a opção **Extrair**.
6. Feche o iKeyman.

Instale o certificado auto-assinado do parceiro no perfil Operador de Hubs. Se o certificado foi assinado por um CA e o certificado raiz de CA e outros certificados que fazem parte da cadeia de certificados não estiverem instalados no perfil Operador de Hubs, instale os certificados no perfil Operador de Hubs.

1. Clique em **Admin da Conta > Perfis > Certificados** para exibir a página Lista de Certificados.

   Certifique-se de ter efetuado login no Community Console como o Operador de Hubs ou como Parceiro Interno.
2. Clique em **Carregar PKCS12**.

   Nota: O arquivo PKCS12 transferido por upload deve conter apenas uma chave privada e o certificado associado. É possível também fazer upload do certificado e da chave privada formatada PKCS#8 separadamente.
3. Selecione **Cliente SSL** como o tipo de certificado.
4. Digite uma descrição do certificado (que é necessário).
5. Altere o status para **Ativado**.
6. Clique em **Procurar** e navegue ao diretório no qual o certificado foi salvo.
7. Selecione o certificado e clique em **Abrir**.
8. Insira a senha.
9. Se desejar selecionar um modo de operação diferente de **Produção** (o padrão), selecione-o na lista.
10. Você possui dois certificados SSL, indique se esse é o certificado primário ou secundário, selecionando **Primário** ou **Secundário** na lista **Uso do Certificado**.
11. Clique em **Upload** e, em seguida, clique em **Salvar**.

Nota: Não é necessário desempenhar as etapas anteriores, se o certificado CA já estiver instalado.

Etapa 2: Autenticar os Clientes: Se a autenticação de cliente SSL for necessária, o parceiro solicitará, por sua vez, um certificado do hub. Utilize o Community Console para importar o certificado no WebSphere Partner Gateway. É possível gerar o certificado utilizando iKeyman. Se o certificado for um certificado auto-assinado, é necessário que seja fornecido ao parceiro. Se for um certificado assinado pelo CA, o certificado raiz de CA deve ser fornecido aos parceiros, para que possa ser incluído aos certificados confiáveis.

É possível ter mais de um certificado SSL. Um é o certificado primário, utilizado por padrão. O outro é um certificado secundário, utilizado se o certificado primário expirar.

Utilizando um Certificado Auto-assinado: Se você irá utilizar um certificado auto-assinado, utilize o seguinte procedimento.

1. Inicie o utilitário iKeyman.
2. Utilize o iKeyman para gerar um certificado auto-assinado e um par de chaves.
3. Utilize iKeyman para extrair o certificado a um arquivo, contendo a chave pública.
4. Distribua o certificado aos parceiros. O método preferencial para a distribuição é enviar o certificado em um arquivo compactado protegido por senha, por e-mail. Seus parceiros devem chamar e solicitar a senha para o arquivo compactado.
5. Utilize o iKeyman para exportar o certificado auto-assinado e o par de chaves privadas no formato de um arquivo PKCS12.
6. Instale o certificado auto-assinado e a chave através do Community Console.
   a. Clique em **Admin da Conta > Perfis > Certificados** para exibir a página Lista de Certificados.

      Certifique-se de ter efetuado login no Community Console como o Operador de Hub.
   b. Clique em **Carregar PKCS12**.

      Nota: O arquivo PKCS12 transferido por upload deve conter apenas uma chave privada e o certificado associado. É possível também fazer upload do certificado e da chave privada formatada PKCS#8 separadamente.
   c. Selecione **Cliente SSL** como o tipo de certificado.
   d. Digite uma descrição do certificado (que é necessário).
   e. Altere o status para **Ativado**.
   f. Clique em **Procurar** e navegue ao diretório no qual o certificado foi salvo.
   g. Selecione o certificado e clique em **Abrir**.
   h. Insira a senha.
   i. Se desejar selecionar um modo de operação diferente de **Produção** (o padrão), selecione-o na lista.
   j. Você possui dois certificados SSL, indique se esse é o certificado primário ou secundário, selecionando **Primário** ou **Secundário** na lista **Uso do Certificado**.
   k. Clique em **Upload** e, em seguida, clique em **Salvar**.

Se estiver fazendo upload dos certificados primários e secundários para a autenticação de cliente SSL e a assinatura digital e estiver fazendo upload dos certificados primários como duas entradas separadas, certifique-se de que os certificados secundários correspondentes sejam transferidos por upload como duas entradas diferentes.

Utilizando um Certificado Assinado por CA: Se você irá utilizar um certificado assinado por um CA, utilize o seguinte procedimento:

1. Utilize iKeyman para gerar um pedido de certificado e um par de chaves para o Receptor.
2. Submeta um CSR (Certificate Signing Request) a um CA.
3. Ao receber o certificado assinado do CA, utilize iKeyman para colocar o certificado assinado no armazenamento de chaves.
4. Distribua o certificado CA de assinatura a todos os parceiros.

Utilizando os Certificados para Ativar a Criptografia

Esta seção descreve os certificados de criptografia.

Criando e Instalando os Certificados de Criptografia de Entrada

Este certificado é utilizado pelo hub para decriptografar arquivos criptografados recebidos dos parceiros. O hub utiliza a chave privada para decriptografar os documentos. A criptografia é utilizada para evitar que todos que não sejam emissores e destinatários pretendidos visualizem os documentos em transição.

Observe a seguinte restrição importante sobre a recepção das mensagens AS2 criptografadas dos parceiros. Se um parceiro envia uma mensagem AS2 criptografada, mas utiliza o certificado errado, a decriptografia falha. Nenhum MDN é retornado ao parceiro para indicar a falha, entretanto. Para que seu parceiro receba os MDNs nesta situação, crie uma conexão com o parceiro com a seguinte definição do documento:

- Pacote: **AS** para o Pacote: **Nenhum**
- Protocolo: **Binário** para o Protocolo: **Binário**
- Tipo de Documento: **Binário** para o Tipo de Documento: **Binário**

A conexão criada deve ser a conexão AS para Nenhum, isto é, a criação de uma conexão através da ativação do recurso AS B2B em um parceiro e do recurso None B2B em outro. Assegure-se de que o gateway de origem no lado do AS é um gateway SMTP (no caso de AS1), gateway HTTP (no caso de AS2) ou gateway FTP (no caso AS3), configurado para o endereço MDN. Assim, o MDN de falha de decriptografia é enviado de volta pelo AS a Nenhuma Conexão Binária.

Etapa 1: Obter um Certificado:

Gerando um Certificado Auto-assinado: Se você irá utilizar um certificado auto-assinado, utilize o seguinte procedimento.

1. Inicie o utilitário iKeyman.
2. Utilize o iKeyman para gerar um certificado auto-assinado e um par de chaves.
3. Utilize iKeyman para extrair o certificado a um arquivo, contendo a chave pública.
4. Distribua o certificado aos parceiros. Eles são necessários para importar o arquivo no produto B2B para utilizar como um certificado de criptografia. Aconselhe-os a utilizá-lo quando desejarem enviar arquivos criptografados ao parceiro interno. Se seu certificado for assinado pelo CA, forneça também o certificado CA.
5. Utilize o iKeyman para salvar o certificado auto-assinado e o par de chaves privadas no formato de um arquivo PKCS12.
6. Navegue para **Perfil** > **{Operador de Hub/parceiro interno}** > **certificados** > **criar novo certificado.**
7. No drop-down **A que Parceiro este(s) Certificado(s) Pertence(m)**, selecione o parceiro ao qual deseja associar o certificado recém transferido por upload.
8. Clique em **Procurar** para localizar parceiros específicos ou de um subconjunto.
9. Clique em **Procurar** ao lado de **Local do Certificado** para fazer upload do certificado.
10. Clique em **Avançar**.
11. Em Fornecer Detalhes do Certificado, insira as seguintes informações do certificado: **Certificado em Folha**, **Certificado CA Raiz** Ou **Certificado CA Intermediário**.

12. Associe este certificado à **Criptografia**.
13. Em **Uso do Certificado**, selecione **Primário** ou **Secundário**.
14. Selecione **ativado** ou **desativado** em **Status** com base em se ativar ou desativar um certificado após fazer upload.
15. Selecione o **Modo de Operação**.
16. Clique em **Concluir** para salvar as alterações e concluir o assistente.

Utilizando um Certificado Assinado por CA: Se você irá utilizar um certificado assinado por um CA, utilize o seguinte procedimento:

1. Inicie o utilitário iKeyman.
2. Utilize iKeyman para gerar um pedido de certificado e um par de chaves para o Receptor.
3. Submeta um CSR (Certificate Signing Request) a um CA.
4. Ao receber o certificado assinado do CA, utilize iKeyman para colocar o certificado assinado no armazenamento de chaves.

Etapa 2: Distribuir o Certificado: Distribua o certificado CA de assinatura a todos os parceiros.

Instalando os Certificados de Criptografia de Saída

O certificado de criptografia de saída é utilizado quando o hub envia documentos criptografados aos parceiros. O WebSphere Partner Gateway criptografa os documentos com as chaves públicas dos parceiros e os parceiros decriptografam os documentos com suas chaves privadas.

O parceiro pode ter mais de um certificado de criptografia. Um é o certificado primário, utilizado por padrão. O outro é um certificado secundário, utilizado se o certificado primário expirar.

Etapa 1: Obter um Certificado do Parceiro: Obtenha o certificado de criptografia do parceiro. O certificado deve estar no formato X.509 DER. Observe que o WebSphere Partner Gateway suporta apenas os certificados X5.09.

Etapa 2: Instalar um Certificado do Parceiro: Instale o certificado através do Community Console sob o perfil do parceiro, concluindo o procedimento a seguir:

1. Navegue para **Perfil** > **Parceiro Externo** > **certificados** > **Carregar Certificados**.
2. Na página **Selecionar Parceiro, Local do Arquivo, Senha** do assistente, insira os seguintes valores:
   - **A qual parceiro este(s) certificado(s) pertence**: Selecione o parceiro para associar o certificado recém transferido por upload. Clique em Procurar para localizar um parceiro ou subconjunto de parceiros específico. Se o parceiro for um Operador de Hub ou Parceiro Interno, insira o local do certificado, local da chave privada e senha (OU) Forneça o truststore ou o armazenamento de chaves com senha. Para o Parceiro Externo, forneça o local do certificado (OU) forneça o local do armazenamento de confiança contendo a cadeia de certificados.
   - **Local do Certificado**: Clique em **Procurar** para selecionar o local do certificado público.
3. Clique em **Avançar** para ir para a página **Detalhes do Certificado** do assistente.
4. Na página **Detalhes do Certificado** do assistente, insira os seguintes detalhes do certificado:

- **Nome do Certificado em Folha** - O nome do certificado em folha. O nome do campo depende se o certificado é um certificado em folha, certificado de CA raiz ou um certificado de CA intermediário.
- **Descrição** - A descrição do Certificado de Folha.
- **Tipo de Certificado** - Associe este certificado à criptografia.
- **Uso do Certificado** - Associe um uso para o certificado. Os valores são Primário e Secundário.
- **Modo de Operação** - Digite o modo de operação.
- **Status** - Selecione ativado ou desativado com base em se ativar ou desativar um certificado após fazer upload. O botão Avançar é ativado somente se o certificado estiver ativado.
- **Gerenciamento do Conjunto** - É possível associar um certificado a um conjunto existente ou criar um novo conjunto. Se o certificado for um certificado secundário, só poderá ser associado a um conjunto existente. Você pode associar o certificado a qualquer conjunto, para um parceiro interno, ao tipo de criptografia ou, para o parceiro externo, com um tipo SSL (Autenticação do cliente de entrada) ou Assinatura (Verificar).

5. Clique em **Avançar** para ir à página Configurar do assistente. Se o certificado for primário, não é necessário criar conjuntos e associar o certificado a um conjunto e à conexão participante. Se você selecionou a caixa de opção **Criar novo conjunto**, então a página **Criar Novo Conjunto** do assistente será aberta. Caso contrário, a página **Incluir no Existente** do assistente será aberta. Se o arquivo contiver uma chave privada do parceiro interno ou o certificado público do parceiro externo, utilizando para SSL / Assinatura Digital, então, é possível clicar em **Concluir**.
6. Na página **Criar Novo Conjunto** do assistente, digite os detalhes do novo conjunto. Para certificados primários, não é necessário criar conjuntos e associá-los ao certificado. Insira os seguintes valores:
   - **Nome do Conjunto** - O nome do conjunto.
   - **Descrição** - A descrição do conjunto.
   - **Status** - Selecione ativado ou desativado. Se estiver desativado, o botão **Avançar** não será ativado.
   - **Tornar configurações padrão** - Selecione esta caixa de opção se desejar que este conjunto seja o padrão.
7. Na página **Incluir no Conjunto Existente** do assistente, selecione os conjuntos a serem incluídos no certificado. Insira os seguintes valores:
   - **Selecione na lista de conjuntos disponíveis para obter o tipo de certificado selecionado** - Na lista, selecione os conjuntos a serem incluídos ao certificado.
   - **Tornar configurações padrão** - Selecione esta caixa de opção se desejar que este conjunto seja o padrão.
8. Na página **Criar Novo Conjunto** ou **Incluir no Conjunto Existente**, clique em **Avançar** para ir para a página **Configurações Padrão** do assistente. O botão **Avançar** só será ativado se o status do conjunto estiver ativado.
9. Selecione **ativado** ou **desativado** em **Status** com base em se ativar ou desativar um certificado após fazer upload.

   Nota: Se você selecionou a caixa de opção **Tornar conjunto padrão** na página anterior (Criar Novo Conjunto ou Incluir no Conjunto Existente), então deverá associar o conjunto a um modo de operação. Isso exibirá os usos do certificado nos modos de operação. A criptografia será desativada

para os parceiros internos. O Cliente SSL e Assinatura Digital não estarão ativadas para parceiros externos.

10. Clique em **Avançar** para ir à página Configuração do assistente. No caso de você clicar em **Concluir** e haver certificados de CA raiz ou intermediários ausentes, será solicitado que faça o upload. Se você clicar em ″Sim″ na janela do prompt, a primeira página do assistente será aberta. Clique em **Cancelar** se desejar fazer upload em uma etapa posterior.
11. Na página Configuração do assistente, insira os seguintes valores:

    Nota: A página Configuração exibe uma lista de usos de certificados (conjuntos) nos modos de operação. O nome do conjunto atual é preenchido para todos, mas você pode reconfigurá-lo.

    - **Do Parceiro** - Este campo será pré-ocupado pelo valor do parceiro interno.
    - **Para Parceiro** - Este drop-down é pré-ocupado com a lista de todos os parceiros externos. Você também pode selecionar o valor ″Todos″ para incluir todos os parceiros externos.
    - **Do Pacote** - No lista drop-down, selecione os objetos de Definições de Fluxo de Documentos do pacote do parceiro interno.
    - **Para Pacote** - Na lista, selecione os objetos de Definições de Fluxo de Documentos do pacote do parceiro externo.
12. Clique em **Incluir Mais Conexões** se desejar associar o conjunto para outras conexões participantes.
13. Clique em **Incluir Certificado Secundário** para incluir um certificado secundário ao conjunto atual.
14. Clique em **Concluir** para fazer upload do Certificado. No caso de haver certificados de CA raiz ou intermediários ausentes, será solicitado que o upload seja efetuado. Se você clicar em ″Sim″ na janela do prompt, a primeira página do assistente será aberta. Clique em **Cancelar** na janela do prompt para fazer upload em um estágio posterior.

Repita esta etapa se o parceiro possui um segundo certificado de criptografia.

Etapa 3: Instalar Todos os Certificados Emitidos por CA: Se o certificado foi assinado por um CA e o certificado raiz de CA e outros certificados que fazem parte da cadeia de certificados não estiverem instalados no perfil Operador de Hubs, instale os certificados seguindo os procedimentos a seguir:

Nota: Não é necessário desempenhar esta etapa se o certificado emitido por CA já estiver instalado.

1. Navegue para **Perfil** > **Operador de Hub**> **certificados** > **criar novo certificado.**
2. No drop-down **A que Parceiro este(s) Certificado(s) Pertence(m)**, selecione o parceiro ao qual deseja associar o certificado recém transferido por upload.
3. Clique em **Procurar** para localizar parceiros específicos ou de um subconjunto.
4. Clique em **Procurar** ao lado de **Local do Armazenamento de Confiança (ou) de Armazenamento de Chaves**.
5. Para o certificado e o armazenamento de confiança, insira **Senha**.
6. No armazenamento de confiança, insira o **Tipo de armazenamento de chaves** e clique em **Avançar**.
7. Na página **Selecionar o certificado de entidade para fazer upload** do assistente, selecione um certificado a ser carregado.

Nota: Ao carregar certificados utilizando um armazenamento de confiança que possui mais de um certificado, **Selecionar a lista de certificados de CA raiz e intermediário a serem transferidos por upload** é preenchido com todos os certificados. É possível também fazer upload de vários certificados.

8. Clique em **Concluir**.

Etapa 4: Ativar a Criptografia: Ative a criptografia no pacote (nível mais alto), parceiro ou nível de conexão (nível mais baixo). Sua configuração pode substituir outras configurações no nível de conexão. O resumo de conexões informará se algum atributo necessário está ausente.

Por exemplo, para alterar os atributos de uma conexão de parceiros, clique em **Admin da Conta > Conexões** e, em seguida, selecione os parceiros. Clique em **Atributos** e, em seguida, edite o atributo (por exemplo, **AS Criptografado**).

Quando a mensagem de erro `Nenhum certificado de criptografia válido foi localizado` é exibida, nem o certificado primário nem o certificado secundário são válidos. Os certificados podem expirar ou podem ter sido anulados. Se os certificados expiraram ou foram revogados, o evento correspondente (`Certificado expirado ou revogado`) também pode ser consultado no Event Viewer. Observe que dois eventos podem estar separados por outros eventos.

Para exibir o Event Viewer, conclua o seguinte:

1. Clique em **Visualizadores > Event Viewer**.
2. Selecione os critérios de procura apropriados.
3. Clique em **Procurar**.

Consulte *WebSphere Partner Gateway Administrator Guide* para obter informações sobre o uso do Event Viewer.

Utilizando os Certificados para Ativar a Assinatura Digital

Criando um Certificado de Assinatura de Saída

O Document Manager utiliza este certificado ao enviar documentos assinados de saída aos parceiros. O mesmo certificado e chave são utilizados para todas as portas e protocolos.

É possível ter mais de um certificado de assinatura digital. Um é o certificado primário, utilizado por padrão. O outro é um certificado secundário, utilizado se o certificado primário expirar.

Gerando um Certificado Auto-assinado: Se você irá utilizar um certificado auto-assinado, utilize o seguinte procedimento.

1. Inicie o utilitário iKeyman.
2. Utilize o iKeyman para gerar um certificado auto-assinado e um par de chaves.
3. Utilize iKeyman para extrair o certificado a um arquivo, contendo a chave pública.
4. Distribua o certificado aos parceiros. O método preferencial para a distribuição é enviar o certificado em um arquivo compactado protegido por senha, por e-mail. Seus parceiros devem chamar e solicitar a senha para o arquivo compactado.
5. Utilize o iKeyman para exportar o certificado auto-assinado e o par de chaves privadas no formato de um arquivo PKCS12.

Instalando os Certificados Auto-assinados de Saída:

1. Navegue para **Perfil** > {**Operador de Hub/Parceiro Interno**} > **certificados** > **Carregar Certificados**.
2. Na página **Selecionar Parceiro, Local do Arquivo, Senha** do assistente, insira os seguintes valores:
   - **A qual parceiro este(s) certificado(s) pertence**: Selecione o parceiro para associar o certificado recém transferido por upload. Clique em Procurar para localizar um parceiro ou subconjunto de parceiros específico. Se o parceiro for um Operador de Hub ou Parceiro Interno, insira o local do certificado, local da chave privada e senha (OU) Forneça o truststore ou o armazenamento de chaves com senha. Para o Parceiro Externo, forneça o local do certificado (OU) forneça o local do armazenamento de confiança contendo a cadeia de certificados.
   - **Chave Privada:** Clique em **Procurar** para selecionar a chave privada do certificado.
   - **Senha:** Se o certificado possui uma senha, insira o valor.
   - **Local do Armazenamento de confiança (ou) do Armazenamento de Chaves:** Clique em **Procurar** para selecionar o local do Armazenamento de chaves. Armazenamento de chaves é um conjunto de chaves privadas juntamente com certificados raiz e de CA confiáveis.
   - **Senha:** Digite a senha para o local do armazenamento de chaves.
   - **Tipo:** Selecione o tipo de Truststore (ou) Armazenamento de Chaves. Os valores disponíveis na lista drop-down são: JKS, JCEKS e PKCS12.
3. Clique em **Avançar** para ir para a página **Detalhes do Certificado** do assistente. A página **Selecionar Entidade Final e Certificados da CA** do assistente será aberta quando você carregar certificados por meio de um truststore que possui mais de um certificado. A lista de certificados disponíveis no truststore é exibida.
4. Na página **Selecionar Certificado da Entidade Final e Certificado de CA** do assistente, insira os seguintes valores:
   - **O armazenamento de chaves contém mais de um certificado de Entidade Final. Selecione o certificado a ser transferido por upload.** - O lista drop-down exibe uma lista de todos os certificados de Entidade Final. Selecione o certificado para fazer upload.
   - **Senha** - Se o armazenamento de chaves possui uma senha, selecione esta caixa de opção e insira a senha na caixa de texto.
   - **Selecione a Lista de Certificados da CA Raiz e Intermediários a serem transferidos por upload** - Na caixa da lista, selecione os certificados da CA Raiz e Intermediários para fazer upload.
5. Clique em **Avançar** para ir para a página **Detalhes do Certificado** do assistente.
6. Na página **Detalhes do Certificado** do assistente, insira os seguintes detalhes do certificado:
   - **Nome do Certificado em Folha** - O nome do certificado em folha. O nome do campo depende se o certificado é um certificado em folha, certificado de CA raiz ou um certificado de CA intermediário.
   - **Descrição** - A descrição do Certificado de Folha.
   - **Tipo de Certificado** - Associe este certificado à criptografia.
   - **Uso do Certificado** - Associe um uso para o certificado. Os valores são Primário e Secundário.
   - **Modo de Operação** - Digite o modo de operação.

- **Status** - Selecione ativado ou desativado com base em se ativar ou desativar um certificado após fazer upload. O botão Avançar é ativado somente se o certificado estiver ativado.
- **Gerenciamento do Conjunto** - É possível associar um certificado a um conjunto existente ou criar um novo conjunto. Se o certificado for um certificado secundário, só poderá ser associado a um conjunto existente. Você pode associar o certificado a qualquer conjunto, para um parceiro interno, ao tipo de criptografia ou, para o parceiro externo, com um tipo SSL (Autenticação do cliente de entrada) ou Assinatura (Verificar).

  Nota: Para o operador do hub, não haverá nenhum gerenciamento de conjuntos. Os certificados serão associados ao conjunto padrão criado.

7. Clique em **Avançar** para ir à página Configurar do assistente. Se o certificado for primário, não é necessário criar conjuntos e associar o certificado a um conjunto e à conexão participante. Se você selecionou a caixa de opção **Criar novo conjunto**, então a página **Criar Novo Conjunto** do assistente será aberta. Caso contrário, a página **Incluir no Existente** do assistente será aberta. Se o arquivo contiver uma chave privada do parceiro interno ou o certificado público do parceiro externo, utilizando para SSL / Assinatura Digital, então, é possível clicar em **Concluir**.
8. Na página **Criar Novo Conjunto** do assistente, digite os detalhes do novo conjunto. Para certificados primários, não é necessário criar conjuntos e associá-los ao certificado. Insira os seguintes valores:
   - **Nome do Conjunto** - O nome do conjunto.
   - **Descrição** - A descrição do conjunto.
   - **Status** - Selecione ativado ou desativado. Se estiver desativado, o botão **Avançar** não será ativado.
   - **Tornar configurações padrão** - Selecione esta caixa de opção se desejar que este conjunto seja o padrão.
9. Na página **Incluir no Conjunto Existente** do assistente, selecione os conjuntos a serem incluídos no certificado. Insira os seguintes valores:
   - **Selecione na lista de conjuntos disponíveis para obter o tipo de certificado selecionado** - Na lista, selecione os conjuntos a serem incluídos ao certificado.
   - **Tornar configurações padrão** - Selecione esta caixa de opção se desejar que este conjunto seja o padrão.
10. Na página **Criar Novo Conjunto** ou **Incluir no Conjunto Existente**, clique em **Avançar** para ir para a página **Configurações Padrão** do assistente. O botão **Avançar** só será ativado se o status do conjunto estiver ativado.
11. Selecione **ativado** ou **desativado** em **Status** com base em se ativar ou desativar um certificado após fazer upload.

    Nota: Se você selecionou a caixa de opção **Tornar conjunto padrão** na página anterior (Criar Novo Conjunto ou Incluir no Conjunto Existente), então deverá associar o conjunto a um modo de operação. Isso exibirá os usos do certificado nos modos de operação. A criptografia será desativada para os parceiros internos. O Cliente SSL e Assinatura Digital não estarão ativadas para parceiros externos.
12. Clique em **Avançar** para ir à página Configuração do assistente. No caso de você clicar em **Concluir** e haver certificados de CA raiz ou intermediários ausentes, será solicitado que faça o upload. Se você clicar em "Sim" na janela

do prompt, a primeira página do assistente será aberta. Clique em **Cancelar** se desejar fazer upload em uma etapa posterior.

13. Na página Configuração do assistente, insira os seguintes valores:

    Nota: A página Configuração exibe uma lista de usos de certificados (conjuntos) nos modos de operação. O nome do conjunto atual é preenchido para todos, mas você pode reconfigurá-lo.

    - **Do Parceiro** - Este campo será pré-ocupado pelo valor do parceiro interno.
    - **Para Parceiro** - Este drop-down é pré-ocupado com a lista de todos os parceiros externos. Você também pode selecionar o valor ″Todos″ para incluir todos os parceiros externos.
    - **Do Pacote** - No lista drop-down, selecione os objetos de Definições de Fluxo de Documentos do pacote do parceiro interno.
    - **Para Pacote** - Na lista, selecione os objetos de Definições de Fluxo de Documentos do pacote do parceiro externo.
14. Clique em **Incluir Mais Conexões** se desejar associar o conjunto para outras conexões participantes.
15. Clique em **Incluir Certificado Secundário** para incluir um certificado secundário ao conjunto atual.
16. Clique em **Concluir** para fazer upload do Certificado. No caso de haver certificados de CA raiz ou intermediários ausentes, será solicitado que o upload seja efetuado. Se você clicar em ″Sim″ na janela do prompt, a primeira página do assistente será aberta. Clique em **Cancelar** na janela do prompt para fazer upload em um estágio posterior.

Se estiver fazendo upload dos certificados primários e secundários para a autenticação de cliente SSL e a assinatura digital e estiver fazendo upload dos certificados primários como duas entradas separadas, certifique-se de que os certificados secundários correspondentes sejam transferidos por upload como duas entradas diferentes.

Obtendo um Certificado Assinado pelo CA: Se você irá utilizar um certificado assinado por um CA, utilize o seguinte procedimento:

1. Inicie o utilitário iKeyman.
2. Utilize iKeyman para gerar um pedido de certificado e um par de chaves para o Receptor.
3. Submeta um CSR (Certificate Signing Request) a um CA.
4. Ao receber o certificado assinado do CA, utilize iKeyman para colocar o certificado assinado no armazenamento de chaves.
5. Distribua o certificado CA de assinatura a todos os parceiros.

Instalando um Certificado de Assinatura de Entrada

O Document Manager utiliza o certificado assinado pelo parceiro para verificar a assinatura do emissor ao receber os documentos. Os parceiros enviam seus certificados auto-assinados no formato X.509 DER para você. Você, por sua vez, instala os certificados dos parceiros através do Community Console, no respectivo perfil do parceiro.

Para instalar o certificado, utilize o seguinte procedimento.

1. Receba o certificado de assinatura X.509 do parceiro no formato DER.
2. Navegue para **Perfil** > **Perfil Externo** > **certificados** > **Carregar Certificados**.
3. Clique em **Procurar** para localizar parceiros específicos ou de um subconjunto.

4. Clique em **Procurar** ao lado de **Local do Certificado** para fazer upload do certificado.
5. Clique em **Avançar** para ir para a página **Detalhes do Certificado** do assistente.
6. Associe este certificado à **Assinatura Digital**.
7. Selecione **ativado** ou **desativado** em **Status** com base em se ativar ou desativar um certificado após fazer upload.
8. Selecione o **Modo de Operação**. Se você é um operador de HUB, não terá a opção de selecionar o **Modo de operação**.
9. Clique em **Concluir** para salvar as alterações e concluir o assistente.
10. Se o certificado for assinado por um CA e o certificado raiz de CA e outros certificados que fazem parte da cadeia de certificados não estiverem instalados no perfil Operador de Hub, instale os certificados agora. Isso é aplicável apenas para Armazenamento de confiança/Armazenamento de chaves.
    a. Clique em **Admin da Conta > Perfis > Certificados** para exibir a página Lista de Certificados.

       Certifique-se de ter efetuado login no Community Console como o Operador de Hub e instale o certificado em seu próprio perfil.
    b. Clique em **Carregar Certificado**.
    c. Selecione **Raiz e Intermediário**.
    d. Digite uma descrição do certificado (que é necessário).
    e. Altere o status para **Ativado**.
    f. Clique em **Procurar** e navegue ao diretório no qual o certificado foi salvo.
    g. Selecione o certificado e clique em **Abrir**.
    h. Clique em **Upload** e, em seguida, clique em **Salvar**.

    Nota: Não é necessário desempenhar a etapa anterior, se o certificado de CA já estiver instalado.
11. Ative a assinatura no pacote (nível mais alto), parceiro ou nível de conexão (nível mais baixo). Sua configuração pode substituir outras configurações no nível de conexão. O resumo de conexões informará se algum atributo necessário está ausente.

    Por exemplo, para alterar os atributos de uma conexão de parceiros, clique em **Admin da Conta > Conexões** e, em seguida, selecione os parceiros. Clique em **Atributos** e, em seguida, edite o atributo (por exemplo, **AS Assinado**).

Criando Grupos de Console

Utilize o recurso Grupo para criar um grupo para um tipo de usuário específico, com privilégios de console específicos. Por exemplo, talvez você queira criar um grupo Testadores para os usuários que precisam testar a conectividade durante o ciclo de testes. Após criar o grupo Testadores, é necessário designar permissões para o grupo com base nos recursos de console aos quais os usuários do grupo devem ter acesso durante o ciclo de testes.

O sistema cria automaticamente os grupos Administrador e Padrão com as configurações de permissões padrão. As configurações de permissão padrão podem ser alteradas por qualquer usuários de grupos de administradores de hub ou pelo grupo de administradores do parceiros.

Aviso: Os grupos Padrão e Administrador são gerados pelo sistema e não podem ser editados ou excluídos. O grupo do Administrador do Hub tem um grupo adicional, Administrador de Hub.

Para criar grupos:

1. Clique em **Administrador de Conta** > **Perfis** > **Grupos**. O sistema exibe a tela Lista do Grupo.
2. Clique em **Criar** no canto superior direito da tela. O sistema exibe a tela Detalhe do Grupo.
3. Digite o **Nome** e a **Descrição** do novo grupo.
4. Clique em **Salvar**. Para incluir grupos adicionais, repita estas etapas.

Criando Usuários

Utilize este recurso para criar perfis de usuário. O sistema utiliza os perfis de parceiros para controlar o acesso ao console, a distribuição de alertas e a visibilidade do usuário.

Um perfil de usuário inclui o nome e as informações de contato do usuário (endereço de e-mail e números de telefones), o status de login (ativado ou desativado), bem como o status de alerta do usuário (ativado ou desativado) e a visibilidade (local ou global). O nome de usuário é exclusivo.

- Se o status de login do usuário for Ativado, o usuário poderá efetuar login no Community Console. Se o status de login do usuário for Desativado, o usuário não poderá efetuar login no Community Console.
- Se o status de alerta do usuário for Ativado, o usuário poderá receber notificações de alerta. Se o status de alerta do usuário for Desativado, o usuário não poderá receber notificações de alerta.
- Se a visibilidade do usuário for Local, o usuário estará visível apenas para sua organização. Se a visibilidade de um usuário for Global, o usuário estará visível para toda a comunidade de hub.

Você também pode gerar automaticamente uma senha para um usuário.

Criando um Novo Usuário

Utilize este recurso para incluir um novo usuário. Após definir seus usuários e grupos, você poderá incluir usuários nos grupos.

1. Clique em **Administrador de Conta** > **Perfis** > **Usuários**. O sistema exibe a tela Lista de Usuários.
2. Clique em **Criar** no canto superior direito da tela. O sistema exibe a tela Detalhes do Usuário.
3. Digite o **Nome do Usuário** (nome de login do usuário).
4. Selecione o **Status** de acordo com o sua intenção de Ativar ou Desativar o acesso desse usuário ao console.
5. Digite o nome do usuário (**Prenome** e **Sobrenome**).
6. Digite o endereço de **E-Mail** que o sistema utilizará para enviar notificações de alerta para o usuário.
7. Digite o **Telefone** e **Números de Faxes** do usuário.
8. Selecione o **Código de Idioma**, **Formatar Código de Idioma** e **Fuso Horário**.

9. Selecione o **Status do Alerta** como se quisesse Ativar ou Desativar a notificação de alerta desse usuário. Quando esta estiver ativada, o usuário receberá todos os alertas assinados. Quando estiver desativada, os usuários não receberão alertas.

   Nota: O valor Assinado é preenchido pelo sistema.
10. Selecione a **Visibilidade do Assinante** como se o usuário estivesse visível apenas para a sua empresa (Local) ou para toda a comunidade do hub (Global).
11. Clique em **Gerar Senha Automaticamente** para gerar uma senha automaticamente. Se você optar por selecionar uma senha para este usuário, digite a senha nas caixas de texto Senha e Digitar Senha Novamente.
12. Clique em **Salvar**. Repita estas etapas para incluir usuários adicionais.

Configurando o Usuário do FTP

Para ativar o usuário atual como um usuário do FTP, faça o seguinte:

1. Clique em **Administrador de Conta** > **Perfis** > **Usuários**. O sistema exibe a tela Lista de Usuários.
2. Selecione o usuário necessário e clique no ícone **Editar**.
3. Clique em **Configuração do FTP**.
4. Insira o **Diretório Home**, que é o caminho relativo do valor especificado para o bcg.ftp.config.rootdirectory. Esse é um campo obrigatório.
5. Ative ou desative a **Permissão de Gravação** ao diretório home.
6. Ative ou desative a permissão para **Criar/Remover o Diretório**.
7. Selecione **Número Max de Logins**, que é o número máximo de logins simultâneos permitidos. Se você selecionar Limite Customizado, insira o valor customizado na caixa de texto.
8. Selecione **Login Máx do Mesmo IP**, que é o login simultâneo máximo permitido do mesmo endereço IP. Se você selecionar Limite Customizado na lista, insira o valor customizado na caixa de texto.
9. Selecione o **Tempo Máximo Inativo**, que é o tempo inativo máximo após o qual a conexão é descartada. Se você selecionar Limite Customizado na lista, insira o valor customizado na caixa de texto.
10. Selecione **Max. de upload**, que é a taxa máxima de upload em bytes/seg. Se você selecionar Limite Customizado na lista, insira o valor customizado na caixa de texto.
11. Selecione **Max. de Download**, que é a taxa máxima de download em bytes/seg. Se você selecionar Limite Customizado na lista, insira o valor customizado na caixa de texto.
12. Clique em **Salvar**.

Incluindo Usuários em Grupos

1. Clique em **Administrador de Conta** > **Perfis** > **Usuários**. O sistema exibe a tela Lista de Usuários.
2. Clique no ícone Visualizar Detalhes para visualizar os detalhes de associação de grupo do usuário de destino.
3. Clique no ícone Editar para editar as associações de grupo do usuário.
4. Selecione um grupo e clique no botão **Incluir ao Grupo** ou **Remover do Grupo** para incluir ou remover um usuário de um grupo.
5. Clique no ícone Desativar Edição quando concluir a edição.

Criando Informações de Contato

Utilize o recurso Contatos para criar informações de contato para o pessoal chave. Você utilizará essas informações de contato para identificar as pessoas que deverão receber notificações de eventos e o sistema gerará notificações de alerta.

Dependendo do tamanho da sua organização, você provavelmente desejará notificar contatos diferentes quando tipos diferentes de eventos ocorrerem. Por exemplo, quando a validação de um documento falhar, o pessoal da segurança deverá ser notificado para que o problema possa ser avaliado. Quando as transmissões do parceiro interno excederem os limites normais, o administrador da sua rede deverá ser notificado para garantir que o sistema esteja lidando eficientemente com o aumento nas transmissões.

Após a criação dos seus contatos, você retornará ao recurso Alerta para vincular os contatos adequados a cada alerta que você criou.

Para criar novos contatos:

1. Clique em **Administrador de Conta** >**Perfis** > **Contatos**. O sistema exibe uma lista dos contatos atuais.
2. Clique em **Criar** no canto superior direito da tela. O sistema exibe a tela Detalhes do Contato.
3. Digite o **Prenome** e **Nome de Família** do contato.
4. Digite o **Endereço** do contato.
5. Selecione o **Tipo de Contato** na lista drop-down (por exemplo, B2B Lead ou Business Lead).
6. Digite o endereço de **E-Mail** do contato.
7. Digite o **Telefone** e **Números de Faxes** do contato.
8. Selecione o **Código do Idioma**, **Formatar Código de Idioma** e **Fuso Horário**.
9. Selecione o **Status do Alerta** como se quisesse Ativar ou Desativar a notificação de alerta desse contato. Se ativado, o contato receberá todos os alertas assinados. Se desativado, o contato não receberá alertas.

   Nota: O valor Assinado é preenchido pelo sistema.
10. Selecione a **Visibilidade Assinada** do contato. Se você selecionar Local, o contato estará visível apenas para sua organização. Se você selecionar Global, o contato estará visível tanto para o administrador do hub, quanto para o parceiro interno. Ambos poderão assinar o contato para receber alertas.
11. Clique em **Salvar**. Há várias formas de incluir o contato em um alerta:

    Para incluir um contato em um alerta existente, consulte “Incluindo um Novo Contato em um Alerta Existente” na página 37.

    Para criar um alerta com base em volume e incluir contatos no alerta, consulte “Criando um Alerta com Base em Volume” na página 33.

    Para criar um alerta com base em evento e incluir contatos no alerta, consulte “Criando um Alerta com Base em Evento” na página 35.

Criando Alertas e Incluindo Contatos

Distribuir informações sobre problemas no sistema para as pessoas corretas, no momento correto, é a chave para a rápida solução do problema.

Os alertas do WebSphere Partner Gateway são utilizados para notificar o pessoal-chave sobre flutuações incomuns no volume de transmissões recebidas, ou quando ocorrem erros do processamento de documentos comerciais.

Uma opção complementar no módulo Visualizador, Visualizador de Eventos, o ajuda a identificar, solucionar problemas e resolver erros de processamento.

Um alerta consiste em uma mensagem de e-mail baseada em texto enviada para contatos assinados ou para uma lista de distribuição do pessoal chave. Os alertas são baseados na ocorrência de um evento de sistema (alerta com base em evento) ou no volume do fluxo de documento esperado (alerta com base em volume).

- Utilize um alerta com base em volume para receber notificações de aumento ou diminuição no volume de transmissões.

  Por exemplo, se você for um parceiro externo, poderá criar um alerta com base em volume que o notificará caso você não receba nenhuma transmissão do parceiro interno em dias úteis (defina o volume como Volume Zero, defina a freqüência como Diário e selecione Segunda até Sexta na opção Dias da Semana). Esse alerta pode evidenciar dificuldades de transmissão do parceiro interno na rede.

  Se você for um parceiro externo, também poderá criar um alerta com base em volume que o avisará quando o número de transmissões do parceiro interno exceder a taxa normal. Por exemplo, se você receber normalmente cerca de 1 000 transmissões por dia, você poderá definir o Volume Esperado como 1 000 e o Desvio de Porcentagem como 25%. O alerta o notificará quando você receber mais de 1 250 transmissões por dia (ele também o notificará quando o volume de transmissões for inferior a 750). Esse alerta poderá identificar o aumento na demanda do parceiro interno, que pode, com o tempo, solicitar que você inclua mais servidores em seu ambiente.

  Observe que os alertas baseados em volume monitoram o volume em relação ao tipo de documentos que você selecionou ao criar o alerta. O WebSphere Partner Gateway consulta apenas os documentos que contêm o tipo de documentos selecionado em seu alerta e gera alertas somente quando todos os critérios do alerta são atendidos.
- Utilize um alerta com base em evento para receber notificações quando ocorrerem erros durante o processamento do documento. Por exemplo, talvez você queira criar um alerta que o notifique sobre falhas no processamento de um documento devido a erros de validação ou porque documentos duplicados foram recebidos. Você também pode criar alertas que permitem identificar a data em que um certificado expirará.

  Você utilizará os códigos de eventos predefinidos do WebSphere Partner Gateway para criar alertas de eventos. Há cinco tipos de eventos: Depuração, Informação, Aviso, Erro, Crítico. Dentro de cada tipo de evento há muitos outros eventos. É possível visualizar e selecionar eventos predefinidos na tela Alerta: Eventos. Por exemplo, 240601 Falha na Nova Tentativa de AS ou 108001 Não É um Certificado.

Nota: O parceiro externo só poderá criar um alerta com base no volume de documentos enviados para o parceiro interno. Para que o parceiro configure um alerta com base no volume de documentos enviados do parceiro interno para o parceiro externo, ele deverá solicitar ao administrador do hub para configurar um alerta com base em volume em nome do parceiro externo, especificando o parceiro externo como o proprietário do alerta.

Dica:

- Utilize um alerta baseado no volume para receber a notificação, quando esperada
- O volume de transmissão do parceiro externo ou interno cai abaixo dos limites de operação. Esse alerta poderá realçar os problemas de transmissão de rede do parceiro interno ou externo.
- Utilize um alerta com base em evento para receber notificações de erros durante o processamento do documento. Por exemplo, é possível criar um alerta com base em evento que o notifique sobre falhas no processamento de seu documento devido a erros de validação.

Criando um Alerta com Base em Volume

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Clique em **Criar** no canto superior direito da tela. O sistema exibe a guia Definir Alertas.
3. Selecione **Alerta de Volume** para o **Tipo de Alerta** (esta é a configuração padrão). O sistema exibe as caixas de texto adequadas para um alerta de volume.
4. Digite um **Nome de Alerta** para o alerta.
5. Selecione um **Parceiro** com direitos de criar um alerta baseado no volume (parceiro interno e administrador do hub apenas).
6. Selecione **Pacote**, **Protocolo** e **Tipo de Documento** nas listas drop-down.

   O Pacote, Protocolo e Tipo de Documento selecionados devem corresponder ao Pacote, Protocolo e Tipo de Documento do parceiro externo de origem.
7. Selecione uma das três opções de volume (Esperado, Intervalo ou Volume Zero) e continue em 8 na página 34:
   - **Esperado** - Selecione Esperado se quiser que um alerta seja gerado quando o volume do tipo de documento desviar de uma quantidade exata. Utilize as seguintes etapas para criar um alerta no volume do tipo de documento esperado:
     a. Na caixa de texto Volume, digite o número de tipos de documentos que você espera receber em um período determinado, selecionado em 8. Digite um número positivo; o alerta não funcionará se você digitar um número negativo.
     b. Na caixa de texto Desvio de Porcentagem, digite um número que defina o limite que o volume do fluxo de documento pode desviar antes que o alerta seja ativado. Por exemplo:
        – Se o volume for igual a 20 e o desvio de porcentagem for igual a 10, o volume de um fluxo de documento menor que 18 ou maior que 22 disparará um alerta.
        – Se o volume for igual a 20 e o desvio de porcentagem for igual a 0, o volume de qualquer fluxo de documento diferente de 20 disparará um alerta.
   - **Intervalo**. Selecione Intervalo para gerar um alerta se o volume do fluxo de documento não estiver dentro de um intervalo mínimo/máximo. Utilize as seguintes etapas para criar um alerta com base em um intervalo de valores:
     a. Na caixa de texto Mínimo, digite o número mínimo de tipos de documentos que você espera receber em um período determinado, selecionado em 8. Um alerta será disparado apenas se o volume do fluxo de documento estiver abaixo dessa quantia.

b. Na caixa de texto Máximo, digite o número máximo de tipos de documentos que você espera receber em um período determinado, selecionado em 8.

Nota: As caixas de texto Mínimo e Máximo devem ser preenchidas durante a criação de um alerta baseado no intervalo de volume.

- **Volume Zero**. Selecione Volume Zero para disparar um alerta se nenhum tipo de documento ocorrer em um período determinado, selecionado em 8.

8. Selecione Diário ou Intervalo para o período determinado (freqüência) que o sistema utilizará para monitorar o volume do fluxo de documento para a geração de alertas.
   - **Diário**. Selecione Diário para monitorar o volume do fluxo de documento em um ou mais dias da semana ou do mês. Por exemplo, selecione Diário se você for monitorar o volume do fluxo de documento em um ou mais dias da semana (por exemplo, segundas ou segundas e quintas) ou em dias do mês específicos (por exemplo, 1º e 15° dias).
   - **Intervalo**. Selecione Intervalo para monitorar o volume do fluxo de documento entre dois dias da semana ou do mês. Por exemplo, selecione Intervalo para monitorar o volume do fluxo de documento todos os dias da semana, entre segunda e sexta-feira, ou entre os dias 5 e 20 de cada mês.
9. Selecione as horas de início e de término (24 horas por dia) que o sistema monitorará o volume do fluxo de documento para os dias selecionados na próxima etapa. Observe que, quando a freqüência de Intervalo for selecionada, o volume do fluxo de documento será monitorado a partir da hora de início do primeiro dia do intervalo até a hora de término do último dia do mesmo intervalo.
10. Selecione os dias apropriados durante a semana ou o mês em que ocorrerá a monitoração de alertas. Se você selecionou Diário como a freqüência, selecione os dias reais da semana ou do mês para a monitoração do alerta. Se você selecionou Intervalo como a freqüência, selecione dois dias da semana ou dois dias do mês entre os quais a monitoração do alerta ocorrerá.
11. Selecione o **Status do Alerta** como Ativado ou Desativado.
12. Clique em **Salvar**.
13. Clique na guia **Notificar**.
14. Clique no ícone Editar.
15. Selecione um parceiro (parceiro interno e administrador do hub, apenas).
16. Se o contato que você deseja incluir estiver listado na caixa de texto Contatos, selecione o contato e clique em **Associar**. Acesse 21.

    Se o contato que você deseja incluir não estiver listado na caixa de texto Contatos, clique em **Incluir Nova Entrada para Contatos**. O sistema exibe a janela pop-up Criar Novo Contato.

    Observe que a opção Incluir Nova Entrada para Contatos é apresentada somente ao Proprietário do Alerta que irá criar contatos associados a ele. Este recurso não permite que o Proprietário do Alerta inclua contatos nos parceiros do Alerta.
17. Digite o nome, o endereço de e-mail, os números de telefone e fax do contato.
18. Selecione o Status de Alerta do contato.
    - Selecione **Ativado** para começar a enviar mensagens de e-mail para este contato quando o sistema gerar este alerta.
    - Selecione **Desativado** se você não quiser enviar mensagens de e-mail para este contato quando o sistema gerar este alerta.

19. Selecione a visibilidade do contato.
    - Selecione **Local** para tornar o contato visível apenas para a sua organização.
    - Selecione **Global** para tornar o contato visível para o administrador do hub e parceiro interno. Ambos poderão assinar o contato para receber alertas.
20. Clique em **Salvar** para salvar o contato. Clique em **Salvar e Associar** para incluir o contato na lista de contatos deste alerta.
21. Clique em **Salvar**.

Nota: As alterações feitas aos alertas com base no volume, após o período de monitoração original, entram em vigor no dia seguinte ao período de monitoração. Por exemplo, um alerta é monitorado das 13h às 15h nas quartas e nas quintas-feiras. Na quarta-feira às 16h, a monitoração do alerta é alterada para o período das 17h às 19h. O alerta não irá monitorar duas vezes na quarta-feira; a alteração entrará em vigor na quinta-feira.

Criando um Alerta com Base em Evento

Nota: O servidor de e-mail de Alerta a ser configurado. Consulte o *Guia de Administração* para configurar o servidor de e-mail de alerta

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Clique em **Criar** no canto superior direito da tela. O sistema exibe a guia Definir Alertas.
3. Selecione **Alerta de Evento** para o **Tipo de Alerta**. O sistema exibe as caixas de texto apropriadas para um alerta com base em evento.
4. Digite um **Nome de Alerta** para o alerta. Esse será o identificador desse alerta.
5. Selecione um **Parceiro** que acionará o alerta (essa opção está disponível apenas para o parceiro interno e o administrador do hub).

   Selecione a opção Qualquer Parceiro para associar o alerta a todos os parceiros no sistema. Quando você executa uma procura de alerta e seleciona Qualquer Parceiro como o Parceiro do Alerta, o sistema exibe todos os alertas que não estão associados a um parceiro específico.
6. Selecione **Pacote**, **Protocolo** e **Tipo de Documento** nas listas drop-down.
7. Selecione o tipo de evento: Depuração, Informação, Aviso, Erro, Crítico ou Todos. Esse atua como um filtro para limitar os eventos que aparecem na lista Nomes dos Eventos.
8. Selecione o evento que ativará o alerta, por exemplo, BCG240601 Falha na Nova Tentativa de AS ou 108001 Não É um Certificado. Para criar um alerta que notificará você sobre a data em que um certificado está prestes a expirar, selecione um dos seguintes eventos:
   - BCG108005 Expiração do Certificado em 60 Dias
   - BCG108006 Expiração do Certificado em 30 Dias
   - BCG108007 Expiração do Certificado em 15 Dias
   - BCG108008 Expiração do Certificado em 7 Dias
   - BCG108009 Expiração do Certificado em 2 Dias
9. Selecione o status desse alerta: Ativado ou Desativado.
10. Clique em **Salvar**.
11. Clique na guia **Notificar**.

12. Clique no ícone Editar.
13. Selecione um parceiro (parceiro interno e administrador do hub, apenas).
14. Se o contato que você deseja incluir estiver listado na caixa de texto Contatos, selecione o contato e clique em **Associar**. Acesse 19.

    Se o contato que você deseja incluir não estiver listado na caixa de texto Contatos, clique em **Incluir Nova Entrada para Contatos**. O sistema exibe a janela pop-up Criar Novo Contato.

    Observe que a opção Incluir Nova Entrada para Contatos é apresentada somente ao Proprietário do Alerta que irá criar contatos associados a ele. Esse recurso não permite que o Proprietário do Alerta inclua contatos nos Parceiros do Alerta.
15. Digite o nome, o endereço de e-mail, os números de telefone e fax do contato. Apenas o endereço de e-mail é utilizado para enviar alertas externos. O resto das entradas é para fins de informações adicionais.
16. Selecione o Status de Alerta do contato.
    - Selecione **Ativado** para começar a enviar mensagens de e-mail para este contato quando o sistema gerar este alerta.
    - Selecione **Desativado** se você não quiser enviar mensagens de e-mail para este contato quando o sistema gerar este alerta.
17. Selecione a visibilidade do contato.
    - Selecione **Local** para tornar o contato visível apenas para a sua organização.
    - Selecione **Global** para tornar o contato visível para o administrador do hub e parceiro interno. Ambos poderão assinar o contato para receber alertas.
18. Clique em **Salvar** para salvar o contato. Clique em **Salvar e Associar** para salvar o contato e incluí-lo na lista de contatos deste alerta.
19. Selecione o Modo de Distribuição:
    - **Enviar alertas imediatamente**. Quando você seleciona esta opção, o sistema envia notificações de alerta para o contato quando ocorre o alerta. Utilize essa opção para alertas críticos.
    - **Agrupar Alertas por**. Quando você seleciona esta opção, é possível especificar quando deseja que o contato receba notificações de alerta. Utilize essa opção para alertas não-críticos.

      As duas opções nesta seção, Quantidade e Período, não são mutuamente exclusivas.

      Se você selecionar a opção Quantidade, você sempre deverá selecionar a opção Período.
      - Se o número de alertas (Quantidade) for alcançado durante o limite de tempo que você selecionou (Período), o sistema irá gerar uma notificação de alerta.
      - Se ocorrer um alerta mas o número de alertas (Quantidade) não for alcançado durante o limite de tempo que você selecionou (Período), o sistema irá gerar uma notificação de alerta no término do limite de tempo.

      A opção Período pode ser usada sem a opção Quantidade, mas a opção Quantidade sempre deve estar associada a um limite de tempo (Período).
      - **Quantidade**. Ao selecionar esta opção, utilize também a opção Período. Digite um número (n). Este é o número de alertas que deve ocorrer durante o período de tempo selecionado (Período) antes que o sistema envie uma notificação de alerta para o contato do alerta.

        Aqui está um exemplo de como essas duas opções trabalham juntas:

Em nosso exemplo, as opções Agrupar Alertas por estão definidas como 10 para Quantidade (10 alertas) e 2 para Período (período de 2 horas). O sistema retém todas as notificações deste alerta até que ocorram 10 alertas em um período de duas horas ou até o término do período.

Quando a contagem de alertas atingir 10 em um período de 2 horas, o sistema enviará todas as notificações de alerta deste alerta para o contato.

Se ocorrer apenas um alerta e 10 alertas não ocorrerem durante o limite de tempo (duas horas), o sistema enviará uma notificação de alerta para o contato do alerta no término do limite de tempo.

– **Período**. Selecione o número de horas (n). O sistema retém a notificação de alerta para n horas. A cada n horas, o sistema envia todas as notificações de alerta retidas para o contato.

Por exemplo, se você digitar 2, o sistema reterá todas as notificações deste alerta que ocorrerem a cada intervalo de duas horas. Quando o intervalo de duas horas expirar, o sistema enviará todas as notificações de alerta deste alerta para o contato.

20. Clique em **Salvar**.

Incluindo um Novo Contato em um Alerta Existente

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Digite o critério de procura a partir das listas drop-down. Digite o Nome do Alerta.
3. Clique em **Procurar**. O sistema exibirá uma lista de alertas que atendem ao critério de procura, se houver algum.
4. Clique no ícone Visualizar Detalhes para visualizar detalhes do alerta.
5. Clique no ícone Editar para editar detalhes do alerta.
6. Clique na guia **Notificar**.
7. Selecione um parceiro (parceiro interno e administrador do hub, apenas).
8. Se o contato que você deseja incluir estiver listado na caixa de texto Contatos, selecione o contato e clique em **Associar**. Acesse 13.

   Se o contato que você deseja incluir não estiver listado na caixa de texto Contatos, clique em **Incluir Nova Entrada para Contatos**. O sistema exibe a janela pop-up Criar Novo Contato.

   Observe que a opção Incluir Nova Entrada para Contatos é apresentada somente ao Proprietário do Alerta que irá criar contatos associados a ele. Esse recurso não permite que o Proprietário do Alerta inclua contatos nos Parceiros do Alerta.
9. Digite o nome, o endereço de e-mail, os números de telefone e fax do contato.
10. Selecione o Status de Alerta do contato.
    - Selecione **Ativado** para começar a enviar mensagens de e-mail para este contato quando o sistema gerar este alerta.
    - Selecione **Desativado** se você não quiser enviar mensagens de e-mail para este contato quando o sistema gerar este alerta.
11. Selecione a visibilidade do contato.
    - Selecione **Local** para tornar o contato visível apenas para a sua organização.
    - Selecione **Global** para tornar o contato visível para o administrador do hub e parceiro interno. Ambos poderão assinar o contato para receber alertas.
12. Clique em **Salvar** para salvar o contato. Clique em **Salvar e Associar** para salvar o contato e incluí-lo na lista de contatos deste alerta.

13. Clique em **Salvar.**

Criando um Novo Endereço

Utilize este recurso para criar os endereços em seu perfil de parceiro. O sistema é configurado para suportar vários tipos de endereços Corporativos, de Cobrança e Técnicos.

Para criar um novo endereço:

1. Clique em **Administrador de Conta** > **Perfis** > **Endereços**. O sistema exibe a tela Endereços.
2. Clique em **Criar Novo Endereço** no canto superior direito da tela. O sistema exibe a tela Endereços.
3. Selecione o Tipo de Endereço na lista drop-down (de Cobrança, Corporativo ou Técnico).
4. Digite o endereço nas caixas de texto apropriadas.
5. Clique em **Salvar**.

Capítulo 3. Criando Destinos

Os destinos definem os pontos de entradas no sistema. Este capítulo apresenta as etapas de criação dos destinos e contém os seguintes tópicos:

Visão Geral

O WebSphere Partner Gateway utiliza destinos para rotear documentos ao destino apropriado. O destinatário pode ser um parceiro externo ou o parceiro interno. O protocolo de transporte de saída determina as informações utilizadas durante a configuração de destino.

Estes são os transportes suportados (por padrão) pelos destinos dos parceiros:

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

  Nota: É possível definir um destino SMTP para parceiros externos apenas (não para o parceiro interno).
- Diretório de arquivos
- Script de FTP

Também é possível especificar um transporte definido pelo usuário, o qual você faz o upload durante a criação do destino.

Configurando um Destino HTTP

Você configura um destino HTTP, de forma que os documentos possam ser enviados do hub para o endereço IP do seu parceiro. Quando um destino HTTP é configurado, você também pode especificar que os documentos sejam enviados por um servidor proxy configurado.

Para começar o processo de criação de um Destino HTTP, utilizar o procedimento a seguir.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página **Lista de Destinos**, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório. Esse é o nome que aparecerá na lista de destinos.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Opcionalmente, selecione um servidor proxy a ser utilizado. A **Lista de Proxies de Redirecionamento** inclui os servidores proxy criados, incluindo o servidor proxy padrão. O valor padrão para este campo é **Utilizar o proxy de redirecionamento padrão**. Se desejar que o parceiro selecionado utilize um servidor proxy diferente, selecione o servidor na lista. Se não desejar utilizar este recurso para o parceiro selecionado, selecione **Não utilizar o proxy de redirecionamento**.
2. Selecione **HTTP/1.1** na lista **Transporte**.
3. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   O formato é: http://*<nome do servidor>:<porta opcional<caminho>*

   Um exemplo desse formato é:

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

   Quando você estiver configurando um destino a ser utilizado para um serviço da Web, especifique a URL privada, indicada pelo provedor de serviços da Web. Neste ponto, o WebSphere Partner Gateway chamará o serviço da Web quando ele agir como um proxy para o provedor de serviços da Web.
4. Ou então, digite o nome e a senha de um usuário, se forem necessários para acessar o servidor HTTP.
5. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
6. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
7. No campo **Número de Encadeamentos**, digite o número de documentos que podem ser processados simultaneamente. O padrão é 3.
8. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.

9. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
10. No campo **Tempo Limite de Conexão**, digite o número de segundos que um soquete permanecerá aberto sem tráfego. O padrão é 120 segundos.
11. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para "Configurando Rotinas de Tratamento" na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino HTTPS

Você configura um destino HTTPS, de forma que os documentos possam ser enviados do hub para o endereço IP do seu parceiro. Quando um destino HTTPS é configurado, é possível também especificar que os documentos sejam enviados por um servidor proxy configurado.

Para criar destinos HTTPS, utilize este procedimento.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Lista de Destinos, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **HTTPS/1.0** ou **HTTPS/1.1** na lista **Transporte**. A configuração de destino HTTP/S não contém configuração de proxy de redirecionamento.
2. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   O formato é: https://*<nome do servidor>:<porta opcional<caminho>*

   Por exemplo:

   `https://anotherserver.ibm.com:57443/bcgreceiver/Receiver`
3. Ou então, digite o nome e a senha de um usuário, se forem necessários para acessar o servidor HTTP seguro.
4. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
5. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.

6. No campo **Número de Encadeamentos**, digite o número de documentos que podem ser processados simultaneamente. O padrão é 3.
7. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.
8. No campo **Validar Certificado SSL do Cliente**, selecione **Sim** se deseja que o certificado digital do parceiro emitente seja validado em relação ao ID comercial associado ao documento.O padrão é **Não**.
9. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
10. No campo **Tempo Limite de Conexão**, digite o número de segundos que um soquete permanecerá aberto sem tráfego. O padrão é 120 segundos.
11. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para "Configurando Rotinas de Tratamento" na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino FTP

Para criar um destino FTP, utilize os procedimentos a seguir.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Detalhes do Destino, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **FTP** na lista **Transporte**.
2. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   O formato é: ftp://*<nome do servidor ftp>*: *<n.º da porta>*

   Por exemplo:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Se não desejar digitar um número de porta, a porta FTP padrão será utilizada.
3. Ou então, digite o nome e a senha de um usuário, se forem necessários para acessar o servidor FTP.
4. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.

5. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
6. No campo **Número de Encadeamentos**, digite o número de documentos que podem ser processados simultaneamente. O padrão é 3.
7. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.
8. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
9. No campo **Tempo Limite de Conexão**, digite o número de segundos que um soquete permanecerá aberto sem tráfego. O padrão é 120 segundos.
10. No campo **Usar Nome de Arquivo Exclusivo**, deixe a caixa selecionada, se desejar. Do contrário, clique na caixa para remover a marca. Se você selecionar **Usar Nome de Arquivo Exclusivo**, o nome do arquivo original será armazenado no banco de dados.
11. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para "Configurando Rotinas de Tratamento" na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino SMTP

Para criar um destino SMTP, utilize estes procedimentos.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Lista de Destinos, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **SMTP** na lista **Transporte**.
2. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   O formato é: mailto:<*usuário@nome do servidor*>

   Por exemplo:

   `mailto:admin@anotherserver.ibm.com`
3. Ou então, digite o nome e a senha de um usuário, se forem necessários para acessar o servidor SMTP.

4. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
5. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
6. No campo **Número de Encadeamentos**, digite o número de documentos que podem ser processados simultaneamente. O padrão é 3.
7. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.
8. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
9. No campo **Autenticação Obrigatória**, indique se o nome e a senha de um usuário foram fornecidos no documento. O padrão é **Não**.
10. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para "Configurando Rotinas de Tratamento" na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino JMS

Para criar destinos JMS, utilize este procedimento.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Lista de Destinos, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **JMS** na lista **Transporte**.
2. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   Em WebSphere MQ JMS, o formato do URI do destino é o seguinte:

   ```
   file:///<user_defined_MQ_JNDI_bindings_path>
   ```

   Por exemplo:

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

   O diretório contém o arquivo ".bindings" do JNDI com base em arquivo. Esse arquivo indica ao WebSphere Partner Gateway como rotear o documento para o destino pretendido. Esse campo é obrigatório.

3. Como opção, digite o nome de usuário e a senha do JMS se forem necessários para acessar a fila JMS.
4. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
5. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
6. No campo **Número de Encadeamentos**, digite o número de documentos que podem ser processados simultaneamente. O padrão é 3.
7. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.
8. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
9. No campo **Autenticação Obrigatória**, indique se o nome e a senha de um usuário foram fornecidos no documento. O padrão é **Não**.
10. No campo **Nome do Depósito de Informações do Provedor JMS**, digite o nome da classe Java que o provedor JMS utiliza para se conectar à fila JMS. Esse campo é obrigatório.
11. No campo **Classe de Mensagem JMS**, digite a classe de mensagem. As opções são qualquer classe válida de mensagem JMS, como TextMessage ou BytesMessage. Esse campo é obrigatório.
12. No campo **Tipo de Mensagem JMS**, digite o tipo de mensagem. Esse campo é opcional.
13. No campo **Pacotes de URL do Provedor**, digite o nome das classes (ou arquivo JAR) que o Java utiliza para entender a URL do contexto JMS. Este campo é opcional.Se você não especificar um valor, o caminho do sistema de arquivos para o arquivo de ligações será utilizado.
14. No campo **Nome da Fila JMS**, digite o nome da fila JMS para a qual os documentos devem ser enviados. Esse campo é obrigatório.
15. No campo **Nome do Depósito de Informações do Provedor JMS JNDI**, digite o nome do depósito de informações do provedor utilizado para se conectar ao serviço de nomes. Esse campo é obrigatório.
16. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para “Configurando Rotinas de Tratamento” na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino de Diretório de Arquivos

Para criar destinos de diretório de arquivo, utilize este procedimento.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Lista de Destinos, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.

2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **Diretório de Arquivos** na lista **Transporte**.
2. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   O formato para sistemas UNIX e Windows em que o diretório de arquivos está na mesma unidade em que o WebSphere Partner Gateway está instalado é: file:///<caminho para o diretório de destino>

   Por exemplo:

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

   em que *localfiledir* é um diretório do diretório raiz.

   Para sistemas Windows em que o diretório de arquivos está em uma unidade separada do WebSphere Partner Gateway, o formato é: file:///<letra da unidade>:/<caminho>
3. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
4. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
5. No campo **Número de Encadeamentos**, digite o número de documentos que devem ser processados simultaneamente. O padrão é 3.
6. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.
7. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
8. No campo **Usar Nome de Arquivo Exclusivo**, deixe a caixa selecionada, se desejar. Do contrário, clique na caixa para remover a marca. Se você selecionar **Usar Nome de Arquivo Exclusivo**, o nome do arquivo original será armazenado no banco de dados.
9. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para "Configurando Rotinas de Tratamento" na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino FTPS

Para criar destinos FTPS, utilize este procedimento.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Lista de Destinos, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **FTPS** na lista **Transporte**.
2. No campo **Endereço**, digite o URI no qual o documento será entregue. Esse campo é obrigatório.

   O formato é: ftp://<*nome do servidor ftp*>: <*n.º da porta*>

   Por exemplo:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Se não desejar digitar um número de porta, a porta FTP padrão será utilizada.
3. Ou então, digite o nome e a senha de um usuário, se forem necessários para acessar o servidor FTP seguro.
4. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
5. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
6. No campo **Número de Encadeamentos**, digite o número de documentos que devem ser processados simultaneamente. O padrão é 3.
7. No campo **Validar IP do Cliente**, selecione **Sim** se deseja que o endereço IP do emissor seja validado antes que o documento seja processado. Caso contrário, selecione **Não**. O padrão é **Não**.
8. No campo **Fila Automática**, selecione **Sim** se deseja que o destino seja colocado off-line (automaticamente) se uma falha na entrega estiver prestes a ocorrer devido ao término do número de novas tentativas. Caso contrário, selecione **Não**. O padrão é **Não**.

   Quando você seleciona **Fila Automática**, todos os documentos permanecem enfileirados até o destino ser colocado manualmente on-line.
9. No campo **Tempo Limite de Conexão**, digite o número de segundos que um soquete permanecerá aberto sem tráfego. O padrão é 120 segundos.
10. No campo **Usar Nome de Arquivo Exclusivo**, deixe a caixa selecionada, se desejar. Do contrário, clique na caixa para remover a marca. Se você selecionar **Usar Nome de Arquivo Exclusivo**, o nome do arquivo original será armazenado no banco de dados.
11. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para “Configurando Rotinas de Tratamento” na página 51. Do contrário, clique em **Salvar**.

Configurando um Destino de Script FTP

Um destino de Script de FTP é executado de acordo com o planejamento que você define. O comportamento de um destino de Script FTP é controlado por um script de comando FTP.

Criando o Script FTP

Para utilizar um destino de Script de FTP, você cria um arquivo que inclui todos os comandos FTP necessários, que possam ser aceitos por seu servidor de FTP.

1. Crie um script para os destinos para indicar as ações a serem executadas. O script a seguir é um exemplo de conexão com o servidor de FTP especificado (com o nome e a senha especificados), alteração do diretório especificado no servidor de FTP e envio de todos os arquivos ao diretório especificado no servidor.

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

   Os espaços reservados (por exemplo, %BCGSERVERIP%) são substituídos quando o destino é colocado em serviço pelos valores que você digita quando cria uma instância específica de um destino de script de FTP, como mostrado na tabela a seguir:

   Tabela 3. Como Parâmetros de Script Mapeiam para Entradas do Campo de Destino de Script de FTP

Parâmetro de script	Entrada do Campo de Destino de Script de FTP
%BCGSERVERIP%	IP do Servidor
%BCGUSERID%	ID do Usuário
%BCGPASSWORD%	Senha
%BCGOPTIONx%	Opção*x*, em Atributos Definidos pelo Usuário

   É possível ter até 10 opções definidas pelo usuário.
2. Salve o arquivo.

Comandos de Script de FTP

É possível utilizar os seguintes comandos ao criar o script:

- ascii, binary, passive

  Esses comandos não são enviados para o Servidor de FTP. Eles modificam o modo de transferência (ascii, binary ou passive) para o Servidor de FTP.
- cd

  Esse comando leva ao diretório especificado.
- excluir

  Esse comando remove um arquivo do servidor de FTP.
- mkdir

  Esse comando cria um diretório no servidor de FTP.
- mput

  Esse comando obtém um argumento único, o qual especifica um ou mais arquivos a serem transferidos para o sistema remoto. Esse argumento pode conter os caracteres curinga padrão para identificar vários arquivos ('*' e '?').

- open

  Esse comando obtém três parâmetros: endereço IP do servidor de ftp, nome do usuário e senha. Eles mapeiam para as variáveis %BCGSERVERIP% %BCGUSERID% e %BCGPASSWORD%, respectivamente. A primeira linha do script Destino de Script de FTP deve ser:`open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%`.
- quit, bye

  Esse comando finaliza uma conexão existente com um Servidor de FTP.
- quote

  Esse comando indica que tudo o que aparecer após QUOTE deve ser enviado ao sistema remoto como um comando. Isto permite enviar comandos a um servidor de FTP remoto que pode não estar definido no protocolo de FTP padrão.
- rmdir

  Esse comando remove um diretório do servidor de FTP.
- site

  Esse comando podem ser utilizar para emitir comandos específicos do site para o sistema remoto. O sistema remoto determina se o conteúdo desse comando será válido.

Destinos do Script de FTP

Se estiver utilizando os destinos do Script de FTP, execute as seguintes tarefas:

Para criar destinos de Script de FTP, utilize os procedimentos a seguir.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.

Detalhes do Destino

Na página Lista de Destinos, execute as seguintes etapas:

1. Digite o nome para identificar o destino. Esse é um campo obrigatório.
2. Opcionalmente, indique o status do destino. **Ativado** é o padrão. Um destino ativado está pronto para enviar documentos. Um destino desativado não pode enviar documentos.
3. Como opção, indique se o destino está On-line ou Off-line. O padrão é **On-line**.
4. Opcionalmente, digite uma descrição para o destino.

Configuração do Destino

Na seção **Configuração de Destino** da página, execute as etapas a seguir:

1. Selecione **Script de FTP** na lista **Transporte**.
2. Digite o endereço IP do servidor de FTP para o qual você está enviando documentos. O valor que você digitar aqui substituirá %BCGSERVERIP% quando o script de FTP for executado.
3. Digite o ID de usuário e a senha necessários para acessar o servidor de FTP. Os valores que você digitar aqui substituirão %BCGUSERID% e %BCGPASSWORD% quando o script de FTP for executado.
4. Se o destino estiver em modo seguro, utilize o valor padrão **Sim** para **Modo FTPS**. Caso contrário, clique em **Não**.
5. Faça o upload do arquivo de script seguindo estas etapas:
   a. Clique em **Fazer Upload de Arquivo de Script**.

b. Digite o nome do arquivo que contém o script para processar documentos ou clique em **Procurar** para navegar até o arquivo.
c. Clique em **Carregar Arquivo** para carregar o arquivo de script para a caixa de texto de arquivo **Script Carregado Atualmente**.
d. Se o arquivo de script for aquele que você deseja utilizar, clique em **Salvar**.
e. Clique em **Fechar Janela**.

6. No campo **Contagem de Novas Tentativas**, digite o número de vezes que você deseja que o destino tente enviar um documento antes de falhar. O padrão é 3.
7. No campo **Intervalo de Novas Tentativas**, digite o tempo que o destino deve aguardar antes de tentar enviar o documento novamente. O padrão é 300 segundos.
8. Em **Tempo Limite de Conexão**, digite o número de segundos que um soquete permanecerá aberto sem tráfego. O padrão é 120 segundos.
9. No campo **Bloquear Usuário**, indique se o destino pedirá um bloqueio, de forma que nenhuma outra instância de um destino de Script de FTP possa obter acesso ao mesmo diretório de servidor de FTP simultaneamente.

Atributos Definidos pelo Usuário

Se você desejar especificar atributos adicionais, execute as etapas a seguir. O valor digitado para a opção substituirá %BCGOPTION*x*% quando o script de FTP for executado (em que *x* corresponde ao número da opção).

1. Clique em **Novo**.
2. Digite um valor ao lado de **Opção 1**.
3. Se houver atributos adicionais a serem especificados, clique em **Novo** novamente e digite um valor.
4. Repita a etapa 3 quantas vezes for necessário para definir todos os atributos.

Por exemplo, suponha que o script de FTP tenha esta aparência:

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

Neste caso, %BCGOPTION% será um nome de diretório.

Planejar

Na seção Planejar da página, execute as seguintes etapas:

1. Indica se você deseja efetuar o planejamento baseado no intervalo ou o planejamento baseado no calendário.
   - Se você selecionar **Planejamento Baseado no Intervalo**, selecione quantos segundos devem ser decorridos para que o destino seja controlado por consulta (ou aceite o valor padrão).
   - Se você selecionar **Planejamento Baseado no Calendário**, escolha o tipo de planejamento (**Planejamento Diário**, **Planejamento Semanal** ou **Planejamento Personalizado**).
     – Se você selecionar **Planejamento Diário**, digite o horário do dia em que o destino deve ser controlado por consulta.
     – Se selecionar **Planejamento Semanal**, selecione um ou mais dias da semana, além do horário do dia.
     – Se selecionar **Planejamento Personalizado**, selecione o horário do dia e, em seguida, escolha **Intervalo** ou **Dias Seletivos** para a semana e o mês.

Com **Intervalo**, você indica as datas de início e de encerramento. (Por exemplo, clique em **Seg** e **Sex** se desejar que o servidor seja controlado por consulta apenas em determinado horário dos dias da semana.) Com **Dias Seletivos**, você escolhe os dias específicos da semana e do mês.

2. Se você desejar configurar a etapa Pré-processo ou Pós-processo para o destino, vá para "Configurando Rotinas de Tratamento". Do contrário, clique em **Salvar**.

Configurando Rotinas de Tratamento

É possível modificar dois pontos de processamento de um destino: Pré-processo e Pós-processo.

Por padrão, nenhuma rotina de tratamento é fornecida para a etapa Pré-processo ou Pós-processo e, portanto, nenhuma rotina de tratamento é listada, por padrão, na **Lista Disponível**. Se você tiver transferido por upload uma rotina de tratamento, poderá selecioná-la e movê-la para a **Lista Configurada**.

Para aplicar uma rotina de tratamento gravada pelo usuário para esses pontos de configuração, primeiro é necessário fazer upload da rotina de tratamento. Consulte o *Hub Configuration Guide* para obter as etapas sobre como fazer upload da rotina de tratamento. Em seguida, execute as seguintes etapas:

1. Selecione **pré-processar** ou **pós-processar** na lista **Rotinas de Tratamento do Ponto de Configuração**.
2. Selecione a rotina de tratamento na **Lista Disponível** e clique em **Incluir**.
3. Se desejar alterar os atributos da rotina de tratamento, selecione-os na **Lista Configurada** e clique em **Configurar**. A lista de atributos que podem ser alterados é exibida. Faça as alterações necessárias e clique em **Definir Valores**.
4. Clique em **Salvar**.

Posteriormente, é possível modificar a **Lista Configurada** da seguinte forma:

- Remova uma rotina de tratamento selecionando-a na **Lista Configurada** e clicando em **Remover**. A rotina de tratamento é movida para a **Lista Disponível**.
- Reorganize a ordem em que a rotina de tratamento é processada, selecionando a rotina de tratamento e clicando em **Mover para Cima** ou **Mover para Baixo**.

Especificando um Destino Padrão

Depois de criar os destinos do parceiro interno ou externo, selecione um dos destinos como o destino padrão.

1. Clique em **Administrador de Conta > Perfis > Destinos**.
2. Clique em **Criar**.
3. Clique em **Visualizar Destinos Padrão**.

   Uma lista de destinos definida para o participante é exibida.
4. Na lista **Produção**, selecione o destino que será o padrão para este parceiro. Também é possível definir destinos padrão para outros tipos de destinos, como **Testar**.
5. Clique em **Salvar**.

Capítulo 4. Gerenciando Usuários e Conexões da Comunidade: Administração de Contas

Os recursos no módulo Administrador de Conta controlam como e por quem o WebSphere Partner Gateway é utilizado.

Por exemplo, é possível controlar o acesso ao Community Console e a cada um de seus recursos. É possível controlar quem recebe alertas quando ocorrem eventos importantes. Exemplos de eventos incluem Conexão do Parceiro Não Encontrada, Erro de Validação de RosettaNet e Falha na Distribuição do Documento.

Você também utilizará este módulo para manter o perfil de parceiro, certificados, destinos, usuários, grupos, contatos, endereços, alertas e recursos B2B do participante. (Os recursos B2B definem os tipos de processos comerciais que o seu sistema pode enviar e receber). Se você estivesse envolvido no processo de configuração, você já estaria familiarizado com esses recursos.

Tabela 4. Recursos de Administração de Contas

Qual recurso você deseja utilizar?
"Gerenciando Destinos"
"Gerenciando Certificados" na página 55
"Gerenciando Grupos" na página 55
"Gerenciando Usuários" na página 56
"Gerenciando Contatos" na página 58
"Gerenciando Alertas" na página 59
"Gerenciando Endereços" na página 61

Gerenciando Destinos

Utilize o recurso Destino para visualizar informações sobre o destino utilizado para rotear documentos para seus destinos apropriados. É possível visualizar o URI de Destino, o protocolo de transporte e o status do destino a partir desse recurso.

Atenção: Alguns valores do destino dependem do protocolo de transporte selecionado. As restrições são anotadas nos procedimentos e na tabela de valores.

Visualizando uma Lista de Destinos

Clique em **Administração de Conta Perfis Destinos** para visualizar uma lista de destinos no sistema.

Visualizando ou Editando Detalhes do Destino

Importante: Ao desativar um destino, você também desativa a conexão do parceiro associada a esse destino. O destino não funcionará. Se você definir o destino como off-line, os documentos serão enfileirados até que ele seja definido novamente como on-line.

1. Clique em **Administrador de Conta** >**Perfis** > **Destinos**. O sistema exibe a tela Lista de Destino.
2. Clique no ícone Visualizar Detalhes para visualizar detalhes do destino.
3. Clique no ícone Editar para editar os detalhes de destino.

4. Edite as informações como solicitado. A tabela a seguir descreve os valores do destino.

Tabela 5. Valores na Tela de Destino

Valor	Descrição
Nome do Destino	Nome do destino. Nota: o nome do destino é um campo de formato livre definido pelo usuário. Os usuários devem usar nomes diferentes para destinos individuais para evitar possíveis confusões.
Transporte	O protocolo utilizado para rotear documentos.
URI de Destino	O URI de destino.
On-line ou Off-line	Se estiver off-line, os documentos serão enfileirados até que o destino seja colocado on-line.
Status	Ativado ou Desativado. Ocorrem falhas nos documentos roteados por meio de um destino com status de desativado.
Padrão	Identifica o destino padrão.

5. Clique em **Salvar**.

Visualizar, Selecionar ou Editar Destinos Padrão

1. Clique em **Administrador de Conta** >**Perfis** > **Destinos**. O sistema exibe a tela Lista de Destino.
2. Clique em **Visualizar Destinos Padrão** no canto superior direito da tela. O sistema exibe a tela Lista de Destinos Padrão.
3. Utilize as listas drop-down para selecionar ou alterar um ou mais destinos padrão.
4. Clique em **Salvar**.

Visualizando o Destino Whereused

Para visualizar os detalhes de onde um destino específico é empregado, utilize o seguinte procedimento:

1. Clique em **Administrador de Conta** > **Perfis** > **Destinos**.
2. Na lista de destino, clique no ícone **Whereused** referente ao destino adequado. A lista de onde todos os destinos selecionados estão sendo utilizados é exibida.

   Nota: Esta tela é fornecida com informações de paginação, uma vez que pode haver vários canais utilizando o destino. Cada página reterá, no máximo, 10 conexões.

Excluindo o Destino

Este recurso de exclusão de destino está disponível para todos os destinos, exceto para o destino padrão. Para excluir um destino, utilize o seguinte procedimento:

1. Clique em **Administrador de Conta** > **Perfis** > **Destinos**.
2. Na lista de destinos, clique no ícone **Excluir** que é referente ao destino a ser selecionado.

   Nota: O ícone **Excluir** não estará disponível para o destino padrão. Além disso, a operação de exclusão será permitida apenas se o destino selecionado não for utilizado nas conexões. No caso de você precisar de informações sobre o uso do destino, consulte “Visualizando o Destino Whereused”.

3. Clique em **OK** na janela de aviso para confirmar a exclusão.

Gerenciando Certificados

Esta seção fornece as etapas para a visualização, edição e exclusão de certificado digital utilizando o Community Console.

Visualizando e Editando Detalhes do Certificado Digital

1. Clique em **Administrador de Conta** > **Perfis** > **Certificados**. O sistema exibe uma lista de certificados digitais existentes.
2. Clique no ícone Visualizar Detalhes para visualizar detalhes do certificado. O sistema exibe a tela Detalhes do Certificado.
3. Clique no ícone Editar para editar o certificado.
4. Edite conforme solicitado.
5. Clique em **Salvar**.

Desativando um Certificado Digital

1. Clique em **Administrador de Conta** > **Perfis** > **Certificados**. O sistema exibe a tela Lista de Certificados.
2. Clique no ícone Visualizar Detalhes para visualizar detalhes do certificado. O sistema exibe a tela Detalhes do Certificado.
3. Clique no ícone Editar para editar o certificado.
4. Clique em **Desativado**.
5. Clique em **Salvar**.

Gerenciando Grupos

É possível visualizar, editar e excluir grupos usando o Community Console. Este recurso estará disponível somente para os usuários do grupo de administradores de parceiros internos/externos.

Visualizando Associados do Grupo e Designando Usuários para os Grupos

1. Clique em **Administrador de Conta** > **Perfis** > **Grupos**. O sistema exibe a tela Lista do Grupo.

Tabela 6. Valores na Tela Lista do Grupo

Valor	Descrição
Nome	O nome do grupo.
Descrição	A descrição do grupo.
Tipo de Grupo	O tipo, por exemplo, Sistema.

2. Clique no ícone Visualizar Membros para visualizar uma lista de membros em um grupo. Se este ícone não aparecer, não haverá membros no grupo. Clique em Associados no submenu.
3. Clique no ícone Editar para editar usuários em um grupo.
4. Clique em **Incluir ao Grupo** para designar usuários para o grupo.
5. Clique no ícone Desativar Edição para salvar e sair.

Visualizando, Editando ou Designando Permissões ao Grupo

A permissão de grupo para usuários e grupos não pode ser configurada nem mesmo pelo usuário do grupo de administradores. As permissões de outros grupos podem ser sempre menores ou iguais àquela de permissões do administrador. Por exemplo, se o administrador tiver permissão para Endereço, a permissão de outros grupos poderá ser ″sem acesso″ ou ″de leitura″.

1. Clique em **Administrador de Conta** > **Perfis** > **Grupos**. O sistema exibe a tela Lista do Grupo.
2. Clique no ícone Visualizar Permissões para visualizar permissões de um grupo. O sistema exibe uma lista de permissões do grupo selecionado.
3. Selecione **Sem Acesso**, **Apenas Leitura** ou **Leitura/Gravação** para cada recurso.
4. Clique em **Salvar**.

Visualizando ou Editando Detalhes do Grupo

1. Clique em **Administrador de Conta** > **Perfis** > **Grupos**. O sistema exibe a tela Lista do Grupo.
2. Clique no ícone Visualizar Detalhes para visualizar detalhes do grupo (Nome e Descrição). O sistema exibe a tela Detalhe do Grupo.
3. Clique no ícone Editar para editar detalhes do grupo (você não pode editar grupos gerados pelo sistema).
4. Edite conforme solicitado.
5. Clique em **Salvar**.

Restrições: Os grupos Padrão e Administrador são gerados pelo sistema e não podem ser editados ou excluídos. O Administrador do Hub tem um grupo adicional, Administrador de Hub.

Excluindo um Grupo

1. Clique em **Administrador de Conta** > **Perfis** > **Grupos**. O sistema exibe a tela Lista do Grupo.
2. Clique no ícone Visualizar Detalhes para visualizar detalhes do grupo. O sistema exibe a tela Detalhes do Grupo.
3. Clique no ícone Editar para editar detalhes do grupo.
4. Clique em **Excluir**. Confirme que você deseja a exclusão.

Aviso: Os grupos Padrão e Administrador são gerados pelo sistema e não podem ser editados ou excluídos.

Gerenciando Usuários

Utilize este recurso para visualizar e editar perfis de parceiros. Este recurso estará disponível somente para os usuários do grupo de administradores de parceiros internos/externos.

Nota: É possível utilizar esse recurso para designar ou gerar automaticamente uma nova senha para um usuário.

1. Clique em **Administrador de Conta** > **Perfis** > **Usuários**. O sistema exibe a tela Lista de Usuários.

A tabela a seguir descreve os valores na tela Lista de Usuários.

Tabela 7. Valores na Tela Lista de Usuários

Valor	Descrição
Nome do Usuário	O nome de login do console.
Nome Completo	O nome completo do usuário.
E-Mail	O endereço de e-mail utilizado para notificações de alerta.
Assinados	Se esta opção for marcada, um ou mais alertas serão designados ao usuário. Se o usuário for removido do sistema, todas as assinaturas de alerta dele também serão removidas.
Status do Login	O status Ativado permite que o usuário efetue login no console.

2. Clique no ícone Visualizar Detalhes para visualizar detalhes de um usuário.
3. Clique no ícone Editar para editar detalhes de um usuário.
4. Edite as informações como solicitado. A tabela a seguir descreve os valores na tela Detalhes do Usuário.

Tabela 8. Detalhes do Usuário

Valor	Descrição
Nome do Usuário	O nome de login do usuário do console.
Ativado	Ativa ou Desativa o acesso ao console.
Nome Fornecido	O Primeiro Nome do usuário.
Sobrenome	O sobrenome do usuário.
e-mail	O endereço de e-mail utilizado para notificações de alerta.
Telefone	O número de telefone do usuário.
Número de Fax	O número de fax do usuário.
Idioma	Selecione a área geográfica do usuário. Ela será padronizada de acordo com o idioma definido pelo administrador de hub.
Idioma do Formato	Selecione o país do usuário. Ela será padronizada de acordo com o idioma definido pelo administrador de hub.
Fuso Horário	Selecione o fuso horário do usuário. Ele será padronizado de acordo com o fuso horário definido pelo administrador de hub.
Status do Alerta	Quando ativado, este usuário receberá todos os alertas assinados. Selecione Disable para que esse usuário pare de receber todos os alertas.
Assinados	Este valor é preenchido pelo sistema.
Visibilidade	Selecione Local para que o usuário fique visível apenas dentro da sua organização. Selecione Global para que o usuário fique visível em sua organização e para o gerenciador.

Nota: O idioma e o fuso horário padrão do sistema após a instalação e a inicialização será o idioma inglês (Estados Unidos) em UTC. O sistema utiliza o UTC para calcular o fuso horário. O UTC padrão não pode ser alterado no nível do sistema. No entanto, todos os usuários podem alterar o fuso horário exibido no Community Console.

Quando o usuário *Hubadmin* efetua login no sistema pela primeira vez, o fuso horário e o idioma do sistema são escolhidos (inglês, UTC). Como o usuário Hubadmin é o superusuário responsável pela configuração do sistema, o fuso horário e o código do idioma do Community Console selecionados por ele se tornarão o novo padrão para todos os usuários do Community Console. Usuários individuais também têm a opção de alterar seus fusos horários e seus idiomas de acordo com as suas necessidades.

5. Clique em **Salvar**.

Excluindo Usuários

É necessário ter as permissões adequadas para permitir usuários. Todos os usuários podem ser excluídos utilizando esta funcionalidade, exceto HUBADMIN.

Utilize este recurso para excluir um usuário:

1. Clique em **Administrador de Conta** > **Perfis** > **Usuários**.
2. Clique no ícone **Excluir** em relação ao usuário a ser excluído.
3. Na janela de aviso, clique em **OK** para confirmar sua exclusão. Clicar em **Cancelar** interromperá a exclusão.

Gerenciando Contatos

Utilize o recurso Contatos para visualizar e editar informações de contato para o pessoal chave.

Dependendo do tamanho da sua organização, você provavelmente desejará notificar contatos diferentes quando tipos diferentes de eventos ocorrerem. Por exemplo, quando a validação de um documento falhar, o pessoal da segurança deverá ser notificado para que o problema possa ser avaliado. Quando as transmissões do parceiro interno excederem os limites normais, o administrador da sua rede deverá ser notificado para garantir que o sistema esteja lidando eficientemente com o aumento nas transmissões.

Visualizando ou Editando Detalhes do Contato

1. Clique em **Administrador de Conta** >**Perfis** > **Contatos**. O sistema exibe uma lista dos contatos atuais.

   A tabela a seguir identifica os valores que aparecem na tela Contatos.

Tabela 9. Valores na Tela Lista de Contatos

Valor	Descrição
Nome Completo	O nome completo do contato.
Tipo de Contato	Descreve a função do contato, por exemplo, B2B Lead ou Business Lead.
E-Mail	O endereço de e-mail utilizado para notificações de alerta.
Visibilidade	• Local - O contato fica visível apenas para a sua organização. • Global - O contato é visível para o administrador do hub e para o parceiro interno. Ambos poderão assinar o contato para receber alertas.
Assinados	Se esta opção for selecionada, um ou mais alertas serão designados a este contato. Se o contato for removido do sistema, todas as assinaturas de alerta dele também serão removidas.
Status do Alerta	Quando o Status do Alerta está ativado, este contato recebe todos os alertas assinados.

2. Clique no ícone Visualizar Detalhes para visualizar detalhes do contato. O sistema exibe a tela Detalhes do Contato.
3. Clique no ícone Editar para editar detalhes do contato.
4. Edite as informações como solicitado. A tabela a seguir descreve os valores do contato.

Tabela 10. Detalhes do Contato

Valor	Descrição
Nome Fornecido	O primeiro nome do contato.
Sobrenome	O sobrenome do contato.
Endereço	O endereço do contato, incluindo rua, cidade, estado e CEP.
Tipo de Contato	Descreve a função do contato, por exemplo, B2B Lead ou Business Lead.
E-mail	O endereço de e-mail do contato para notificações de alerta.
Telefone	O número de telefone do contato.
Número de Fax	O número de fax do contato.
Status do Alerta	Quando esta opção está ativada, este contato recebe todos os alertas assinados. Selecione Disable para que esse contato pare de receber todos os alertas.
Assinados	Este valor é preenchido pelo sistema.
Visibilidade	• Local - O contato fica visível apenas para a sua organização. • Global - O contato é visível para o administrador do hub e para o parceiro interno. Ambos poderão assinar o contato para receber alertas.

5. Clique em **Salvar**.

Removendo um Contato

1. Clique em **Administrador de Conta** >**Perfis** > **Contatos**. O sistema exibe uma lista dos contatos atuais.
2. Clique no ícone Excluir para excluir o contato apropriado.

Gerenciando Alertas

Os alertas do WebSphere Partner Gateway são utilizados para notificar o pessoal-chave sobre flutuações incomuns no volume de transmissões recebidas, ou quando ocorrem erros do processamento de documentos comerciais.

Uma opção complementar no módulo Visualizador, Visualizador de Eventos, ajuda a identificar melhor e resolver erros de processamento.

Visualizando ou Editando Detalhes do Alerta e Contatos

O parceiro interno pode visualizar todos os alertas, independente do Proprietário do Alerta (criador).

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Selecione o critério de procura nas listas drop-down. Digite o Nome do Alerta. Você também pode clicar em **Procurar** sem selecionar nenhum critério de procura (o sistema exibirá todos os alertas).
3. Clique em **Procurar**. O sistema exibe a tela Resultados da Procura de Alertas.
4. Clique no ícone Visualizar Detalhes para visualizar detalhes de um alerta.
5. Clique no ícone Editar para editar detalhes do alerta.
6. Edite as informações como solicitado.
7. Clique na guia **Notificar**.
8. Selecione um parceiro (parceiro interno ou administrador do hub, apenas). O parceiro interno pode visualizar todos os alertas, independentemente do Proprietário do Alerta.

9. Edite os contatos deste alerta, se desejar.
10. Clique em **Salvar**.

Procurando Alertas

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Selecione o critério de procura nas listas drop-down. Digite o Nome do Alerta. Você também pode clicar em **Procurar** sem selecionar nenhum critério de procura (o sistema exibirá todos os alertas).

Tabela 11. Critério de Procura de Alertas para Parceiros

Valor	Descrição
Tipo de Alerta	Volume, evento ou todos os tipos de alertas.
Nome do Alerta	O nome do alerta.
Status do Alerta	Os alertas que estão ativados, desativados ou todos.
Contatos Assinados	Os contatos assinados do alerta. As seleções são Há Assinantes, Não Há Assinantes ou Todos.
Resultados por Página	Controla o modo como os resultados da procura são exibidos.

Tabela 12. Critério de procura de alertas para parceiro interno e administrador do hub

Valor	Descrição
Proprietário do Alerta	O criador do alerta.
Alertar Parceiro	O Parceiro ao qual o alerta se aplica.
Tipo de Alerta	Volume, evento ou todos os tipos de alertas.
Nome do Alerta	O nome do alerta.
Status do Alerta	Os alertas que estão ativados, desativados ou todos.
Contatos Assinados	Os contatos assinados do alerta. As seleções são Há Assinantes, Não Há Assinantes ou Todos.
Resultados por Página	Controla o modo como os resultados da procura são exibidos.

3. Clique em **Procurar**. O sistema exibirá uma lista de alertas que atendem ao critério de procura, se houver algum.

Desativando ou Ativando um Alerta

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Selecione o critério de procura nas listas drop-down. Digite o Nome do Alerta.
3. Clique em **Procurar**. O sistema exibirá uma lista de alertas que atendem ao critério de procura, se houver algum.
4. Localize o alerta e clique em **Desativado** ou **Ativado** em Status. Somente o administrador do hub e o Proprietário do Alerta (criador) possuem permissão para editar o Status do alerta.

Removendo um Alerta

1. Clique em **Administrador de Conta** > **Alertas**. O sistema exibe a tela Procurar Alertas.
2. Selecione o critério de procura nas listas drop-down. Digite o Nome do Alerta.
3. Clique em **Procurar**. O sistema exibirá uma lista de alertas que atendem ao critério de procura, se houver algum.

4. Localize o alerta e clique no ícone Excluir para excluir. Somente o administrador do hub e o Proprietário do Alerta (criador do alerta) podem remover um alerta.

Notificação de Evento

O WebSphere Partner Gateway permite configurar um Alerta de Evento, de modo que na ocorrência de um Evento, tanto o Parceiro de Origem quanto o de Destino do evento sejam notificados. Há agora duas opções disponíveis para a Notificação de Alerta. Eles são:

- Notificar Todas as Partes Relacionadas
- Notificar Contatos Assinados Apenas

Quando a opção Notificar Todas as Partes Relacionadas estiver selecionada, o alerta automaticamente notificará os contatos dos Parceiros de Origem e de Destino do Evento, além dos contatos do Proprietário do Alerta. O usuário não precisa (e não está permitido a) especificar ″Contatos Assinados″ quando esse modo está selecionado. Quando o modo Notificar Contatos Assinados Apenas estiver selecionado, o alerta será enviado apenas aos contatos assinados.

Depois de determinar as partes a serem notificadas, poderá especificar se:

- Enviará os alertas imediatamente
- Armazenará os alertas em lote (por contagem ou tempo)

Nota: O servidor de e-mail de Alerta deve ser configurada para utilizar essa funcionalidade adicional. Consulte o *Guia do Administrador do Sistema* para obter instruções sobre como configurar esse servidor.

Gerenciando Endereços

Utilize este recurso para gerenciar os endereços em seu perfil de parceiro.

Editando um Endereço

1. Clique em **Administrador de Conta** > **Perfis** > **Endereços**. O sistema exibe a tela Endereços.
2. Localize o endereço que você deseja editar e clique no ícone Editar.
3. Faça as alterações necessárias. A tabela a seguir descreve os valores dos endereços.

Tabela 13. Valores dos Endereços

Valor	Descrição
Tipo de Endereço	Corporativo, de Faturamento e Técnico
Endereço	O endereço, incluindo rua, cidade, estado e CEP.

4. Clique em **Salvar**.

Excluindo um Endereço

1. Clique em **Administrador de Conta** > **Perfis** > **Endereços**. O sistema exibe a tela Endereços.
2. Localize o endereço que você deseja excluir e clique no ícone Excluir.
3. Verifique se você deseja excluir o endereço.

Capítulo 5. Visualizando Eventos e Documentos: Visualizadores

Os Visualizadores fornecem uma visualização sobre o funcionamento geral do sistema. Eles também são ferramentas de resolução de problemas de eventos.

O módulo Visualizadores inclui os seguintes recursos:

- "Visualizador de Eventos"
- "Visualizador de AS" na página 66
- "Visualizador de ebMS" na página 69
- "Visualizador de RosettaNet" na página 71
- "Visualizador de Documentos" na página 73
- "Fila de Destino" na página 78

Os Visualizadores de RosettaNet e de AS incluem critérios de procura adicionais para a administração de hub. Para obter informações adicionais, consulte o *Administrator Guide*.

Nota: O termo parceiros é utilizado nas telas do Visualizador para identificar um membro da comunidade de hub, incluindo o parceiro interno.

Visualizador de Eventos

O Visualizador de Eventos permite procurar eventos por hora, data, tipo, nome e local. A administração de hub também pode procurar parceiros, IP de Origem e ID de Evento.

Os dados que o Visualizador de Eventos gera identificam, entre outras coisas, o Nome do Evento, o Registro de Data e Hora e o IP de Origem, e permitem visualizar detalhes do evento e do documento para diagnosticar o problema. É possível, também, visualizar o documento não processado, que identifica o campo, o valor e o motivo do erro.

Um evento informa você de que algo incomum ocorreu no sistema. Um evento pode informá-lo de que uma operação ou função do sistema foi bem-sucedida (por exemplo, um parceiro foi incluído com êxito no sistema ou uma conexão do parceiro foi criada com êxito entre os parceiros interno e externo). Um evento também pode identificar um problema (por exemplo, o sistema não pôde processar um documento ou o sistema detectou um erro não-crítico em um documento). A maioria dos documentos é reenviada várias vezes, portanto, quando um documento falha e gera um alerta, trata-se de algo que é necessário investigar e corrigir para evitar que falhas semelhantes ocorram futuramente.

O WebSphere Partner Gateway inclui eventos predefinidos. Utilize o recurso Alertas do produto, módulo Administração de Contas, para criar alertas com base em evento. Esse processo identifica os eventos que o preocupam. Em seguida, utilize o recurso Contatos, também no módulo Administração de Contas, para identificar os membros da equipe a quem o sistema notificará se esses eventos ocorrerem.

O Visualizador de Eventos exibe eventos com base em critérios de procura específicos. É possível localizar um evento específico e, em seguida, pesquisar por que ele ocorreu. O Visualizador de Eventos permite procurar eventos por hora, data, tipo (depuração, informação, aviso, erro e crítico), nome (por exemplo, 210031) e localização.

Os dados disponíveis por meio do Visualizador de Eventos incluem o nome do evento, o registro de data e hora, o usuário e as informações do parceiro. Esses dados o ajudam a identificar o documento ou o processo que criou o evento. Se o evento estiver relacionado a um documento, você também poderá visualizar o documento não processado, que identifica o campo, o valor e o motivo do erro.

Tipo de Eventos

O WebSphere Partner Gateway inclui os seguintes tipos de eventos.

Tabela 14. Tipos de Eventos

Tipo de evento	Descrição
Depuração	Os eventos de depuração são utilizados para suporte e para operações de baixo nível do sistema. A visibilidade e a utilização desses eventos estão sujeitas ao nível de permissão do usuário. Nem todos os usuários têm acesso aos eventos de depuração.
Informações	Os eventos informativos são gerados na conclusão bem-sucedida de uma operação do sistema. Esses eventos também são usados para fornecer o status dos documentos que estão sendo processados no momento. Os eventos informativos não requerem ação do usuário.
Aviso	Os eventos de aviso ocorrem devido a anomalias não-críticas no processamento de documentos ou funções do sistema que permitem que a operação continue.
Erro	Os eventos de erro ocorrem devido a anomalias no processamento de documentos que causam a interrupção do processo.
Crítico	Os eventos críticos são gerados quando os serviços são interrompidos devido a falhas no sistema. Os eventos críticos requerem a intervenção da equipe de suporte.

Executando Tarefas do Visualizador de Eventos

Tabela 15. Tarefas do Visualizador de Eventos

O que você deseja fazer?	Consulte
Procurar eventos.	página 64
Visualizar detalhes do evento.	página 65

Procurando Eventos

1. Clique em **Visualizadores** > **Visualizador de Evento**.

   Os eventos são organizados por gravidade, da esquerda para a direita, na tela Procura de Visualizador de Eventos. As informações à esquerda constituem o tipo de evento com menor gravidade. Os eventos críticos à direita possuem maior gravidade (os eventos de depuração não podem ser visualizados por todos os usuários). Para qualquer evento selecionado, esse e todos os eventos com gravidade maior serão exibidos no Visualizador de Eventos. Por exemplo, se o tipo de evento de Aviso for selecionado no critério de procura, os eventos de Aviso, Erro e Críticos serão exibidos. Se os eventos informativos forem selecionados, todos os tipos de eventos serão exibidos.

2. Selecione o critério de procura nas listas drop-down.

Tabela 16. Critério de Procura do Evento

Valor	Descrição
Data e hora de início	A data e a hora em que o primeiro evento ocorreu. O padrão é 10 minutos antes.
Data e hora de término	Data e a hora em que o último evento ocorreu.
partners	Selecione todos os parceiros ou um parceiro específico (parceiro interno, apenas).
Tipo de evento	Tipo de evento: Depuração, Informação, Aviso, Erro ou Crítico.
Nome do Evento	Procure nomes de eventos disponíveis com base no tipo de evento selecionado.
Localização do evento	A localização na qual o evento foi gerado: todas, desconhecida, origem (de), destino (para).
Classificar por	Valor utilizado para classificar os resultados.
Crescente ou Decrescente	Classifique em ordem crescente ou decrescente.
Resultados por página	Número de registros exibidos por página.
Atualizar	A configuração padrão é Desativada. Quando Atualizar é Ativado, o Visualizador de Eventos executará primeiro uma nova consulta e, em seguida, permanecerá no modo de atualização.
Taxa de Atualização	Controla a freqüência na qual os resultados da procura são atualizados (parceiro interno, apenas).

3. Clique em **Procurar**. O sistema exibe uma lista de eventos.

Dica: A lista de eventos pode ser filtrada novamente com base no tipo de evento selecionado no início da tela Visualizador de Eventos. A próxima atualização de tela refletirá o novo tipo de evento selecionado.

Visualizando Detalhes do Evento

1. Clique em **Visualizadores** > **Visualizador de Evento**.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe uma lista de eventos.
4. Clique no ícone Visualizar Detalhes próximo ao evento que você deseja visualizar. O sistema exibe detalhes do evento e os documentos associados a ele.
5. Clique no ícone Visualizar Detalhes próximo ao documento que você deseja visualizar, se existir algum.
6. Clique no ícone Exibir Documento Não-Processado para visualizar o documento não-processado, se existir algum.
7. Clique no ícone Visualizar Erros de Validação para visualizar erros de validação.

Quando a mensagem de erro ″Nenhum certificado de criptografia válido foi localizado″ é exibida, nem o certificado primário nem o certificado secundário são válidos. Os certificados podem expirar ou podem ter sido anulados. Se os certificados expiraram ou foram anulados, você verá o evento correspondente (Nenhum certificado de criptografia válido foi localizado) no Visualizador de Eventos.

Dica: Se um evento de documento duplicado for exibido em Detalhes do Visualizador de Eventos, visualize o documento original enviado anteriormente, clicando no ícone Visualizar Documento Original em Detalhes do Documento.

Visualizador de AS

Utilize o Visualizador de AS para procurar e visualizar as informações de transporte dos documentos que utilizam os protocolos de comunicação AS1, AS2 ou AS3. É possível visualizar IDs de mensagens, URI de destino e status de MDN (Message Disposition Notification) e detalhes do documento (o documento e o wrapper).

O Visualizador de AS também pode visualizar transações B2B empacotados e detalhes de processos B2B que utilizam o protocolo de comunicação AS1, AS2 ou AS3 (Applicability Statement 1 ou 2). É possível visualizar a coreografia do processo B2B e os documentos comerciais associados, sinais de confirmação, estado do processo, cabeçalhos HTTP e conteúdos dos documentos transmitidos.

Como o seu predecessor AS1, que define um padrão para as transmissões de dados usando SMTP, o AS2 define um padrão para as transmissões de dados usando HTTP.

O AS2 identifica como conectar, distribuir, validar e responder a dados; ele não se preocupa com o conteúdo do documento, apenas com o transporte. O AS2 cria um wrapper em um documento para que ele possa ser transportado pela Internet usando HTTP ou HTTPS. Juntos, o documento e o wrapper são chamados de mensagem. O AS2 fornece segurança e criptografia para pacotes HTTP. O AS2 fornece uma base de criptografia com distribuição garantida. O AS3 fornece um novo padrão para transmitir documentos de modo seguro via FTP ou FTPS.

Um componente importante do AS2 é o mecanismo de recebimento, que é referido como um MDN (Message Disposition Notification). Isso garante ao remetente do documento o recebimento bem-sucedido pelo destinatário. O remetente especifica como o MDN será enviado de volta (de forma síncrona ou assíncrona; assinado ou não).

É possível utilizar o Visualizador de AS para visualizar o ID de mensagem, os registros de data e hora, o Tipo de Documento, o Tipo de Destino, o Status Síncrono, bem como detalhes do documento. Informações adicionais sobre o processamento do documento são exibidas durante a visualização dos detalhes do documento.

Executando Tarefas do Visualizador de AS

Tabela 17. Tarefas do Visualizador de AS1/AS2

O que você deseja fazer?	Consulte
Procurar mensagens AS	página "Procurando Mensagens"
Visualizando Documentos Originais	página "Visualizando Detalhes da Mensagem" na página 68

Procurando Mensagens

1. Clique em **Visualizadores** > **Visualizador de AS**. O sistema exibe a tela Visualizador de AS.

2. Selecione o critério de procura nas listas drop-down.

Tabela 18. Critérios de Procura do Visualizador de AS

Valor	Descrição
Data e Hora de Início	Data e a hora em que o processo foi iniciado.
Data e Hora de Término	Data e hora em que o processo foi concluído.
Parceiro de Origem	Identifica o parceiro de transmissão (parceiro interno apenas)
Parceiro de Destino	Identifica o parceiro de recepção.
Procurar em	Especifica se o documento a ser procurado é o tipo de documento de origem ou de destino.
ID do Negócio de Origem de AS	O número de identificação de negócio do parceiro de origem, por exemplo, Duns.
ID do Negócio de Origem da Carga Útil	Número de identificação de origem da carga útil.
Modo de Operação	Produção, Teste, Parceiro Externo do Simulador de RN ou Parceiro Interno do Simulador de RN. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Pacote	Descreve o formato, o empacotamento, a criptografia e a identificação do tipo de conteúdo do documento.
Protocolo	Formato de documento disponível para os parceiros, por exemplo, RosettaNet de XML.
Tipo de Documento	O processo de negócios específico.
ID da Mensagem	O número de ID designado ao documento empacotado AS1, AS2 ou AS3. O critério de procura pode incluir o caractere curinga asterisco (*). Comprimento máximo, 255 caracteres.
ID de Documento	O número de identificação exclusivo designado ao documento.
Síncrono / Assíncrono	Procura por documentos recebidos no modo síncrono e assíncrono. O modo síncrono significa que a conexão entre o iniciador e o Gerenciador de Documentos permanece aberta até que a transação seja concluída, incluindo o pedido e o MDN (Message Disposition Notification).
Status do MDN	Esse campo permite selecionar o status do MDN nessa mensagem.
Classificar por	Classificar os resultados por este valor.
Decrescente ou Crescente	Crescente - Exibe primeiro a data e a hora mais antiga ou o final do alfabeto. Decrescente - Exibe a data e a hora mais recente ou o início do alfabeto.
Resultados por página	Utilize para selecionar o número de registros exibidos por página.

3. Clique em **Procurar**. O sistema exibe uma lista de mensagens.

Visualizando Detalhes da Mensagem

1. Clique em **Visualizadores** > **Visualizador de AS**. O sistema exibe a tela Visualizador de AS.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe uma lista de mensagens.
4. Clique no ícone Visualizar Detalhes próximo à mensagem que você deseja visualizar. O sistema exibe a mensagem e os detalhes dos documentos associados a ela.

Tabela 19. Visualizador de AS: Detalhes do Pacote

Valor	Descrição
ID da Mensagem	O número de ID designado ao documento empacotado AS1, AS2 ou AS3. Esse número identifica apenas o pacote. O próprio documento possui um número de ID de documento que é exibido durante a visualização dos detalhes do documento. Comprimento máximo, 255 caracteres.
Parceiro de Origem	Parceiro que inicia um processo de negócios.
Parceiro de Destino	Parceiro que recebe o processo de negócio.
A data e a hora de Origem	A data e a hora em que o documento começa a ser processado.
Tipo de Destino	Teste ou produção. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
URI do MDN	O endereço de destino do MDN. O endereço pode ser especificado como um URI de HTTP ou como um endereço de e-mail.
Texto de Disposição do MDN	Este texto fornece o status da mensagem original que foi recebida (com êxito ou com falha). Os exemplos incluem: • Automatic-=action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically;processed/Warning;duplicate-document. • Automatic-action/MDN-sent-automatically;processed/Error;description-failed. • Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Opcional) Clique no ícone Exibir Documento Não-Processado para visualizar o documento não-processado.

Visualizador de ebMS

O mecanismo ebMS (ebXML Message Service) fornece uma maneira padrão de trocar Mensagens de negócios entre os Parceiros Comerciais ebXML. Fornece uma forma confiável de trocar mensagens comerciais sem depender das tecnologias e soluções de proprietário. Uma mensagem ebXML contém estruturas de um cabeçalho da mensagem (necessário para roteamento e entrega) e uma seção de carga útil. O ebMS fornece uma forma padrão de trocar mensagens comerciais entre Parceiros Comerciais do ebXML. Uma mensagem ebXML é um envelope de mensagem MIME/Multipart independente de protocolo de comunicação

Executando Tarefas do Visualizador ebMS

Tabela 20. tarefas do Visualizador ebMS

O que você deseja fazer?	Consulte
Procurar Processos ebMS	"Procurando Processos do ebMS"
Visualizar Processos ebMS	"Visualizar Detalhes do Processo ebMS" na página 70
Visualizar Documentos Brutos	"Visualizar Documentos Brutos" na página 70
Visualizando Status do Documento	"Visualizando o Status do Documento" na página 71

Procurando Processos do ebMS

1. Clique em **Visualizadores** > **Visualizador de ebMS**. O sistema exibe a tela de Procura do Visualizador de ebMS.

2. Selecione o critério de procura nas listas drop-down.

Valor	Descrição
Data e Hora de Início	A data e a hora em que o processo foi iniciado.
Data e Hora de Término	A data e a hora em que o processo foi concluído.
Parceiro de Origem	Identifica o parceiro de envio.
Parceiro de Destino	Identifica o parceiro de recepção.
ID do Negócio de Origem	O número de identificação de negócio do parceiro iniciador, por exemplo, DUNS.
Modo de Operação	Produção, teste, Parceiro Externo do Simulador RN ou Parceiro Interno do Simulador RN. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Protocolo	Protocolos disponíveis para os parceiros.
Tipo de Documento	Tipo de documento a ser processado.
ID de Conversação	A informação de identificação exclusiva designada ao processo. O critério pode incluir o caractere curinga asterisco (*).
Classificar por	Classificar resultados, por exemplo, por Data e Hora Recebido.
Decrescente ou Crescente	Crescente - Exibe primeiro a data e a hora mais antiga ou o final do alfabeto. Decrescente - Exibe a data e a hora mais recente ou o início do alfabeto.
Resultados por Página	Exibe n números de resultados por página.

3. Clique em **Procurar**. O sistema exibe os processos de ebMS que correspondem a seu critério de procura.

Visualizar Detalhes do Processo ebMS

1. Clique em **Visualizadores > Visualizador de ebMS**. O sistema exibe a tela do Visualizador de ebMS.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe os resultados da sua procura.

Tabela 21. Valores de critério de procura do Visualizador de ebMS

Valor	Descrição
Parceiros	Parceiros envolvidos no processo de negócios.
Time Stamp de Origem	A data e a hora em que o primeiro documento começa a ser processado.
Tipo de Documento	O processo comercial específico, por exemplo: ebMS 2.0 : Produção de ALMService
Modo de Operação	Modo de Operação, por exemplo: Produção
ID de Conversação	Número de identificação exclusivo atribuído a esse evento

Visualizar Documentos Brutos

Para visualizar o documento bruto:

1. Clique em **Visualizadores > Visualizador de ebMS**.
2. Selecione o critério de procura a partir das listas drop-down, consulte "Procurando Processos do ebMS" na página 69

3. Clique em **Procurar**.
4. Clique no ícone "**Clique para visualizar documento bruto**" sob a seção **Legenda**.

- Para resolver problemas com documentos que falharam durante o processamento, consulte "Visualizando Erros de Validação de Dados" na página 76.
- O visualizador de documentos não processados exibe o cabeçalho HTTP com o documento não processado.

Visualizando o Status do Documento

1. Clique em **Visualizadores > Visualizador de ebMS**.
2. Selecione o critério de procura a partir das listas drop-down, consulte "Procurando Processos do ebMS" na página 69
3. Clique em **Procurar**.
4. Clique em **Status do Pedido**.
5. Clique em **Visualizar Status**.

Visualizador de RosettaNet

Utilize o Visualizador de RosettaNet para localizar o processo específico que gerou um evento. Ao identificar o processo de destino, é possível visualizar os detalhes dele, bem como o documento não processado.

O RosettaNet é um grupo de empresas que criaram um padrão de mercado para transações de e-business. Os PIPs (Partner Interface Processes) definem os processos comerciais entre os membros da comunidade de hub. Cada PIP identifica um documento comercial específico e o modo como ele é processado entre o parceiro interno e os parceiros externos.

O Visualizador de RosettaNet exibe a coreografia dos documentos que constituem um processo de negócios. Os valores que podem ser visualizados com o Visualizador de RosettaNet incluem o estado, os detalhes, os documentos não processados e os eventos do processo associados.

O Visualizador de RosettaNet exibe os processos com base em critérios de procura específicos.

Executando Tarefas do Visualizador de RosettaNet

Tabela 22. Tarefas do Visualizador de RosettaNet

O que você deseja fazer?	Consulte
Procurar processos de RosettaNet.	página 71
Visualizar detalhes do processo de RosettaNet.	página 72
Visualizar documentos não processados.	página 73

Procurando Processos de RosettaNet

1. Clique em **Visualizadores** > **Visualizador de RosettaNet**. O sistema exibe a tela Procurar Visualizador de RosettaNet.

2. Selecione o critério de procura nas listas drop-down. START HERE

Tabela 23. Critério de Procura de RosettaNet

Valor	Descrição
Data e Hora de Início	A data e a hora em que o processo foi iniciado.
Data e Hora de Término	A data e a hora em que o processo foi concluído.
Parceiro de Origem	Identifica o parceiro de envio.
Parceiro de Destino	Identifica o parceiro de recepção.
ID do Negócio de Origem	O número de identificação de negócio do parceiro iniciador, por exemplo, DUNS.
Modo de Operação	Produção, teste, Parceiro Externo do Simulador RN ou Parceiro Interno do Simulador RN. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Protocolo	Protocolos disponíveis para os parceiros.
Tipo de Documento	Tipo de documento a ser processado.
ID de Instância de Processo	O número de identificação exclusivo designado ao processo. O critério pode incluir o caractere curinga asterisco (*).
Classificar por	Classificar resultados, por exemplo, por Data e Hora Recebido.
Decrescente ou Crescente	Crescente - Exibe primeiro a data e a hora mais antiga ou o final do alfabeto. Decrescente - Exibe a data e a hora mais recente ou o início do alfabeto.
Resultados por Página	Exibe n números de resultados por página.

3. Clique em **Procurar**. O sistema exibe os processos de RosettaNet que atendem ao seu critério de procura.
4. Clique no ícone Visualizar Detalhes próximo ao processo ebMS que você deseja visualizar. O sistema exibe detalhes e documentos associados ao processo selecionado.
5. Clique no ícone Visualizar Detalhes próximo ao documento que você deseja visualizar. O sistema exibe o documento e os detalhes dos eventos associados a ele.

Visualizando Detalhes do Processo de RosettaNet

1. Clique em **Visualizadores** > **Visualizador de RosettaNet**. O sistema exibe a tela Procurar Visualizador de RosettaNet.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe os resultados da sua procura.

Tabela 24. Detalhes do Processamento de Documentos

Valor	Descrição
Parceiros	Parceiros envolvidos no processo de negócios.
Registro de Data e Hora	A data e a hora em que o primeiro documento começa a ser processado.
Tipo de Documento	O processo de negócios específico, por exemplo, RosettaNet (1.1): 3A7.
Tipo de Destino	Por exemplo, Produção.
ID de Instância de Processo	Número exclusivo designado ao processo pelo membro da comunidade de origem.
ID de Documento	O identificador de documento do proprietário designado pelo parceiro que envia. O campo não está em um local fixo e varia de acordo com o tipo de documento.
Parceiro de Origem	Parceiro Iniciador.
Parceiro de Destino	Parceiro de Recebimento.

4. Clique no ícone Visualizar Detalhes próximo ao processo RosettaNet que você deseja visualizar. O sistema exibe detalhes e documentos associados ao processo selecionado.
5. Clique no ícone Visualizar Detalhes próximo ao documento que você deseja visualizar. O sistema exibe o documento e os detalhes dos eventos associados a ele.

Visualizando Documentos Não Processados

1. Clique em **Visualizadores** > **Visualizador de RosettaNet**. O sistema exibe a tela Procurar Visualizador de RosettaNet.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe uma lista de processos.
4. Clique no ícone Visualizar Detalhes próximo ao processo que você deseja visualizar. O sistema exibe detalhes e documentos associados ao processo selecionado.
5. Clique no ícone Exibir Documento Bruto próximo ao Tipo de Documentos para exibir o documento bruto.

Restrições: Os documentos não processados maiores que 100 K são truncados.

Dica:

- Para resolver problemas com documentos que falharam durante o processamento, consulte "Visualizando Erros de Validação de Dados" na página 76.
- O visualizador de documentos não processados exibe o cabeçalho HTTP com o documento não processado.

Visualizador de Documentos

O Visualizador de Documentos é utilizado para localizar e visualizar um documento específico que você deseja pesquisar. É possível procurar documentos por data, hora, tipo de processo (Processo de Origem ou Processo de Destino), conexão do parceiro, tipo de destino, status do documento, protocolo, tipo de documento e versão do processo.

Alguns protocolos, como XML (Extensible Markup Language) customizado que utiliza os formatos do XML, podem extrair informações dos documentos e salvá-las de modo que você as procure utilizando o Visualizador de Documentos. Essa é a finalidade dos atributos do campo de procura do usuário numa definição de formato XML. No caso do documento roteado que utiliza um formato XML incluir campos de procura, as informações do documento obtidas por meio dos campos de procura podem ser o destino de uma procura. Um exemplo é um documento XML customizado que é uma ordem de compra. Por meio do seu conhecimento da estrutura do documento, é possível definir um formato de XML com um campo de procura que extraia o número da ordem de compra. Quando documentos são roteados utilizando esse formato de XML, é possível procurá-los utilizando o número da ordem de compra, digitando o número no campo de procura Definido pelo Usuário apropriado, na tela de procura do Visualizador de Documentos.

Também é possível definir o roteamento de documentos EDI (Electronic Data Interchange) que extrai informações do documento. Isso pode ser feito pela

codificação de um mapa DIS de modo que ele seja preenchido pelos valores dos campos de procura Definidos pelo Usuário.

Também é possível gravar uma saída de usuário que extrairá as informações do documento de modo que elas possam ser o destino de uma procura. Use o método de saída do usuário BusinessDocumentInterface.setAttribute() para preencher os valores dos campos de procura Definidos pelo Usuário.

Os resultados da procura exibem todos os documentos que satisfazem os critérios de procura e identificam os registros de data e hora, o processo, a conexão do parceiro e os tipos de destino. Localize o documento de destino e utilize os recursos do visualizador para visualizar o documento não processado. É possível, também, utilizar o Visualizador de Documentos para reenviar documentos que falharam ou que obtiveram êxito.

Procurando Documentos

1. Clique em **Visualizadores** > **Visualizador de Documento**. O sistema exibe a tela Procurar Visualizador de Documentos.
2. Selecione o critério de procura nas listas drop-down.

Tabela 25. Critério de Procura do Visualizador de Documentos

Valor	Descrição
Data e hora de início	Data e a hora em que o processo foi iniciado.
Data e hora de término	Data e hora em que o processo foi concluído.
Parceiro de Origem	Identifica o parceiro de envio.
Parceiro de Destino	Identifica o parceiro de recepção. .
Procurar em	Procurar no tipo de documento de Origem ou de Destino.
Modo de Operação	Produção, teste, Parceiro Externo do Simulador RN ou Parceiro Interno do Simulador RN. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Status do documento	Status do documento atual no sistema. É possível escolher Em Andamento, Bem-sucedido ou Com Falha. O padrão é Todos.
Pacote	Descreve o formato, o empacotamento, a criptografia e a identificação do tipo de conteúdo do documento.
Protocolo	Tipo de protocolo de processo disponível para os parceiros.
Tipo de Documento	O processo de negócios específico.
ID de Documento	Criado pelo parceiro de origem. O critério pode incluir o caractere curinga asterisco (*).
ID de Referência	Número de ID criado pelo sistema para monitorar o status do documento.
Endereço IP de Origem	Endereço IP do parceiro de origem.
Filtrar	Procurar documentos recebidos no modo síncrono. Isso significa que a conexão entre o iniciador e o Gerenciador de Documentos permanece aberta até que a transação seja concluída, incluindo o pedido e a confirmação ou o pedido e a resposta.
Classificar por	Valor utilizado para classificar os resultados.
Resultados por página	Número de registros exibidos por página.
Decrescente	Classificar resultados em ordem decrescente ou crescente.
Campos de Procura Definidos pelo Usuário	Desempenhe a procura com base nos critérios definidos pelo usuário.

Nota: Os eventos de aviso são exibidos por padrão. Para ver todos os eventos, selecione Depurar.

3. Clique em **Procurar**. O sistema exibe uma lista de documentos que atendem ao seu critério de procura.

Tabela 26. Informações Disponíveis sobre o Documento Utilizando o Visualizador de Documentos

Valor	Descrição
Parceiros	Os parceiros de origem e de destino envolvidos no processo comercial.
Registro de Data e Hora	A data e a hora em que o processamento do documento é iniciado e concluído.
Tipo de Documento	O processo de negócios que está sendo efetuado.
Tipo de Destino	Teste ou produção. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Síncrona	Identifica que o documento foi recebido no modo síncrono. Isso significa que a conexão entre o iniciador e o Gerenciador de Documentos permanece aberta até que a transação seja concluída, incluindo o pedido e a confirmação ou o pedido e a resposta.

Visualizando Detalhes do Documento, Eventos e Documentos Não Processados

1. Clique em **Visualizadores** > **Visualizador de Documento**. O sistema exibe a tela Procurar Visualizador de Documentos.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe uma lista de documentos.
   - Para visualizar detalhes e eventos de um documento, clique no ícone de pasta aberta ao lado do documento exibido sob o cabeçalho Documentos Associados. O sistema exibe detalhes e eventos do processo para o documento selecionado. Para documentos EDI Interchange, se houver transações EDI filhas da remoção de envelope ou envelopamento, elas poderão ser mostradas selecionando o botão de rádio de origem ou destino **Filhos de documentos**. Consulte o *Administrator Guide* para obter mais informações sobre como visualizar documentos EDI.
   - Para visualizar o documento não-processado com cabeçalho HTTP, clique no ícone Exibir Documento Não-Processado próximo ao documento. O sistema exibe o conteúdo do documento não processado.

As seguintes informações de processamento do documento são exibidas durante a visualização de detalhes do documento:

Tabela 27. Valores de Processamento do Documento Disponíveis com o Visualizador de Documentos

Valor	Descrição
ID de Referência	O número de identificação exclusivo designado ao documento pelo sistema.
ID de Documento	O número de identificação exclusivo designado ao documento pelo parceiro de origem.
A Data e Hora do Documento	A data e hora em que o documento foi criado pelo parceiro.
Destino	O destino pelo qual o documento foi transmitido.

Tabela 27. Valores de Processamento do Documento Disponíveis com o Visualizador de Documentos (continuação)

Valor	Descrição
Tipo de Documento de Conexão	Ações executadas em um documento pelo sistema para assegurar sua compatibilidade com os requisitos comerciais entre os parceiros.
Origem e Destino	Os parceiros de origem e de destino envolvidos no processo comercial.
Em Registro de Data e Hora	A data e hora em que o documento foi recebido pelo sistema do parceiro.
A Data e Hora do Estado Final	A data e hora em que o documento foi roteado com êxito pelo sistema para o parceiro de destino.
ID de Negócio de Origem e Destino	O número de identificação de negócio dos parceiros de Origem e de Destino, por exemplo, DUNS.
Tipo de Documento de Origem e Destino	O processo comercial específico efetuado entre os parceiros de origem e destino.

Restrições: Os documentos não processados maiores que 100 K são truncados.

Dica: Se o sistema exibir um evento Documento Duplicado, visualize o documento original enviado anteriormente, selecionando o ícone de seta azul próximo ao evento Documento Duplicado e, em seguida, clique no ícone Visualizar Documento Original.

Dica: Para resolver problemas com documentos que falharam durante o processamento, consulte "Visualizando Erros de Validação de Dados" na página 76.

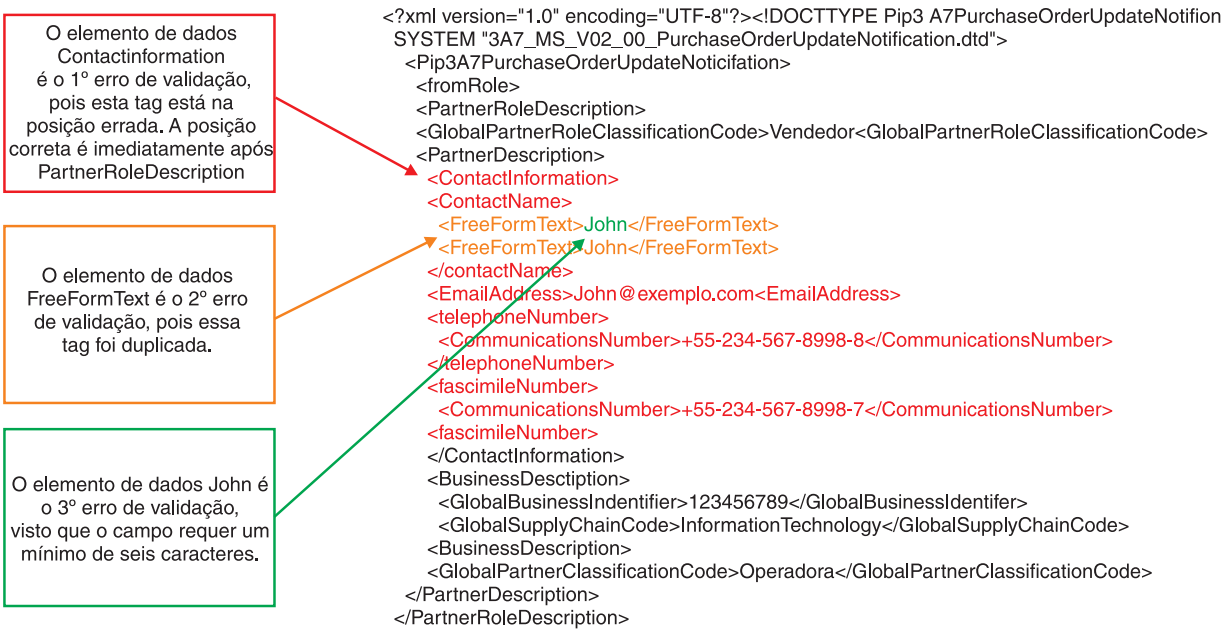
Visualizando Erros de Validação de Dados

É possível procurar rapidamente documentos cujo processamento falhou usando textos codificados por cores em campos XML que contenham erros de validação. Os campos que contêm erros de validação são exibidos em vermelho. Se ocorrerem até três erros de validação diferentes dentro de campos XML aninhados, as seguintes cores serão usadas para a distinção entre os campos de erro:

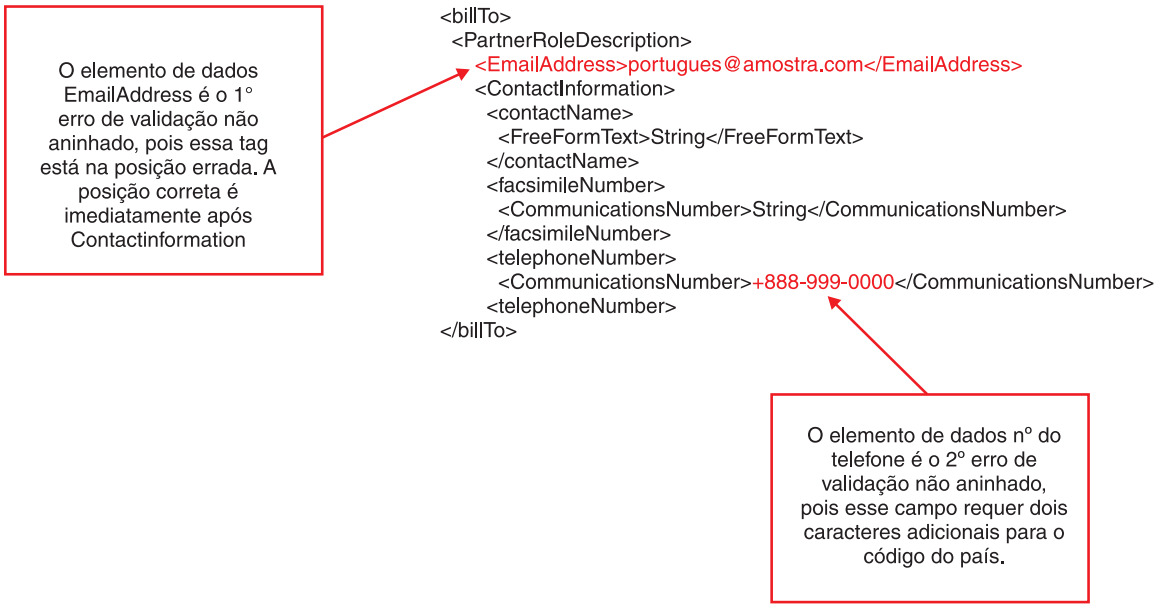
Tabela 28. Erros de Validação de Documentos Codificados por Cores

Valor	Descrição
Vermelho	Primeiro erro de validação
Laranja	Segundo erro de validação
Verde	Terceiro erro de validação

A seguir, um exemplo de erros de validação XML aninhados:



Exemplo de erros de validação XML não-aninhados:



Para visualizar os erros de validação em um documento não processado, consulte "Visualizando Documentos Não Processados" na página 73.

Restrições: O console exibe apenas os primeiros 100 KB de um documento não processado. Os erros de validação acima de 100 KB não podem ser visualizados.

Utilizando o Recurso Parar Processo

Clique em **Parar Processo** para interromper um documento que está atualmente em andamento. Esse recurso não está restrito apenas para usuário hubadmin. As permissões do grupo precisam ser configuradas para disponibilizar esse recurso.

Nota: A interrupção do documento pode levar até uma hora. Durante este tempo, o Visualizador de Documentos continuará a exibir o status do documento como em andamento.

Fila de Destino

A Fila de Destino permite visualizar os documentos enfileirados para entrega a partir de qualquer destino no sistema. Também permite visualizar todos os destinos que possuem documentos enfileirados para entrega, exibir e remover documentos em uma fila e ativar ou desativar destinos.

A Fila de Destinos pode ser utilizada para assegurar que documentos sensíveis à hora não fiquem parados na fila. Também pode ser utilizada para assegurar que o número máximo de documentos a serem enfileirados não seja excedido. Com a Fila de Destino, é possível:

- Ver uma lista de todos os destinos que contêm documentos enfileirados para entrega
- Visualizar um documento que ficou em uma fila de destino durante um período de tempo estendido (30 segundos ou mais). Isso pode indicar um problema com o documento propriamente dito. É possível, também, visualizar detalhes do documento para resolver problemas da fila.

  Nota: Se você estiver implementando um Destino de Script de FTP com um planejamento de calendário ou intervalo, os documentos poderão ficar nesta fila por um longo período, até que esse intervalo ou data e hora seja atingido. Esta é a operação esperada e os documentos não deverão ser removidos da fila.
- Visualize os detalhes do destino de modo a garantir a operação apropriada. Os documentos que fazem backup em uma Fila de Destino podem indicar uma falha no gerenciador de entrega ou no destino.
- Confirme o status do destino. Um destino off-line faz com que os documentos sejam coletados na fila até que o destino fique on-line. O status do destino não afeta a funcionalidade da conexão e os documentos continuarão a ser processados e colocados na fila para entrega.
- Limite o tamanho da lista Fila de Destino com os campos **Nome do Parceiro** e **Destino**.

Visualizando a Lista de Destinos

Para visualizar uma lista de documentos que residem no destino, utilize o seguinte procedimento:

1. Selecione **Visualizadores** > **Fila de Destino**. O Console exibe a janela Fila de Destino.

2. Insira os parâmetros mostrados na Tabela 29.

Tabela 29. Janela Fila de Destino

Critérios	Descrição
Nome do Parceiro	Para concluir este campo, você pode: 1. Especifique o nome do Parceiro. 2. Especificar parte do nome do parceiro nesse campo e, em seguida, clicar em **Mostrar Parceiros**. Selecione o parceiro na lista de parceiros. 3. Especificar o curinga * e clicar em **Mostrar Parceiros**. Selecione o parceiro na lista de parceiros. Clicar em **Mostrar Parceiros** exibe um campo Parceiro na página. O campo**Parceiro** lista todos os parceiros disponíveis em ordem alfabética.
Destino	O primeiro item na lista é `Todos`, que é selecionado por padrão. O restante da lista está em uma lista ordenada de transportes de destino. Nessa lista, você pode selecionar apenas um único destino. O padrão é `Todos`. **Nota:** A lista Destino é automaticamente preenchida com os destinos do parceiro selecionado e a lista é apresentada em ordem alfabética.
Enfileirado pelo menos	Número mínimo de minutos que um documento ficou aguardando na fila de destino. Por exemplo, se 6 minutos for selecionado, todos os destinos contendo documentos que ficaram aguardando pela entrega durante 6 minutos ou mais serão exibidos. O padrão é `0`.
Classificar por	Classifica resultados da procura por parceiro (padrão) ou Nome de Destino.
Atualizar	Ativar ou desativar (padrão) a atualização.
Mínimo Enfileirado	Número mínimo de documentos em uma fila de destino. O padrão é `1`.
Direção	Clique em **Ascendente** para exibir documentos iniciando com a data e a hora mais antiga ou o final do alfabeto ou **Descendente** para exibir documentos iniciando com a data e a hora mais recente ou o início do alfabeto.
Taxa de Atualização	Número de segundos que o Console aguarda antes de atualizar os dados exibidos.

3. Clique em **Procurar**. O sistema localiza todos os documentos no destino que correspondem aos critérios de procura. A **Tabela 30** mostra as informações retornadas da procura.

Tabela 30. Resultados Depois da Procura na Fila de Destino

Critérios	Descrição
Parceiro	Parceiro comercial associado ao destino
Destino	Nome do destino
Enfileirado	Número de documentos na fila de destino aguardando pela entrega. Link para os detalhes do destino
Estado	Mostra se o destino está on-line ou off-line
Último Envio	Última data e hora em que um documento foi enviado ao destino com êxito

Nota: Para que o Console exiba um destino, o destino deve atender a todos os requisitos dos critérios de procura utilizando a lógica AND.

Visualizando Documentos Enfileirados

Para visualizar documentos enfileirados para um Parceiro específico:

1. Clique em **Visualizadores** > **Fila de Destino**.
2. Na janela Procura de Fila de Destinos, clique em **Procura de Documentos**.
3. Na janela Procura de Documentos da Fila, especifique os critérios de procura (consulte a Tabela 31 na página 80).

Tabela 31. Janela Procura de Documentos da Fila

Critérios	Descrição
Nome do Parceiro	Para concluir este campo, você pode: 1. Especificar o nome do Parceiro no campo. 2. Especificar parte do nome do parceiro nesse campo e, em seguida, clicar em **Mostrar Parceiros**. Selecione o parceiro a partir da lista. 3. Especificar o curinga * e clicar em **Mostrar Parceiros**. Selecione o parceiro na lista de parceiros. **Nota:** Clicar em **Mostrar Parceiros** exibe um campo Parceiro na página. O campo**Parceiro** lista todos os parceiros disponíveis em ordem alfabética.
Destino	O primeiro item na lista é `Todos`, que é selecionado por padrão. O restante da lista está em uma lista ordenada de transportes de destino. Nessa lista, você pode selecionar apenas um único destino. O padrão é `Todos`. **Nota:** A lista Destino é automaticamente preenchida com os destinos do parceiro selecionado e a lista é apresentada em ordem alfabética.
Classificar por	Selecione se a lista deve ser classificada por Parceiro (o padrão), por Destinos, por ID de Referência ou por Registro de Data e Hora Enfileirado (a hora em que o documento foi enviado pela última vez).
ID de Referência	Digite o número de identificação exclusivo designado ao documento pelo sistema.
Direção	Clique em **Ascendente** para exibir documentos iniciando com a data e a hora mais antiga ou o final do alfabeto ou **Descendente** para exibir documentos iniciando com a data e a hora mais recente ou o início do alfabeto.
ID de Documento	Digite o número de identificação exclusivo designado ao documento pelo parceiro de origem.
Resultados por Página	Especifica o número de documentos exibidos em uma página.
Máximo de Documentos Permitidos	Especifica o número de registros a serem exibidos.

4. Clique em **Procurar**. Os resultados das procuras nas filas são exibidos.

Removendo Documentos da Fila de Entrega

O procedimento a seguir descreve como remover documentos da fila de entrega. É necessário efetuar login como administrador de hub para remover documentos da fila.

1. Clique em **Visualizadores** > **Fila de Destino**.
2. Na janela Fila de Destinos, clique em **Procurar**.
3. Preencha os parâmetros na janela (consulte a Tabela 30 na página 79).
4. Clique no ícone Excluir para excluir o documento.

Visualizando os Detalhes do Destino

Para visualizar informações sobre um determinado destino, incluindo uma lista de documentos na fila, utilize o seguinte procedimento:

1. Clique em **Visualizadores** > **Fila de Destino**.
2. Na janela Fila de Destino, digite os critérios de procura (consulte a Tabela 29 na página 79).
3. Clique em **Procurar**.
4. Na lista de destinos, clique no link de contagem de documentos na coluna **Enfileirado**. Os detalhes do destino e uma lista de documentos enfileirados aparecem.

Alterando o status de destino

Para colocar um destino on-line ou off-line, utilize o seguinte procedimento:

1. Clique em **Visualizadores** > **Fila de Destino**.
2. Na janela Fila de Destino, digite os critérios de procura (consulte a Tabela 29 na página 79).
3. Clique em **Procurar**.
4. Na lista de destinos, clique no link de contagem de documentos na coluna **Enfileirado**. Os detalhes do destino e uma lista de documentos enfileirados aparecem.
5. Clique em **On-line** em **Informações do Destino** para colocar um destino off-line ou clique em **Off-line** para colocar o destino on-line. (É necessário efetuar login como administrador de hub para alterar o status do destino.)

Capítulo 6. Analisando o Tipo de Documento: Ferramentas

Utilize a ferramenta Análise de Documento para obter uma visão geral detalhada sobre o número de documentos no sistema, por estado (Recebido, Em Andamento, Com Falha e Bem-sucedido). O critério de procura inclui a data, a hora, o tipo de processo (Origem ou Destino), o tipo de destino, o protocolo, o tipo de documento e a versão do processo. Utilize os resultados da procura para localizar e visualizar os documentos que obtiveram falha, para investigar o motivo das falhas.

O Relatório de Volume do Documento é uma ferramenta valiosa usada para gerenciar, rastrear e resolver problemas com o fluxo de documentos comerciais. O relatório exibe o volume de documentos processados pelo sistema em um período de tempo específico. Este relatório pode ser visualizado, impresso e salvo (exportado) para ser enviado para outros membros da equipe. É possível personalizá-lo para visualizar informações com base em critérios de procura específicos.

A ferramenta Testar Conexão do Parceiro é usada para testar o destino ou o servidor da Web.

Tabela 32. Ferramentas

Qual recurso você deseja utilizar?	**Consulte**
Análise de Documento	página 83
Relatório de Volume de Documentos	página 86
Testar Conexão do Parceiro	página 87
Relatórios EDI	página 90
Relatórios do FTP	página 94

Análise de Documento

Utilize a ferramenta Análise de Documento para obter uma visão geral detalhada sobre o número de documentos no sistema, por estado, em um período de tempo específico.

Utilize o critério de procura para localizar documentos com falha e investigar o motivo das falhas.

A tela Análises do Documento inclui um alarme. Se um processo falhar, a linha que contém o processo que obteve a falha piscará em vermelho.

Estados do Documento

A tabela a seguir descreve os diferentes estados do documento.

Tabela 33. Status do Documento

Estado	Descrição
Recebido	O documento foi recebido pelo sistema e está aguardando o processamento.
Em Andamento	No momento o documento está em uma das seguintes etapas de processamento: • **Incompleto**. Por exemplo, o sistema está aguardando outros documentos. • **Validação de Dados**. Por exemplo, o sistema está verificando o conteúdo do documento. • **Conversão**. Por exemplo, o sistema está convertendo o documento para outro protocolo. • **Fila**. Por exemplo, o documento está aguardando para ser roteado para o parceiro interno ou externo.
Com Falha	O processamento do documento foi interrompido devido a erros no sistema, validação de dados ou duplicações.
Bem-sucedido	A mensagem final que conclui o processamento do documento foi transmitida do sistema para o parceiro de destino.

Visualizando Documentos no Sistema

1. Clique em **Ferramentas** > **Análise do Documento**. O sistema exibe a tela Procurar Análises do Documento.
2. Selecione o critério de procura nas listas drop-down.

Tabela 34. Critério de Procura do Documento

Valor	Descrição
Data e Hora de Início	A data e a hora em que o processo foi iniciado.
Data e Hora de Término	A data e a hora em que o processo foi concluído.
Parceiro de Origem	O parceiro que iniciou o processo de negócios (parceiro interno, apenas).
Parceiro de Destino	O parceiro que recebeu o processo de negócios (parceiro interno, apenas).
Procurar em	Procurar no tipo de documento de origem ou de destino.
Tipo de Destino	Por exemplo, Produção ou Teste. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Pacote	Descreve o formato, o empacotamento, a criptografia e a identificação do tipo de conteúdo do documento.
Protocolo	Protocolo de documento disponível para os parceiros.
tipo de documento	O processo de negócios específico.
Classificar por	Classifica os resultados por Nome de Parceiro de Origem ou de Destino.
Atualizar	Controla se os resultados da procura são atualizados periodicamente (parceiro interno, apenas).
Taxa de Atualização	Controla a freqüência na qual os resultados da procura são atualizados (parceiro interno, apenas).

3. Clique em **Procurar**. O sistema exibe o Resumo de Análise do Documento.

Visualizando Detalhes do Evento e do Processo

1. Clique em **Ferramentas** > **Análise do Documento**. O sistema exibe a tela Procurar Análises do Documento.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe o Resumo de Análise do Documento.
4. Clique no ícone Visualizar Detalhes próximo aos parceiros de Origem e Destino que você deseja visualizar. O sistema exibe uma lista de todos os documentos para os parceiros selecionados. A quantidade do documento é organizada em colunas pelo estado de processamento do documento.
5. Selecione o link de quantidade nas colunas Recebido, Em Andamento, Com Falha ou Bem-sucedido. O sistema apresenta detalhes do processamento do documento no Relatório de Análise do Documento. Se você tiver selecionado Com Falha, o relatório também incluirá um Resumo dos Eventos do Documento.

Processamento do Arquivo XML Customizado

O WebSphere Partner Gateway V6.0 e versões anteriores forneciam suporte para processamento de Linguagem de marcação extensível (XML) utilizando formatos XML. O WebSphere Partner Gateway V6.0 e os formatos XML anteriores não permitem o uso completo da linguagem de expressão XPath para extrair informações de processamento dos documentos. Por isso o WebSphere Partner Gateway V6.1 recriou o modo como esses formatos XML funcionam. No WebSphere Partner Gateway V6.1, as expressões XPath versão 1.0 podem ser utilizadas nos formatos. O processamento ampliado com suporte completo de XPath limita o tamanho dos arquivos que podem ser utilizados com os formatos XPath XML completos. Para permitir que arquivos grandes sejam processados, você tem a opção de definir isso ao definir uma família de documento. Os formatos em uma família com a opção de processamento de arquivos grandes possuem o mesmo processamento restrito de XPath fornecido pelo WebSphere Partner Gateway V6.0 e versões, mas os arquivos grandes podem ser processados. Quando a opção de arquivo grande é utilizada em uma família de documentos, então essas limitações são colocadas nas expressões utilizadas nos formatos XML que estão armazenados na família:

1. Só podem ser utilizados caminhos de elemento único que começam na raiz do documento.
2. Os caminhos de elemento não podem incluir prefixos de espaço de nomes mesmo se aparecerem nos documentos.

A janela Gerenciar Formatos XML inclui uma lista drop-down etiquetada com opções de Arquivo grande. A lista inclui as opções: *Nenhum*, *Utilizar processador de arquivo grande*, e *Utilizar processador de arquivo grande com reconhecimento de espaço de nome*. O usuário seleciona uma opção de arquivo grande se estiver gravando formatos XML que correspondem a documentos grandes que não podem ser tratados utilizando o processador XPath completo. A opção de reconhecimento de espaço de nomes significa que os caminhos de elemento incluem prefixos de espaço de nomes quando aparecem em um documento.

Nota: Essa opção não pode ser alterada depois de criada a família. Por isso a família do documento já pode incluir os formatos XML que ficarão inválidos caso o tipo da família seja alterado. O processamento do Arquivo XML customizado está indisponível para parceiros.

Relatório de Volume do Documento

O Relatório de Volume do Documento é uma ferramenta valiosa usada para gerenciar, rastrear e resolver problemas com o fluxo de documentos comerciais. O relatório exibe o volume de documentos processados pelo sistema em um período de tempo específico. Este relatório pode ser visualizado, impresso e salvo (exportado) para ser enviado para outros membros da equipe.

É possível personalizá-lo para visualizar informações com base em critérios de procura específicos.

O Relatório de Volume do Documento mostra o número de documentos que estão em andamento no momento, por estado:

Tabela 35. Status do Documento

Valor	Descrição
Total Recebido	O número total de documentos recebidos pelo sistema.
Em Andamento	Os documentos que estão Em Andamento estão sendo testados e validados. Nenhum erro foi detectado, mas o processo ainda não está concluído.
Com Falha	O processamento do documento foi interrompido devido a um erro.
Bem-sucedido	A mensagem final que conclui o processamento do documento foi transmitida do sistema para o parceiro de destino.

Utilize este relatório para executar as seguintes tarefas:

- Determinar se os processos comerciais chave foram concluídos.
- Rastrear tendências no volume de processos para controlar custos.
- Gerenciar a qualidade do processo - êxito e falha.
- Se você for parceiro interno, ajude os parceiros a monitorar a eficiência do processo.

Criar um Relatório de Volume do Documento

1. Clique em **Ferramentas** > **Relatório de Volume do Documento**. O sistema exibe a tela Procurar Relatório de Volume do Documento.

2. Selecione o critério de procura nas listas drop-down.

Tabela 36. Critério de Procura do Relatório de Volume do Documento

Valor	Descrição
Data e hora de início	A data e a hora em que o processo foi iniciado.
Data e hora de término	A data e a hora em que o processo foi concluído.
Parceiro de Origem	O parceiro que iniciou o processo de negócios (parceiro interno, apenas).
Parceiro de Destino	O parceiro que recebeu o processo de negócios (parceiro interno, apenas).
Procurar em	Procurar no tipo de documento de origem ou de destino.
Tipo de Destino	Produção ou teste. O teste está disponível apenas em sistemas que suportam o tipo de destino de teste.
Pacote	Descreve o formato, o empacotamento, a criptografia e a identificação do tipo de conteúdo do documento.
Protocolo	O tipo de protocolo, por exemplo, XML, EDI, arquivo simples.
tipo de documento	O processo de negócios específico.
Classificar por	Classificar resultados por este critério (Tipo de Documento ou Tipo de Documento de Destino).
Resultados por Página	Número de registros exibidos por página.

3. Clique em **Procurar**. O sistema exibe o relatório.

Exportando o Relatório de Volume do Documento

1. Clique em **Ferramentas** > **Relatório de Volume do Documento**. O sistema exibe a tela Procurar Relatório de Volume do Documento.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe o relatório.
4. Clique no ícone Exportar Relatório para exportar o relatório. Navegue até o local desejado para salvar o arquivo.

Nota: Os relatórios são salvos como arquivos .CSV (Comma-Separated Value). O nome do arquivo tem o sufixo ".csv".

Imprimindo Relatórios

1. Clique em **Ferramentas** > **Relatório de Volume do Documento**. O sistema exibe a tela Procurar Relatório de Volume do Documento.
2. Selecione o critério de procura nas listas drop-down.
3. Clique em **Procurar**. O sistema exibe o relatório.
4. Clique no ícone Imprimir para imprimir o relatório.

Testar Conexão do Parceiro

O recurso Testar Conexão do Parceiro permite testar o destino ou o servidor da Web. Se você for o parceiro interno, também poderá selecionar um parceiro específico. O teste consiste em enviar um pedido POST em branco para um destino ou uma URL. O pedido assemelha-se à digitação da URL da Yahoo (www.yahoo.com) no campo de endereço do navegador. Nada é enviado; trata-se de um pedido vazio. A resposta recebida do destino ou do servidor da Web indicará seu status:

- Se uma resposta for retornada, o servidor estará ativo.
- Se nenhuma resposta for retornada, o servidor estará inativo.

Importante: O recurso Testar Conexão do Parceiro funciona com HTTP que não requer parâmetros de conexão.

Para testar uma conexão de parceiro:

1. Clique em **Ferramentas > Testar Conexão do Parceiro**. O sistema exibe a tela Testar Conexão do Parceiro.
2. Selecione o critério de teste nas listas drop-down.

Tabela 37. Testar Valores da Conexão do Parceiro

Valor	Descrição
Parceiro	Parceiro a ser testado (parceiro interno, apenas).
Destino	Exibe os destinos disponíveis com base no parceiro selecionado acima.
URL	Preenchido dinamicamente com base no destino selecionado acima.
Comando	Post ou Get.

3. Clique em **Testar URL**. O sistema exibe os resultados do teste. Para obter informações sobre o código de status retornado, consulte as seções a seguir.

Códigos de Resultados do Servidor da Web

Séries 200:

- 200 - OK - Transmissão bem-sucedida. Isso não é um erro. Aqui está o arquivo que você solicitou.
- 201 - Criado - O pedido foi preenchido e resultou na criação de um novo recurso. O recurso criado recentemente pode ser referido pelas URLs retornadas no campo de cabeçalho da URL de resposta, com a URL mais específica para o recurso fornecido por um campo de cabeçalho de localização.
- 202 - Aceito - O pedido de processamento foi aceito, mas o processamento ainda não foi concluído.
- 203 - Nenhuma Informação Autorizada - A informação META retornada no cabeçalho da entidade não é o conjunto definitivo, pois está disponível a partir do servidor de origem, mas é coletada de uma cópia local ou de terceiros.
- 204 - Nenhum Conteúdo - O servidor preencheu o pedido, mas não há nenhuma informação nova para ser enviada de volta.
- 206 - Conteúdo Parcial - Você solicitou um intervalo de bytes no arquivo. Aqui estão eles. Isso é novo no HTTP 1.1

Séries 300:

- 301 - Movido Permanentemente - O recurso solicitado foi designado para uma nova URL permanente e nenhuma referência futura a este recurso deverá ser feita com uma das URLs retornadas.
- 302 - Movido Temporariamente - O recurso solicitado reside temporariamente em uma nova URL. Redirecionamento para uma nova URL. A página original foi movida. Isso não é um erro; a maioria dos navegadores busca a nova página ao obter este resultado.

Séries 400:

- 400 - Pedido Inválido - O pedido não pôde ser entendido pelo servidor, pois sua sintaxe é inválida. Pedido inválido feito pelo cliente.
- 401 - Não Autorizado - O pedido requer a autenticação do usuário. A resposta deve incluir um campo de cabeçalho de Autenticação WWW que contém um

desafio aplicável para a origem solicitada. O usuário solicitou um documento mas não forneceu um nome de usuário ou uma senha válida.

- 402 - Pagamento Requerido - Este código não é suportado no momento, mas é reservado para uso futuro.
- 403 - Proibido - O servidor entendeu o pedido mas está se recusando a executá-lo devido a um motivo não especificado. O acesso é explicitamente negado para este documento (Isso pode acontecer porque o servidor da Web não possui permissão de leitura para o arquivo que está sendo solicitado.) O servidor se recusa a enviar este arquivo. A permissão pode ter sido explicitamente desativada.
- 404 - Não Encontrado - O servidor não encontrou nada que correspondesse a URL solicitada. Esse arquivo não existe. Isso é obtido quando se fornece uma URL inválida para o navegador. Isso também pode ser obtido se o servidor tiver sido instruído a proteger o documento informando às pessoas não-autorizadas que ele não existe. Os erros 404 são o resultado dos pedidos por página que não existem e podem ser originados por um URL digitado incorretamente, por um indicador que aponta para um arquivo que não existe mais, por mecanismos de procura que buscam um arquivo robots.txt (usado para marcar páginas que você não deseja que sejam indexadas pelos mecanismos de procura), por pessoas que detectam nomes de arquivos, por links inválidos do seu site ou de outros sites, etc.
- 405 - Método Não Permitido - O método especificado na linha de pedido não é permitido para o recurso identificado pela URL de pedido.
- 406 - Não Aceitável - O servidor encontrou um recurso que corresponde a URL de pedido, mas não encontrou um que satisfizesse às condições identificadas pelos cabeçalhos de pedido de Aceitação e de Aceitação de Codificação.
- 407 - Autenticação de Proxy Requerida - Este código é reservado para uso futuro. Ele é semelhante ao 401 (Não-autorizado) mas indica que o cliente deve se autenticar primeiramente com um proxy. O HTTP 1.0 não fornece um meio para a autenticação do proxy.
- 408 - Tempo Limite do Pedido - O cliente não produziu um pedido dentro do tempo que o servidor estava preparado para aguardar.
- 409 - Conflito - O pedido não pôde ser concluído devido a um conflito com o estado atual do recurso.
- 410 - Desaparecido - O recurso solicitado não está mais disponível no servidor e nenhum endereço de redirecionamento é conhecido.
- 411 - Autorização Recusada - As credenciais do pedido fornecidas pelo cliente foram rejeitadas pelo servidor ou não eram suficientes para conceder autorização para acessar o recurso.
- 412 - Falha na Pré-condição
- 413 - Entidade de Pedido Muito Grande
- 414 - URI de Pedido Muito Grande
- 415 - Tipo de Mídia Não-suportado

Séries 500:

- 500 - Erro Interno de Servidor - O servidor encontrou uma condição inesperada que o impediu de preencher o pedido. Algo de errado aconteceu com o servidor da Web e ele não pôde fornecer uma resposta significativa. Geralmente não há nada a ser feito pelo navegador para corrigir este erro. O administrador do servidor provavelmente precisará verificar o log de erro do servidor para ver o que aconteceu. Normalmente esta é a mensagem de erro para um script CGI que não foi codificado corretamente.

- 501 - Método Não Implementado - O servidor não suporta a funcionalidade requerida para preencher o pedido. O método de aplicativo (GET ou POST) não é implementado.
- 502 - Destino Inválido - O servidor recebeu uma resposta inválida do destino ou do servidor de envio de dados que ele acessou ao tentar preencher o pedido.
- 503 - Serviço Temporariamente Indisponível - O servidor está indisponível no momento para lidar com o pedido devido a um sobrecarga temporária ou manutenção do servidor. O servidor está sem recursos.
- 504 - Tempo Limite do Destino - O servidor não recebeu uma resposta em tempo hábil do destino ou do servidor de envio de dados que ele acessou ao tentar concluir o pedido.
- 505 - Versão HTTP Não Suportada

Relatórios EDI

Utilize os Relatórios EDI para procurar FA (Functional Acknowledgements) de EDI (Electronic Data Interchange) vencidos. É possível também procurar transações EDI (Electronic Data Interchange) rejeitadas. As seções a seguir detalham o procedimento para utilizar os Relatórios EDI.

Procura de Vencimentos de FAs EDI

A página Procura de Vencimentos de FAs EDI fornece os critérios de procura para desempenhar uma procura por FAs (confirmações funcionais) EDI (electronic data interchange) vencidas.

Nota: Todos os registros retornados por procuras de vencimentos de FAs EDI anteriores que foram removidos dos relatórios resultantes serão ignorados por procurar posteriores. Portanto, os registros removidos não serão exibidos em relatórios posteriores. Os registros poderão ser removidos de um relatório selecionando-se **Ignorar Registros Selecionados** na página Relatório de Vencimentos de FAs EDI. Apenas o administrador de hub pode remover registros de um relatório.

Para procurar os registros de Vencimentos de FA EDI, faça o seguinte:

1. Clique em **Ferramentas > Relatórios EDI**. A tela Procura de Vencimentos de FAs EDI é exibida.

2. Selecione um ou mais critérios de procura na lista drop-down:

Tabela 38. Critérios de Procura de Vencimento de FAs EDI

Valor	Descrição
Data e hora de início	A data e a hora de início da transação.
Data e hora de término	A data e a hora em que a transação foi concluída.
Parceiro de Origem	O parceiro que iniciou a transação.
Parceiro de Destino	O parceiro que recebeu a transação.
Procurar em	Procure no tipo de documento de origem ou de destino.
Pacote	Descreve o formato, o empacotamento, a criptografia e a identificação do tipo de conteúdo do documento.
Protocolo	O tipo de protocolo, por exemplo, XML, EDI, arquivo simples. Os protocolos exibidos variam dependendo do valor selecionado no campo Pacote.
Tipo de Documento	Especifique o tipo de documento. Os tipos exibidos variam dependendo do valor selecionado no campo Protocolo.
ID de Referência	Especifica um ID de transação.
Classificar por	Especifica os critérios para a classificação dos resultados de procura. Os padrões são Vencimento Expirado e Descendente. Utilize Descendente para exibir primeiro os FAs mais vencidos. Selecione Ascendente para exibir primeiros os FAs menos vencidos.
Resultados por Página	Especifica o número de resultados da procura de transações a ser exibido por página.

3. Clique em **Procurar** para exibir o relatório Procura de Vencimento de FAs EDI.

Visualizando os Relatórios de Vencimentos de FAs EDI

Dependendo dos critérios de procura selecionados na página Procura de Vencimentos de FAs EDI, o resultado da procura será exibido na página Relatório de Vencimentos de FAs EDI.

Os dados a seguir, quando aplicável, são exibidos no relatório de FAs EDI Vencidas.

Tabela 39. Relatório de Vencimentos de FAs EDI

Valor	Descrição
Date	A data que o EDI foi enviado do parceiro de origem para o parceiro de destino.
Horário	A hora (GMT) que o EDI foi enviado do parceiro de origem para o parceiro de destino.
ActivityID	O VUID (Virtually Unique ID) da transação.
Parceiro Comercial de Origem	O parceiro que enviou a transação.
Pacote de Origem	O pacote de origem da transação.
Protocolo de Origem	O protocolo de origem da transação.
Tipo de Documento de Origem	O tipo de documento de origem da transação.
Parceiro de Negociação de Destino	O parceiro que enviou a transação.
Pacote de Destino	O pacote de destino da transação.
Protocolo de Destino	O protocolo de destino da transação.
Tipo de Documento de Destino	O tipo de documento de destino da transação.
Número de Intercâmbio	O número de intercâmbio da transação.
Número do Grupo	O número do grupo da transação.
Número da Transação	O número de identificação da transação.
FA Expirado em	A data de expiração do FA para a transação.
Vencido por	A quantidade de tempo que o FA está vencido.
Ignorar Registros Selecionados	Ao selecionar esta opção para um registro, esse registro particular é removido do relatório. Depois que um registro é removido de um relatório, ele é ignorado por procuras de vencimentos de FAs EDI posteriores e, portanto, não é exibido nos relatórios resultantes. Apenas o administrador de hub pode remover registros de um relatório.

Procura de Transação Rejeitada de EDI

A página Procura de Transações Rejeitadas EDI contém critérios para o desempenho de procuras para transações EDI (electronic data interchange) que possuem uma FA (functional acknowledgment) contendo um código de erro. Os registros de transações sem FAs não são retornados por uma procura de transações rejeitadas EDI.

Para procurar os registros de EDI rejeitados, faça o seguinte:

1. Clique em **Ferramentas > Relatórios EDI > Relatório EDI Rejeitado**.

2. Selecione um ou mais critérios de procura na lista drop-down:

Tabela 40. Critérios de Procura de Transações de EDI Rejeitado

Valor	Descrição
Data e hora de início	A data e a hora de início da transação.
Data e hora de término	A data e a hora em que a transação foi concluída.
Parceiro de Origem	O parceiro que iniciou a transação.
Parceiro de Destino	O parceiro que recebeu a transação.
Procurar em	Procure no tipo de documento de origem ou de destino.
Pacote	Descreve o formato, o empacotamento, a criptografia e a identificação do tipo de conteúdo do documento.
Protocolo	O tipo de protocolo, por exemplo, XML, EDI, arquivo simples. Os protocolos exibidos variam dependendo do valor selecionado no campo Pacote.
Tipo de Documento	Especifique o tipo de documento. Os tipos exibidos variam dependendo do valor selecionado no campo Protocolo.
ID de Referência	Especifica um ID de transação.
Classificar por	Especifica os critérios para a classificação dos resultados de procura. Os padrões são Vencimento Expirado e Descendente. Utilize Descendente para exibir primeiro os FAs mais vencidos. Selecione Ascendente para exibir primeiros os FAs menos vencidos.
Resultados por Página	Especifica o número de resultados da procura de transações a ser exibido por página.

3. Clique em **Procurar** para visualizar o relatório Transação de EDI Rejeitada.

Visualizando os Relatórios Transação de EDI Rejeitada

Dependendo dos critérios de procura selecionados na página Procura de Transação de EDI Rejeitada, o resultado da procura será exibido na página Relatório de Transação de EDI Rejeitada.

Os dados a seguir, quando aplicável, são exibidos no relatório Transação EDI Rejeitada.

Tabela 41. Relatório de Transação Rejeitada de EDI

Valor	Descrição
Date	A Data na qual o EDI foi recebido.
Horário	A hora (GMT) que a transação EDI foi enviada do parceiro de origem para o parceiro de destino.
ActivityID	O VUID (Virtually Unique ID) da transação.
Parceiro Comercial de Origem	O parceiro que enviou a transação.
Pacote de Origem	O pacote de origem da transação.
Protocolo de Origem	O protocolo de origem da transação.
Tipo de Documento de Origem	O tipo de documento de origem da transação.
Parceiro de Negociação de Destino	O parceiro que recebeu a transação.
Pacote de Destino	O pacote de destino da transação.
Protocolo de Destino	O protocolo de destino da transação.
Tipo de Documento de Destino	O tipo de documento de destino da transação.
Número de Intercâmbio	O número de intercâmbio da transação.
Número do Grupo	O número do grupo da transação.
Número da Transação	O número de identificação da transação.
Código de Status	O código de status do FA.
Texto de Status	O texto de status do FA.

Relatórios FTP

Os Relatórios FTP fornecem detalhes sobre as Estatísticas do FTP e Conexões do FTP.

Estatísticas do FTP

A página Estatísticas do FTP exibirá o Status do Servidor FTP no Modo de Leitura.

Nota: As estatísticas não serão exibidas se o Servidor FTP ou o Servidor de Gerenciamento FTP não estiver disponível.

Para visualizar o status do servidor FTP, faça o seguinte:

1. Clique em **Ferramentas > Relatórios do FTP**. A página Estatísticas do FTP é exibida.

2. As seguintes informações sobre o status do servidor são exibidas:

Tabela 42. Estatística do FTP

Valor	Descrição
Horário de início do servidor	Hora de início do servidor FTP.
Número de diretórios criados	Número de diretórios criados pelos usuários utilizando mkdir.
Número de diretórios removidos	Número de diretórios removidos pelos usuários utilizando rmdir.
Número de arquivos transferidos por upload	Número de arquivos transferidos por upload por todos os usuários.
Número de arquivos transferidos por download	Número de arquivos transferidos por download por todos os usuários.
Número de arquivos excluídos	Número de arquivos excluídos por todos os usuários utilizando o comando de exclusão.
Bytes Transferidos por Upload	Número total de bytes transferidos por upload.
Bytes Transferidos por Download	Número total de bytes transferidos por download.
Logins Atuais	Exibe os logins existentes.
Total de Logins	Total de logins desde a última reconfiguração.
Total de logins com falha	Número total de logins com falha.
Conexões Atuais	Conexões atuais desde a última reconfiguração.
Total de Conexões	Total de conexões desde a última reconfiguração.

3. Clique em **Recarregar** para atualizar os logins atuais.
4. Clique em **Reconfigurar** para reconfigurar os valores.

Conexões FTP

Visualize as Conexões FTP através dos métodos mencionados abaixo:

1. Clique em **Ferramentas > Relatórios FTP > Conexões FTP.**
2. As seguintes informações de conexão são exibidas no relatório:

Tabela 43. Conexões do FTP

Valor	Descrição
Nome do Login	O ID do usuário de login para esta conexão. Se estiver em branco, isso significa que o usuário só estabeleceu uma conexão, mas não efetuou login.
Hora do Login	A hora em que o usuário efetuou login. Se estiver em branco, isso significa que o usuário só estabeleceu uma conexão.
Hora do Último Acesso	A hora em que o usuário acessou esta conexão pela última vez. Se estiver em branco, isso significa que o usuário só efetuou login e não emitiu nenhum comando ainda.
Endereço do Cliente	O IP do cliente a partir do qual o usuário efetuou login.

Glossário

A

Ação. (1) Ações executadas em um documento pelo sistema para assegurar sua compatibilidade com os requisitos comerciais entre os parceiros. (2) Uma série de etapas de processamento, como validação e transformação de documentos.

Administração de Contas. O módulo Administração de Contas permite visualizar e editar as informações que identificam sua empresa para a rede. Essa tela também é utilizada para gerenciar privilégios de acesso do console para outras pessoas em sua organização.

Alerta. Os alertas fornecem notificações e resoluções rápidas quando limites operacionais pré-estabelecidos são violados. Um alerta consiste em uma mensagem de e-mail baseada em texto enviada para contatos individuais ou para uma lista de distribuição do pessoal chave, dentro ou fora da rede. Os alertas podem ser baseados na ocorrência de um evento de sistema ou no volume de processo esperado.

Assinatura Digital. Uma assinatura digital é uma assinatura eletrônica utilizada para autenticar a identidade dos parceiros e para assegurar que o conteúdo original de um documento que foi enviado não tenha sido alterado.

Ativação. Conectar um parceiro ao sistema.

Ativo. O estado no qual um parceiro concluiu com êxito os testes de regras comerciais e o parceiro interno emitiu um pedido de serviço para movê-los para um status ativo.

C

Classificação. Identifica a função do parceiro em um processo de negócios.

Community Console. O Community Console é uma ferramenta baseada na Web utilizada para monitorar o fluxo de documentos comerciais de sua empresa para e a partir dos parceiros internos ou externos.

Conexão do Parceiro. A conexão de parceiros define a conexão entre dois ambientes específicos de membros da comunidade através dos quais apenas um processo é executado.

Conjunto de Certificados. Um conjunto de certificados primários e secundários que podem ser associados a uma conexão participante.

Contagem de Tentativas. Indica se a transação é a primeira tentativa ou se houve outras tentativas. 1 é a primeira tentativa. 2 ou mais indica o número de novas tentativas.

Contato assinado. Um contato assinado é um indivíduo que foi designado a receber alertas de e-mail.

Conversão. Quando um documento é convertido de um protocolo para outro.

Coreografia. A ordem requerida de documentos necessários para concluir um processo de negócios com êxito.

Código de Sinal Comercial. Identifica o tipo de sinal (documento) enviado em resposta a uma ação. Exemplos incluem o recebimento ou a confirmação de aceitação ou exceções gerais.

Curinga. O critério de procura de curingas inclui o asterisco (*).

D

Definição de Documento. Fornece ao sistema todas as informações necessárias para receber, processar e rotear documentos entre os membros da comunidade. Os tipos de Definição de Documento incluem pacote, protocolo, tipo de documento, atividade e ação.

Desmembrar. Para extrair um documento de um envelope EDI.

Destino. Um ponto de rede B2B que atua como entrada para outra rede. Os problemas de compatibilidade e de conversão de dados podem ser resolvidos por um destino para garantir a transferência de dados.

Documento. Uma coleção de informações que seguem uma convenção organizacional. As informações podem ser textos, imagens e sons.

DUNS. O número D&B D-U-N-S é uma seqüência de identificação de nove dígitos exclusiva que fornece identificadores exclusivos de entidades comerciais simples enquanto vincula estruturas familiares corporativas. O D&B vincula os números D&B D-U-N-S de pais, subsidiárias, matrizes e escritórios em mais de 64 milhões de membros da família corporativa em todo o mundo. Usado pelas organizações com os padrões comerciais mais influentes do mundo, ele é reconhecido, recomendado e geralmente requerido por mais de 50 associações comerciais e industriais globais, incluindo as Nações Unidas, o Governo Federal Americano, o Governo Australiano e a Comissão

Européia. Na economia global atual, o número D&B D-U-N-S tornou-se o padrão para o rastreio de empresas em todo o mundo.

E

EDI. A transferência de informações de computador para computador em um formato estruturado e pré-determinado. Tradicionalmente, o foco da atividade EDI é a substituição de formas comerciais predefinidas, como ordens de compra e faturas, com formatos eletrônicos definidos de forma semelhante.

Em Resposta ao ID. O número de ID de Em Resposta à Ação Comercial.

Em Resposta à Ação Comercial. Identifica o tipo de documento comercial enviado em resposta a uma ação no mesmo processo.

Encerrado. A data e a hora em que o último documento em um processo é transacionado ou cancelado.

Estado. (1) Os documentos que estão sendo processados pelo sistema estão em um dos quatro estados (2) recebido, em andamento, com falha ou bem-sucedido.

Evento. Uma mensagem gerada pelo sistema associado ao processamento de documentos.

F

Ferramentas. O módulo Ferramentas permite solucionar falhas no processo permitindo que você veja documentos com falhas, campos de dados e seus eventos associados.

Filho de Parceiro Interno. Filho do Parceiro Interno é um tipo de parceiro especial que atua como um parceiro no console, mas como um parceiro interno durante o roteamento.

Filtro. Para remover dados de uma sub-transação baseada em parâmetros predefinidos.

FTP. O FTP (File Transfer Protocol), um protocolo de Internet padrão, é a forma mais simples de trocar arquivos entre computadores pela Internet.

G

Gerenciador de Entrada. Recupera documentos do NAS e os prepara para a ação apropriada ao mecanismo de processo de negócios.

Global. Alertas podem ser designados à pessoa de contato pelo parceiro e pelo parceiro interno.

Grupo. Uma coleção de usuários com privilégios de acesso ao console para executar funções selecionadas.

H

HTTP. O HTTP (Hypertext Transfer Protocol) é o conjunto de regras (protocolo) para a troca de arquivos (texto, imagens gráficas, som, vídeo e outros arquivos multimídia) na Web.

HTTPS. O HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) é um protocolo da Web que criptografa e decriptografa pedidos de páginas de usuários, bem como as páginas que são retornadas pelo servidor da Web.

I

ID da Transação. Número de ID do processo de negócios.

ID de Instância da Ação. Identifica documentos que não possuem conteúdo comercial, por exemplo, ordens de compra ou RFQ.

ID de Instância de Processo. O número de identificação exclusivo de um determinado processo de negócios.

ID de Instância do Sinal. Identifica documentos que são confirmações positivas ou negativas enviadas em resposta às ações.

M

Mitigação de Dados. O processo de teste e reparo de erros no formato e na estrutura do documento com base nos padrões do processo de negócios.

Modo de Operação. Identifica documentos que são roteados para um determinado gateway durante testes ou para a produção.

P

Pacotes. Identifica formatos de pacotes de documentos que podem ser recebidos pelo servidor do sistema. Por exemplo, AS1 e AS2.

Parceiro Externo. Um membro da comunidade de hub que troca transações comerciais com o parceiro interno.

Perfil. O módulo Perfil permite visualizar e editar as informações que identificam sua empresa para o sistema.

PIP (Partner Interface Process). Define processos de negócios entre os parceiros internos e os Parceiros (no WebSphere Partner Gateway, os Parceiros são

participantes). Cada PIP identifica um documento comercial específico e o modo como ele é processado.

Processo de Negócios. Um conjunto predefinido de transações que representa o método de execução do trabalho necessário para atingir o objetivo de um negócio.

Produção. O gateway de destino usado para rotear documentos.

Protocolo de Documentos. Um conjunto de regras e instruções (protocolo) para a formatação e transmissão de informações através de uma rede. Exemplos incluem RosettaNet, XML, arquivo simples e EDI.

Protocolo de Transporte. Um conjunto de regras (protocolo) usado para enviar dados no formato de unidades de mensagem entre computadores pela Internet. Os exemplos incluem HTTP, HTTPS, SMTP e FTP.

Protocolos. Identifica os tipos específicos de formatos de documentos para uma variedade de processos comerciais. Por exemplo, RosettaNet e XML.

Provisionamento. O provisionamento (ou on-boarding) consiste na conclusão de uma seqüência de etapas requeridas para conectar o gateway B2B de um usuário à infra-estrutura do sistema.

R

Relatórios. O módulo Relatórios permite que os usuários criem relatórios detalhados sobre o volume de documentos que está sendo processado, bem como os eventos gerados pelo sistema.

RNIF. O RNIF (RosettaNet Implementation Framework) é uma diretriz para a criação de um contêiner de envelope padrão para todos os PIPs (Partner Interface Processes).

RTF. O RTF (Rich Text Format) é um formato de arquivo que permite trocar arquivos de texto entre diferentes processadores de textos em diferentes sistemas operacionais. Por exemplo, é possível criar um arquivo usando o Microsoft Word no Windows 98, salvá-lo como um arquivo RTF (ele terá um sufixo de nome de arquivo .rtf) e enviá-lo para alguém que utiliza o WordPerfect 6.0 no Windows 3.1.

S

Serviço. Identifica se a mensagem é baseada em RosettaNet.

Servlet. Um programa pequeno executado no servidor da Web que grava o documento recebido para o NAS.

Sinal. O documento enviado em resposta a uma ação.

SMTP. O Simple Mail Transfer Protocol é um protocolo usado ao enviar e receber e-mails.

SR. Pedido de serviço

SSL. Secure sockets layer é um método de segurança de envio de dados usando o protocolo HTTP.

Substituir. Substituir dados em uma sub-transação por outros dados com base em parâmetros predefinidos.

T

Teste. O estado no qual um parceiro está em processo de mitigação de dados ou testes de regras comerciais durante o processo de provisionamento.

Teste das Regras de Negócios. O processo de teste e reparo de erros de conteúdo em um documento entre os parceiros.

Transação. Uma seqüência de troca de informações e trabalho relacionada que é tratada como uma unidade para as finalidades de transação comercial entre os parceiros.

Transformar. Substituir o conteúdo de um documento por dados de uma tabela de referência cruzada.

U

URL. Uma URL (Uniform Resource Locator) é o endereço de um documento ou processo (recurso) acessível na Internet.

V

Validação. A validação é o ato de comparar uma sub-transação de processo com os requisitos especificados para determinar sua validade e invalidade. O conteúdo e a seqüência de transações são parâmetros típicos.

Versão. Uma determinada liberação de um protocolo de documento.

Versão do Sinal. A versão do processo de negócios enviado como um sinal.

Visibilidade. A visibilidade define se uma pessoa de contato pode ser designada a um alerta por um participante (local) ou também pelo parceiro interno (global).

Avisos

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos neste documento em outros países. Consulte seu representante IBM local sobre os produtos e serviços atualmente disponíveis na sua região. Qualquer referência a um produto, programa ou serviço da IBM não tem a intenção de afirmar ou inferir que somente esse produto, programa ou serviço possa ser utilizado. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, o usuário é responsável por avaliar e verificar a operação de qualquer produto, programa ou serviço não-IBM.

A IBM pode ter patentes ou solicitações de patentes relativas a assuntos tratados neste documento. O fornecimento desta publicação não lhe garante direito algum sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local:

A INTERNATIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO ÀS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns estados não permitem a renúncia das garantias diretas ou indiretas em determinadas transações, conseqüentemente, é possível que esta instrução não se aplique a você.

Esta publicação pode incluir imprecisões técnicas ou erros tipográficos. As informações contidas nesta publicação estão sujeitas a alterações periódicas. Tais alterações serão incorporadas em novas edições da publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites não-IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites. O material nestes Web sites não faz parte do material para este produto IBM e o uso destes sites é de sua própria responsabilidade.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Estas informações podem estar disponíveis, observadas as condições e os termos apropriados, incluindo, em alguns casos, o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, Contrato de Licença do Programa Internacional da IBM ou de qualquer outro contrato equivalente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, os resultados obtidos em outros ambientes operacionais podem variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão iguais nos sistemas geralmente disponíveis. Além disso, algumas medidas podem ter sido estimadas por extrapolação. Os resultados reais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para o seu ambiente específico.

As informações relacionadas a produtos que não são da IBM foram obtidas dos fornecedores destes produtos, de suas declarações publicadas ou de outras fontes disponíveis publicamente. A IBM não testou necessariamente estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Estas informações contêm exemplos de dados e relatórios utilizados em operações comerciais diárias. Para ilustrá-las da forma mais completa possível, os exemplos podem incluir nomes de pessoas, empresas, marcas e produtos. Todos esses nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa comercial real é mera coincidência.

Todas as declarações relacionadas aos objetivos e intenções futuras da IBM estão sujeitas a alterações ou cancelamento sem aviso prévio, e representam apenas metas e objetivos.

LICENÇA DE COPYRIGHT

Estas informações podem conter programas aplicativos de amostra na linguagem-fonte, que ilustram técnicas de programação em várias plataformas operacionais. É possível copiar, modificar e distribuir estes programas de exemplo sem a necessidade de pagar à IBM, com objetivos de desenvolvimento, utilização, marketing ou distribuição de programas aplicativos em conformidade com a interface de programação de aplicativo para a plataforma operacional para a qual os programas de exemplo são criados. Estes exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou confirmar a confiabilidade, manutenção ou função destes programas.

O Websphere Partner Gateway contém código nomeado ICU4J que é licenciado ao Cliente pela IBM sob os termos do Acordo Internacional de Licença do Programa, sujeitos aos termos de Componentes Excluídos. No entanto, a IBM precisa fornecer o seguinte idioma ao Cliente como um aviso:

AVISO DE COPYRIGHT E DE PERMISSÃO

Informações sobre Interface de Programação

As informações sobre interface de programação, se fornecidas, destinam-se a facilitar a criação de software aplicativo utilizando este programa.

As interfaces de programação de uso geral permitem que o Cliente desenvolva o software aplicativo que obtém os serviços das ferramentas deste programa.

Entretanto, essas informações também podem conter informações sobre diagnósticos, modificações e ajustes. As informações sobre diagnósticos, modificações e ajustes são fornecidas para ajudá-lo a depurar o seu software aplicativo.

Aviso: Não utilize estas informações sobre diagnósticos, modificações e ajustes como uma interface de programação, pois elas estão sujeitas a alterações.

Marcas Registradas e Marcas de Serviço

Os termos a seguir são marcas ou marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países:

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

Microsoft, Windows, Windows NT e o logotipo Windows são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

MMX, Pentium e ProShare são marcas ou marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

Java e todas as marcas registradas baseadas em Java são marcas registradas da Sun Microsystems, Inc. nos Estados Unidos e/ou em outros países.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Outros nomes de empresas, produtos ou serviços podem ser marcas registradas ou marcas de serviço de terceiros.

WebSphere Partner Gateway Enterprise e Advanced Editions, versão 6.1.

Índice Remissivo

A

C

D

E

F

G

I

M

N

P

R

S

T

U

V

Impresso em Brazil