Sterling B2B Integrator

Security (V5.2.3 ou posterior)

Versão 5.2.3

Sterling B2B Integrator

Security (V5.2.3 ou posterior)

Versão 5.2.3

Nota

Antes de usar estas informações e o produto suportado por elas, leia as informações nos “Avisos” na página 119.

Índice

Security (V5.2.3 ou posterior)

Sterling B2B Integrator usa uma variedade de mecanismos de segurança, incluindo senhas do sistema para funções administrativas, políticas de senha baseadas nas políticas de segurança da sua empresa e segurança baseada em função para fornecer níveis diferentes de acesso a diferentes usuários dentro da organização.

Os seguintes recursos de segurança são fornecidos com o Sterling B2B Integrator:

- A segurança baseada em função fornece aos usuários acesso a arquivos, processos de negócios, modelos da Web, serviços e recursos de produtos de acordo com as permissões associadas com a conta do usuário.
- Políticas de senha são conjuntos de decisões de segurança que você faz e aplica a diferentes contas de usuário de acordo com políticas de segurança em sua empresa. Essas opções incluem itens como número de dias durante os quais uma senha é válida e os comprimentos máximo e mínimo de uma senha.
- A autenticação LDAP pode ser usada para delegar autenticação de uma conta do usuário externo a um diretório LDAP e para fornecer autenticação usando as mesmas informações de segurança usadas para outros aplicativos em sua empresa. Se sua empresa já tiver adotado LDAP, é possível usar seus diretórios LDAP existentes com o aplicativo.
- Passphrase de Instalação do Sistema - Durante a instalação, você cria um passphrase do sistema para sua instalação do Sterling B2B Integrator. O passphrase é uma sequência altamente complexa com mais de 16 caracteres. O passphrase do sistema é necessário para iniciar o sistema e para acessar informações do sistema protegidas.
- Suporte para certificados x.509 para criptografia, assinatura e segurança da camada de transporte.
- Módulo de software certificado por Federal Information Processing Standards (FIPS) 140-2 e suporte para hardware certificado por FIPS 140-2 do nCipher e Safenet.
- Secure Socket Layering (SSL) e Segurança da Camada de Transporte (TLS).

Além disso, os recursos de segurança a seguir podem ser configurados:

- O recurso de segurança com tempo limite atingido fornece capacidade para configurar o tempo limite da sessão do usuário.
- O recurso Política de Senha Customizada permite incluir regras de política de senha adicionais. Essas regras de senha adicionais podem ajudar a evitar o uso de senhas fracas que podem ser facilmente descobertas por hackers e a rejeitar senhas inconformes.
- O recurso Conexão Única (SSO) é um processo de autenticação que permite que usuários acessem vários aplicativos inserindo apenas um nome de usuário e uma senha.
- O recurso Criptografia de Documento permite a configuração de uma camada adicional de segurança além das permissões tradicionais de arquivo e banco de dados.

Segurança Baseada em Função

Visão Geral de Segurança Baseada em Função

A segurança baseada em função fornece aos usuários acesso a alguns arquivos, processos de negócios, modelos da Web, serviços e recursos de produtos de acordo com as permissões associadas com a conta do usuário.

Para entender como administrar a segurança baseada em função, você precisa compreender como grupos, permissões e as contas do usuário trabalham juntos.

- As permissões fornecem acesso às páginas da interface com o usuário e à funcionalidade fornecida pela página.
- Grupos são coleções de permissões.
- As contas de usuário são designadas às permissões e às políticas de senha.

O gerenciamento da segurança baseada em função inclui as seguintes tarefas:

- Criar permissões
- Criar grupos
- Criar políticas de senha
- Criar contas de usuário

Grupos

Grupos são coleções de permissões. Os grupos possibilitam manter permissões de acesso para vários usuários a partir de um único local. Grupos ajudam a minimizar a quantidade de trabalho envolvido com manutenção de contas, especialmente quando vários usuários executam a mesma função de tarefa. É possível associar várias permissões para diferentes usuários criando grupos para cada função de tarefa em vez de cada usuário. Também é possível designar um grupo como subgrupo a outro grupo.

Por exemplo, um departamento de compras tem cinco especialistas em compras executando as mesmas tarefas. Em vez de aplicar permissões a cada conta do usuário especialista em compras individual, é possível criar um grupo de compras e manter as permissões de acesso para todos os especialistas em compras em um grupo. Dentro do grupo de compras, é possível designar subgrupos para refinar ainda mais suas permissões de acesso de acordo com o tipo de compra conduzido pelo especialista. É possível designar subgrupos denominados materiais de escritório, máquinas, equipamentos gerais ou veículos ao grupo de compras para refinar as permissões de acesso.

Para evitar sobrescrever ao aplicar upgrades ou correções, não modifique os grupos que vêm pré-configurados com o sistema.

As tarefas do grupo incluem:

- Criar um grupo
- Procurar um grupo
- Editar um grupo
- Excluir um grupo

Grupos Pré-configurados

Para designar permissões aos usuários, é possível designar os grupos pré-configurados. Os usuários herdam todas as permissões associadas aos grupos.

Um grupo predefinido pode ser designado a um usuário quando Acessibilidade e Tema estão definidos para a conta do usuário.

Você deve ter permissão para o módulo Contas para criar grupos.

Convenções de Nomenclatura de Grupo

Use as convenções de nomenclatura a seguir para grupos:

- IDs do grupo devem ser distintos.
- Nomes fazem distinção entre maiúsculas e minúsculas.
- Dois nomes de grupos com capitalização diferente são considerados nomes distintos.
- Se um nome de grupo tiver sido usado, ele não poderá ser usado como nome de um novo grupo. Uma mensagem de erro será exibida.

Procurar por Grupos

Sobre Esta Tarefa

Para procurar um grupo:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Grupos**.
2. Conclua uma das ações a seguir:
   - Em Procurar, insira uma parte do **Nome do Grupo** ou o **Nome do Grupo** inteiro que você está procurando e clique em **Ir!** A página Grupos lista todos os grupos que correspondem ao seu critério de procura.
   - Em Listar, selecione TODOS ou a letra com a qual começa o nome do grupo que você está procurando no campo **Em Ordem Alfabética** e clique em **Ir!** A página Grupos lista todos os grupos que correspondem ao seu critério de procura.

Criar Grupos

Sobre Esta Tarefa

Antes de começar, você precisa saber:

- ID do Grupo para o grupo que você está criando.
- Nome do grupo para o grupo que você está criando.
- Nome do Proprietário para o grupo.
- Identidade do parceiro comercial para associar ao grupo. Apenas um parceiro comercial pode ser associado a um grupo, mas uma conta do usuário pode ser associada a vários grupos. Isso permite que uma conta do usuário seja associada a mais de um parceiro comercial. O campo de identidade é usado para rotear mensagens no Mailbox.

Para criar um grupo:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Grupos**.
2. Próximo de **Criar um Novo Grupo**, clique em **Ir!**
3. Na página Novo Grupo, insira o **ID do Grupo**.
4. Insira **Nome do Grupo**.
5. Insira **Proprietário**.
6. Selecione a **Identidade**.

7. Clique em **Avançar**.
8. Na página Designar Subgrupos, se você quiser filtrar grupos pelo nome, em Dados de Filtro no campo **Por Nome**, insira uma parte do nome ou o nome inteiro do grupo que deseja filtrar e clique no botão de filtro.
9. Selecione os grupos que deseja designar a este grupo. Mova os grupos da área de janela Disponível para a área de janela Designado.
10. Clique em **Avançar**.
11. Na página Designar Permissões, deseja filtrar permissões?
    - Para filtrar por nome, em Dados de Filtro no campo **Por Nome**, insira uma parte do nome ou o nome inteiro da permissão que deseja filtrar e clique no botão de filtro à direita do campo **Por Tipo**.
    - Para filtrar por tipo, em Dados de Filtro, selecione o tipo de permissão que deseja filtrar na lista Por Tipo e clique no botão de filtro à direita do campo **Por Tipo**.
12. Selecione as permissões que deseja designar a esse grupo. Mova as permissões da área de janela Disponível para a área de janela Designado. Por padrão, as permissões associadas aos subgrupos designados a esse grupo já estão selecionadas. As permissões associadas não são exibidas na coluna disponível; mas são exibidas na página de confirmação.
13. Clique em **Avançar**.
14. Revise as informações sobre o grupo.
15. Clique em **Concluir**.

Editar Grupos

Sobre Esta Tarefa

Quando você edita um grupo, é possível atualizar:

- Configurações
- Subgrupos
- Permissões

Não é possível alterar o ID do Grupo. Se for necessário alterar o ID do grupo, você deverá criar um novo grupo.

Para editar um grupo:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Grupos**.
2. Procure o grupo que deseja editar usando Procura de Nome de Grupo ou Listar em Ordem Alfabética e clique em **Ir!**
3. Selecione **Editar** para o grupo que deseja atualizar.
4. Atualize qualquer uma das configurações do grupo e clique em **Avançar**.
5. Atualize qualquer um dos subgrupos designados e clique em **Avançar**.
6. Atualize qualquer uma das permissões designadas e clique em **Avançar**.
7. Clique em **Avançar**.
8. Revise as informações sobre o grupo.
9. Clique em **Concluir**.

Excluir Grupos
Sobre Esta Tarefa

Não é possível remover o grupo de Administradores ou a permissão Contas da UI do Sterling B2B Integrator de um usuário administrador. Isso permite que o administrador do sistema administre o sistema.

Para excluir um grupo:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Grupos**.
2. Na página Grupos, localize o grupo que deseja excluir usando a opção Procurar ou Listar.
3. Na página Grupos, próximo do grupo que deseja excluir, clique em **Excluir**.

   O sistema exclui o grupo e exibe a mensagem:

   ```
   A atualização do sistema foi concluída com sucesso.
   ```

Revisar Nome do Grupo e ID
Sobre Esta Tarefa

Para revisar um nome do grupo e um ID:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Grupo**.
2. Na página Grupo, localize o grupo que deseja revisar usando as opções Procurar ou Listar.
3. Selecione o grupo. O nome do grupo e o ID são exibidos.

Permissões

Permissões fornecem acesso a diferentes módulos dentro do Sterling B2B Integrator e formam a base da segurança baseada em função. As permissões de um usuário consistem em permissões dos grupos mais quaisquer permissões designadas individualmente.

Use permissões para:

- Gerenciar acesso de vários usuários a partir de um único local.
- Gerenciar contas do usuário com mínimo de esforço, especialmente para diversos usuários que executam a mesma função de tarefa.

Tarefas de permissões incluem:

- Criar uma permissão
- Procurar uma permissão
- Editar um nome de permissão
- Excluir uma permissão

Antes de criar, editar ou excluir uma permissão, decida quais módulos os usuários nesse grupo precisam ou não acessar para executar suas funções designadas. Você deve receber a permissão para o módulo Contas para criar permissões.

Para evitar sobrescrever ao aplicar upgrades ou correções, não modifique as permissões que vêm pré-configuradas com o sistema. Quando agrupamentos customizados de permissões forem requeridos, crie um novo grupo.

Convenções de Nomenclatura de Permissões

As convenções de nomenclatura de permissão incluem:

- Nomes fazem distinção entre maiúsculas e minúsculas e dois nomes com letras maiúsculas e minúsculas diferentes são considerados como nomes exclusivos. Por exemplo, "Qualquer documento" e "Qualquer Documento" são dois nomes de permissão diferentes.
- Se um nome tiver sido usado para uma permissão existente, ele não poderá ser usado como o nome de uma nova permissão. Uma mensagem de erro será exibida.

Mesmo que duas permissões possam ter o mesmo nome com diferentes letras maiúsculas e minúsculas, isto não é recomendado.

Permissões Herdadas de Grupos

Estes são os grupos pré-instalados e as permissões herdadas quando um grupo de permissões é designado a uma conta do usuário. As mesmas permissões são herdadas quando um grupo é designado como um subgrupo.

Cada grupo contém permissões para itens de menu, mais a permissão de UI correspondente que é usada para conceder acesso à página. Por exemplo, EBXML contém UI EBXML.

Nome do Grupo	ID do Grupo	Permissões Herdadas do Grupo
ACCOUNTS	ACCOUNTS	PasswordPolicy, Permissions, UI Accounts, UserNews
ADAPTER_UTILITIES	ADAPTER_UTILITIES	BEATuxedo, CDNetmaps, CDNetmapXref, CDNodes, SAPRoutes, SAPRouteXREF, SAPSuiteBuilder, UI Adapter Utilities
ADVANCED_SETUP	ADVANCED_SETUP	DeliveryChannels, DocumentExchange, Identities, Packaging, Profiles, Transports, UI Advanced Trading Profile Setup
AS2 Edition	as2admin	Todas as permissões do subgrupo BPMONITOR, mais AS2 UI, TestNow, UI AS2 Trading Profile Setup, UI BP Manager, UI Ca Certs, UI Delete Trading Partner Data, UI Logs, UI Scheduler, UI System Certs, UI trading Parners
Notificação de Evento Anormal	eventAbnormal	Nenhum
Contas	acctadmin	Todas as permissões do subgrupo ACCOUNTS, mais UI Groups, UI User Accounts.
Notificações de Alerta	notificações	Nenhum
BPMONITOR	BPMONITOR	BPSSCorrelation, BusinessProcesses, CentralSearch, CommunicationSessions, Correlation, CurrentActivities, CurrentDocuments, CurrentProcesses, DataFlows, Documents, EBXMLCorrelation, EDICorrelation, EDIINT, GentranServerforUnix, Message Entry Workstation Home, SWIFTNETCorrelation, UI BP Monitor, RosettaNet
Processo de Negócios	bpadmin	Todas as permissões dos subgrupos BPMONITOR e SERVICES, mais o Gerenciador de BP UI, Processo de Negócios UI, BP de Exclusão de UI.
CD Server Proxy Administrator	cdsp_admin	Todas as permissões do subgrupo ACCOUNTS, BPMONITOR, CD Server Proxy User, OPERATIONS e SERVICES, mais UI Groups, UI Licenses, UI Password Policy, UI SQL Tool, UI User Accounts.

Nome do Grupo	ID do Grupo	Permissões Herdadas do Grupo
CD Server Proxy User	cdsp_user	Este grupo é designado por padrão quando uma conta do usuário é criada com Acessibilidade CDSP. Todas as permissões dos subgrupos ACCOUNTS, BPMONITOR, OPERATIONS e SERVICES, mais CDSP Services, UI CA Certs, UI Import/Export, UI Lock Manager, UI Logs, UI Perimeter Servers, UI Reports, UI Support Case Tool, UI System Certs, UI Trusted Certs.
Usuário de Linha de Comandos	commandlineuser	eInvoicing, eInvoicing ALL BUYERS, eInvoicing ALL SUPPLIERS, eInvoicing Archive, eInvoicing Configuration, eInvoicing CREATE/EDIT AGREEMENT, eInvoicing DELETE AGREEMENT, VIEW AGREEMENT
DEPLOYMENT	DEPLOYMENT	Implementação de UI, Tags de Recurso
Usuários do Painel	dashboardUsers	Este grupo é designado por padrão quando uma conta do usuário é criada com acessibilidade Dashboard UI e qualquer um dos seguintes temas de painel: • AFT • Padrão • Operador de Gerenciamento de Comunidade, Participante, Patrocinador Participante ou Patrocinador Console de Gerenciamento de Administração, Portlet Procura de Processo de Negócios, Portlet Estatísticas de Cache, Portlet Uso de Cache, Portlet Gerenciamento de Comunidade, Portlet Estatísticas de Comunidade, Portlet Uso do Conjunto de Bancos de Dados, Portlet Status do Banco de Dados, Portlet Uso do Banco de Dados, Portlet Procura de Documento, Portlet Rastreamento de Documento, Portlet Gráfico de Barras de Documentos Processados, Portlet Série Temporal de Documentos Processados, Portlet Event Viewer, Portlet IFrame, Portlet Visualizador de Arquivo de Log, Portlet 2 Visualizador de Arquivo de Log, Portlet ParticipatingCommunities, Portlet Peers, Portlet Estatísticas de Prioridade da Fila, Portlet Links Rápidos, Portlet Feed RSS, Portlet Comunidades Patrocinadas, Portlet Alertas do Sistema, Portlet Procura da Web, Portlet Web View Plus
Implementação	deploymentadmin	Todas as permissões dos subgrupos ADAPTER_UTILITIES, DEPLOYMENT, EBXML, MAILBOX, MAPS, SERVICES, WEB_EXTENSIONS e WEB_SERVICES, mais UI Connect:Direct, UI Delete CPA e CPSS Schema/Extension, UI Delete Map, UI Delete PGP Profile, UI Delete SAP Routes, UI Delete Schema, UI Delete Service Instance, UI Delete SWIFTNet Routing Rule, UI Delete Web Resource, UI Delete Web Templates, UI Delete WSDL, UI Delete XSLT Template, UI Generate/Download WAR Files, UI Import/Export, UI Scheduler, UI Schemas, UI SSH Local Identity Key, UI SWIFTNet Routing Rule, UI XSLT
Administradores do EBICS	EBICS_ADM	UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS File Format Configuration, UI EBICS Offer Configuration, UI EBICS Order Type Configuration, UI EBICS Partner Profile Configuration, UI EBICS User Permission Configuration, UI EBICS User Profile Configuration, UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS Subscriber Key Validation,

Nome do Grupo	ID do Grupo	Permissões Herdadas do Grupo
Operadores do EBICS	EBICS_OPERATOR	UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS File Format Configuration, UI EBICS Offer Configuration, UI EBICS Order Type Configuration, UI EBICS Partner Profile Configuration, UI EBICS Subscriber Key Validation, UI EBICS User Permission Configuration, UI EBICS User Profile Configuration
EBXML	EBXML	BPSS, BPSSExtension, CPA, UI EBXML
ENVELOPES	ENVELOPES	ControlNumberHistory, ControlNumbers, EDISequenceCheckQueue, Envelopes, TransactionRegister, Envelopes UI
Notificações de Eventos Excepcionais	eventExceptional	Nenhum
CAIXA DE CORREIO	CAIXA DE CORREIO	Configuration, Messages, Routing Rules, UI Mailbox, VirtualRoots
MAPS	MAPS	ExtendedRuleLibraries, Maps, Standards, UI Maps
Administradores do Mailbox	mboxadmins	Todas as permissões dos grupos MAILBOX e Mailbox Browser Interface Users, mais DeadLetter Mailbox, Mailbox Global Delete, Mailbox Global Query, EBICS_DEADLETTER Mailbox
Usuários da Interface do Navegador do Mailbox	mbiusers	Mailbox Add Business Process, Mailbox Extract Business Process, Mailbox Path List Process, Mailbox Query Business Process, Mailbox Search Business Process, Mailbox Self Registration Business Process, Mailbox View Business Process, MBISearch JSP
OPERATIONS	OPERATIONS	JDBCMonitor, MessageMonitor, Perfdumps, SequenceManager, Statistics, ThreadMonitor, Troubleshooter, Tuning, UI Federated Systems, UI Operations
Parceiros Comerciais Provisórios	provisionalpartners	Nenhum
SERVICES	SERVICES	Configuration, Installation/Setup, UI Services
SSH	SSH	AuthorizedUserKey, KnownHostKey, RemoteProfiles, UI SSH, UserIdentityKey
Comprador do Web Suite Demo da Sessão	sd_buyer	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite Query Business Process, WebSuite RA Send Business Process, WebSuite Self Registration Business Process, WebSuite Session Demo Confirm Send Template, WebSuite Session Demo PO Send Business Process, WebSuite Session Demo PO Template, WebSuite Session Demo PO View Template, WebSuite Session Demo Query List Template

Nome do Grupo	ID do Grupo	Permissões Herdadas do Grupo
Fornecedores do Web Suite Demo da Sessão	sd_supplier	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite PO to Advance Ship Notice Template, WebSuite PO to Invoice Template, WebSuite PO Turn Business Process, WebSuite Query Business Process, WebSuite RA Send Business Process, WebSuite Self Registration Business Process, WebSuite Session Demo Confirm Send Template, WebSuite Session Demo PO Send Business Process, WebSuite Session Demo PO View Template, WebSuite Session Demo Query List Template
Sterling B2B Integrator Admin	super	Todas as permissões dos subgrupos ACCOUNTS, ADAPTER_UTILITIES, ADVANCED_SETUP, BPMONITOR, DEPLOYMENT, EBXML, ENVELOPES, MAILBOX, MAPS, Mailbox Administrators, OPERATIONS, SERVICES, SSH, WEB_EXTENSIONS e WEB_SERVICES, mais UI Archive, UI AS2 Trading Profile Setup, UI Basic Trading Profile Setup, UI BP Manager, UI Business Process, UI CA Certs, UI CodeLists, UI Connect:Direct, UI Contracts, UI Delete BP, UI Delete CPA and CPSS Schema/Extension, UI Delete Map, UI Delete PGP Profile, UI Delete SAP Routes, UI Delete Schema, UI Delete Service Instance, UI e SWIFTNet Routing Rule, UI Delete Trading Partner Data, UI Delete Web Resource, UI Delete Web Templates, UI Delete WSDL, UI Delete XSLT Template, UI Federated, UI Generate/Download WAR Files, UI Groups, UI Import/Export, UI Licenses, UI Lock Manager, UI Logs, UI Notify, UI Perimeter Servers, UI PGP Profile Manager, UI Reports, UI Scheduler, UI Schemas, UI SQL Tool, UI SSH Local Identity Key, UI Support Case Tool, UI SWIFTNet Routing Rule, UI System Certs, UI Trading Partners, UI Trusted Certs, UI User Accounts, UI XSLT
Operações do Sistema	operador	Todas as permissões do subgrupo OPERATIONS, mais UI Archive, UI Licenses, UI Lock Manager, UI Logs, UI Notify, UI Perimeter Servers, UI Reports, UI Scheduler, UI SQL Tool, UI Support Case Tool
Perfis de Comércio	tpadmin	Todas as permissões dos subgrupos ADVANCED_SETUP, ENVELOPES e SSH, mais UI AS2 Trading Profile Setup, UI Basic Trading Profile Setup, UI CA Certs, UI CodeLists, UI Contracts, UI Delete Trading Partner Data, UI System Certs, UI Trading Partners, UI Trusted Certs
WEB_EXTENSIONS	WEB_EXTENSIONS	Utilities, WebResources, WebTemplates
WEB_SERVICES	WEB_SERVICES	SchemaMappings, SecurityToken, UI Web Services, WebServicesManager, WSDLCheckin

Nome do Grupo	ID do Grupo	Permissões Herdadas do Grupo
Compradores do Web Suite	wsbuyers	WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack View Template, WebSuite PO Send Business Process, WebSuite PO Template, WebSuite PO View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite RA Send Business Process, WebSuite Remittance Advice Template, WebSuite Remittance Advice View Template, WebSuite Self Registration Business Process
Funcionários do Web Suite	wsemployees	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite ER Send Business Process, WebSuite Expense Report Template, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req Send Business Process, WebSuite Purchase Req Template, Websuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet Template, WebSuite TimeSheet View Template, WebSuite TS Send Business Process
Finanças do Web Suite	wsfinance	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process
Recursos Humanos do Web Suite	wshr	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet View Template
Gerentes do Web Suite	wsmanagers	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite ER Send Business Process, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req Send Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet View Template, WebSuite TS Send Business Process

Nome do Grupo	ID do Grupo	Permissões Herdadas do Grupo
Compradores do Web Suite	wspurchaser	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process
Fornecedores do Web Suite	wssupplier	WebSuite ASN Send Business Process, WebSuite ASN Template, WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Send Business Process, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Send Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite PO to Advance Ship Notice Template, WebSuite PO to Invoice Template, WebSuite PO to PO Ack Template, WebSuite PO Turn Business Process, WebSuite PO View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Remittance Advice View Template, WebSuite Self Registration Business Process

Permissões Necessárias para Acessar Recursos da UI

Este é o conjunto mínimo de permissões necessárias para acessar um item de menu e sua página e funcionalidade associadas. Designar o conjunto de permissões mínimas também pode disponibilizar algumas funcionalidades adicionais para o usuário. Se você não tiver permissão para um item de menu e sua funcionalidade associada, ele não será exibido.

No Menu de Administração > Processo de Negócios, Recursos da UI	Nome da Permissão / ID da Permissão
Processo de Negócios > Gerente	UI BP Manager (BPMANAGE) mais UI Business Process (BUSINESS_PROCESS)
Processo de Negócios > Monitor > Procura Avançada > Processo de Negócios	BusinessProcesses (PLTADM2) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > Correlação SWIFTNET	SWIFTNETCorrelation (GISADM9) mais UI BP Monitor (BPMONITOR) e UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
Processo de Negócios > Monitor > Procura Avançada > Fluxos de Dados	DataFlows (GISADM1) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > Documentos	Documents (GISADM2) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > Sessões de Comunicação	Communication Sessions (GISADM3) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > Correlação	Correlation (GISADM4) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > Correlação BPSS	BPSSCorrelations (GISADM5) mais UI BP Monitor (BPMONITOR)

No Menu de Administração > Processo de Negócios, Recursos da UI	Nome da Permissão / ID da Permissão
Processo de Negócios > Monitor > Procura Avançada > Correlação EBXML	EBXMLCorrelation (GISADM6) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > Correlação EDI	EDICorrelation (GISADM7) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Avançada > EDIINT	EDIINT (STDSADM6) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Procura Central	CentralSearch (GISADM10) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Processos Atuais	CurrentProcesses (PLTADM3) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Documentos Atuais	CurrentDocuments (GISADM11) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Monitor > Atividades Atuais	CurrentActivities (PLTADM4) mais UI BP Monitor (BPMONITOR)
Processo de Negócios > Estação de Trabalho de Entrada de Mensagem	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

No Menu de Administração > Parceiro Comercial, Recursos da UI	Nome da Permissão / ID da Permissão
Parceiro Comercial > Configuração > Básica	UI Basic Trading Profile Setup (BASIC_SETUP)
Parceiro Comercial > Configuração > Avançada > Identidades	Identities (GISADM12) mais UI Advanced Trading Profile Setup (ADVANCED_SETUP) A exclusão também requer permissão UI Delete Trading Partner (TP_DELETE)
Parceiro Comercial > Configuração > Avançada > Transportes	Transports (GISADM13) mais UI Advanced Trading Profile Setup (ADVANCED_SETUP) A exclusão também requer permissão UI Delete Trading Partner (TP_DELETE)
Parceiro Comercial > Configuração > Avançada > Troca de Documentos	DocumentExchange (GISADM14) mais UI Advanced Trading Profile Setup (ADVANCED_SETUP) A exclusão também requer permissão UI Delete Trading Partner (TP_DELETE)
Parceiro Comercial > Configuração > Avançada > Canais de Entrega	DeliveryChannels (GISADM15) mais UI Advanced Trading Profile Setup (ADVANCED_SETUP) A exclusão também requer permissão UI Delete Trading Partner (TP_DELETE)
Parceiro Comercial > Configuração > Avançada > Empacotamento	Packaging (GISADM16) mais UI Advanced Trading Profile Setup (ADVANCED_SETUP) A exclusão também requer permissão UI Delete Trading Partner (TP_DELETE)

No Menu de Administração > Parceiro Comercial, Recursos da UI	**Nome da Permissão / ID da Permissão**
Parceiro Comercial > Configuração > Avançada > Perfis	Profiles (GISADM17) mais UI Advanced Trading Profile Setup (ADVANCED_SETUP) A exclusão também requer permissão UI Delete Trading Partner (TP_DELETE)
Parceiro Comercial > Certificados Digitais > CA	UI CA Certs (CA_CERTS) mais UI System Certs (SYSTEM_CERTS) UI System Certs inclui a opção System.
Parceiro Comercial > Certificados Digitais > Confiáveis	UI Trusted Certs (TRUSTED_CERTS)
Parceiro Comercial > Certificados Digitais > Sistema	UI System Certs (SYSTEM_CERTS)
Parceiro Comercial > Envelopes de Documento > Envelopes	Envelopes (STDSADM1) mais UI Envelope (ENVELOPE)
Parceiro Comercial > Envelopes de Documento > Números de Controle	ControlNumbers (STDSADM2) mais UI Envelope (ENVELOPE)
Parceiro Comercial > Envelopes de Documento > Registro de Transação	TransactionRegister (STDSADM3) mais UI Envelope (ENVELOPE)
Parceiro Comercial > Envelopes de Documento > Histórico dos Números de Controle	ControlNumberHistory (STDSADM4) mais UI Envelope (ENVELOPE)
Parceiro Comercial > Envelopes de Documento > Fila de Verificação de Sequência EDI	EDISequenceCheckQueue (STDSADM5) mais UI Envelope (ENVELOPE)
Parceiro Comercial > Contratos	UI Contracts (CONTRACTS) mais UI Advanced Trading Partner Setup (ADVANCED_SETUP)
Parceiro Comercial > Listas de Códigos	UI CodeLists (CODELISTS)
Parceiro Comercial > AS2	UI AS2 Trading Profile Setup (AS2_SETUP)
Parceiro Comercial > SSH > Perfis Remotos	RemoteProfiles (ASSETADM1) mais UI SSH
Parceiro Comercial > SSH > Chave do Host Conhecido	KnownHostKey (ASSETADM2) mais UI SSH
Parceiro Comercial > SSH > Chave de Identidade do Usuário	UserIdentityKey (ASSETADM3) mais UI SSH
Parceiro Comercial > SSH > Chave do Usuário Autorizado	AuthorizedUserKey (ASSETADM4) mais UI SSH
Parceiro Comercial > AS3	UI AS3 Trading Profile Setup (AS3_SETUP)
Parceiro Comercial > Perfil do Parceiro de FTP Odette > Parceiro Físico	OftpPhysicalPartner (ASSETOFTP1) mais UI Adapter Utilities (ADAPTER_UTILITIES)
Parceiro Comercial > Perfil do Parceiro de FTP Odette > Contrato do Parceiro Físico	OftpPhysicalPartnerContract (ASSETOFTP3) mais UI Adapter Utilities (ADAPTER_UTILITIES)

No Menu de Administração > Parceiro Comercial, Recursos da UI	Nome da Permissão / ID da Permissão
Parceiro Comercial > Perfil do Parceiro de FTP Odette > Parceiro Lógico	OftpLogicalPartner (ASSETOFTP2) mais UI Adapter Utilities (ADAPTER_UTILITIES)
Parceiro Comercial > Perfil do Parceiro de FTP Odette > Contrato do Parceiro Lógico	OftpLogicalPartnerContract (ASSETOFTP4)
Parceiro Comercial > PGP > Gerente de Servidor	PGP Server Manager (ASSETADM55) mais UI PGP Profile Manager (PGP)
Parceiro Comercial > PGP > Gerente de Patrocinador	PGP Sponsor Manager (ASSETADM56) mais UI PGP Profile Manager (PGP)
Parceiro Comercial > PGP > Gerente de Parceiro	PGP Partner Manager (ASSETADM57) mais UI PGP Profile Manager (PGP)

No Menu de Administração > Implementação, Recursos da UI	Nome da Permissão / ID da Permissão
Implementação > Serviços > Instalação/Configuração	Installation/Setup (PLTADM9) mais UI Services (SERVICES)
Implementação > Serviços > Configuração	Configuração (PLTADM10) mais Serviços da UI (SERVIÇOS), UI BP Manager (BPMANAGE). Na V5.2.4.3 e superior, a UI Adapters StartStop também é requerida.
Implementação > Planejamentos	UI Scheduler (SCHEDULER)
Implementação > Mapas	Maps (ASSETADM5) mais UI_Maps
Implementação > Normas	Standards (STDSADM7) mais UI_Maps
Implementação > Bibliotecas de Regras Estendidas	ExtendedRuleLibraries (ASSETADM6) mais UI_Maps
Implementação > XSLT	UI XSLT (XSLT)
Implementação > Extensões da Web > Recursos da Web	WebResources (GISADM19) mais UI Web Extensions e UI Web Services (WEB_SERVICES) UI Web Services permite que o usuário efetue o registro de entrada de um novo arquivo de Recursos da Web
Implementação > Extensões da Web > Utilitários	Utilities (GISADM20) mais UI Web Extensions. Visível apenas no caso de um upgrade de uma versão anterior.
Implementação > Esquemas	UI Schemas (SCHEMAS)
Implementação > Caixas de Correio > Configuração	Configuration (MBXADM1) mais UI Mailbox (MAILBOX)
Implementação > Caixas de Correio > Raízes Virtuais	VirtualRoots (MBXADM2) mais UI Mailbox (MAILBOX)
Implementação > Caixas de Correio > Regras de Roteamento	RoutingRules (MBXADM3) mais UI Mailbox (MAILBOX)
Implementação > Caixas de Correio > Mensagens	Messages (MBXADM4) mais UI Mailbox (MAILBOX)
Implementação > EBXML > BPSS	BPSS (ASSETADM7) mais UI EBXML (EBXML)

No Menu de Administração > Implementação, Recursos da UI	**Nome da Permissão / ID da Permissão**
Implementação > EBXML> Extensão BPSS	BPSSExtension (ASSETADM8) mais UI EBXML (EBXML)
Implementação > EBXML > CPA	CPA (ASSETADM9) mais UI EBXM (EBXML)
Implementação > Gerenciador de Recursos > Identificações de Recurso	Resource Tags (PLTADM1) mais UI Deployment (DEPLOYMENT)
Implementação > Gerenciador de Recursos > Importar/Exportar	UI Import/Export (IMPORT_EXPORT)
Implementação > Utilitários do Adaptador > SAP Suite Builder	SAPSuiteBuilder (ASSETADM10) mais UI Adapter Utilities
Implementação > Utilitários do Adaptador > Rotas do Sap > Rotas do Sap	SAPRoutes (ASSETADM11) mais UI Adapter Utilities
Implementação > Utilitários do Adaptador > Rotas do Sap > SapRouteXRef	SAPRouteXREF (ASSETADM12) mais UI Adapter Utilities
Implementação > Utilitários do Adaptador > BEATuxedo	BEATuxedo (ASSETADM13) mais UI Adapter Utilities O item de menu não é exibido, a menos que o jar BEATuxedo esteja instalado.
Implementação > Utilitários do Adaptador > Regra de Roteamento SWIFTNET	UI SWIFTNet Routing Rule (SWIFTNET_ROUTING_RULE)
Implementação > Utilitários do Adaptador > Perfil de Serviço SWIFTNET	UI SWIFTNet Service Profile (SWIFTNET_SVC_PROFILE)
Implementação > Utilitários do Adaptador > Perfil de Serviço de Cópia SWIFTNET	UI SWIFTNet Copy Profile (SWIFTNET_COPY_PROFILE)
Implementação > Utilitários do Adaptador > Gerente de Política de Bloqueio de Acesso	LockoutPolicyManager (ASSETADM50)
Implementação > Utilitários do Adaptador > C:D Netmaps > C:D Node	CDNetmaps (ASSETADM51) mais UI Adapter Utilities (ADAPTER_UTILITIES)
Implementação > Utilitários do Adaptador > C:D Netmaps > C:D Netmaps	CDNodes (ASSETADM52) mais UI Adapter Utilities (ADAPTER_UTILITIES)
Implementação > Utilitários do Adaptador > C:D Netmaps > C:D Netmap X-REF	CDNetmapXref (ASSETADM53) mais UI Adapter Utilities (ADAPTER_UTILITIES)
Implementação > Utilitários do Adaptador > Configuração de Política	Adapter Policies (ASSETADM54)
Implementação > Utilitários do Adaptador > Raiz Virtual do Sistema de Arquivos	File System Virtual Root (ASSETADM58)
Implementação > Chave de Identidade do Host SSH	UI SSH Local Identity Key (SSH_LCL_ID_KEY) e UI SSH (SSH)
Implementação > Serviços da Web > Gerente	WebServicesManager (ASSETADM16) e UI Web Services (WEB_SERVICES)
Implementação > Serviços da Web > Mapeamentos de Esquema	SchemaMappings (ASSETADM17), UI Web Services (WEB_SERVICES) e UI EBXML (EBXML)
Implementação > Serviços da Web > Registro de Entrada do WSDL	WSDLCheckIn (ASSETADM18) mais UI Web Services (WEB_SERVICES)
Implementação > Serviços da Web > Token de Segurança	SecurityToken (ASSETADM18) mais UI Web Services (WEB_SERVICES)

No Menu de Administração > e-Invoicing, Recursos da UI	Nome da Permissão / ID da Permissão
e-Invoicing > Contratos	eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT) A exclusão também requer a permissão eInvoicing DELETE AGREEMENT (EINV_DELETE_AGREEMENT).
e-Invoicing > Archive Integrado	eInvoicing Archive (EINVOICING_ARCHIVE) mais eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE)
e-Invoicing > Configuração	eInvoicing Configuration (EINVOICING_CONFIGURATION)

No Menu de Administração > Operações, Recursos da UI	Nome da Permissão / ID da Permissão
Sistema > Solucionador de Problemas	Troubleshooter (PLTADM17) mais UI Operations (OPERATIONS)
Sistema > Desempenho > Ajuste	Tuning (PLTADM18) mais UI Operations (OPERATIONS)
Sistema > Desempenho > Estatísticas	Statistics (PLTADM19) mais UI Operations (OPERATIONS)
Sistema > Desempenho > Monitor de JVM	Perfdumps (GISADMIN27) mais UI Operations (OPERATIONS)
Sistema > Ferramentas de Suporte > Gerente de SQL	UI SQL Tool (SQLMANAGER)
Sistema > Ferramentas de Suporte > Caso de Suporte	UI Support Case Tool (SUPPORT_CASE)
Sistema > Logs	UI Logs (SYSTEM_LOGS)
Sistema > Licenças	UI Licenses (LICENSES)
Relatórios	UI Reports (REPORTS)
Monitor de Encadeamento	ThreadMonitor (PLTADM24) mais UI Operations (OPERATIONS)
Monitor JDBC	JDBCMonitor (PLTADM25) mais UI Operations (OPERATIONS) e UI SQL Tool (SQLMANAGER)
Gerenciador de Archive	UI Archive (ARCHIVE-UI) mais UI Operations (OPERATIONS), UI BP Manage (BPMANAGE) e UI Business Process (BUSINESS_PROCESS)
Gerenciador de Bloqueios	UI Lock Manager (LOCK_MANAGER)
Monitor de Mensagem	MessageMonitor (GISADM24) mais UI Operations (OPERATIONS)
Serviços de Perímetro	UI Perimeter Servers (PSERVERS)
Servidores Proxy	UI Proxy Servers (PROXYSERVERS) mais grupo de administradores do Sterling B2B Integrator

No Menu de Administração > Contas, Recursos da UI	Nome da Permissão / ID da Permissão
Grupos	UI Groups (GROUPS) mais UI Accounts (ACCOUNTS)
Permissões	Permissions (PLTADM27) mais UI Accounts (ACCOUNTS)
Contas do Usuário	UI User Accounts (USER_ACCOUNTS) mais UI Accounts (ACCOUNTS)
Política de Senha	PasswordPolicy (PLTADM29) mais UI Accounts (ACCOUNTS)
Notícias do Usuário	UserNews (GISADM25) mais UI Accounts (ACCOUNTS)
Minha Conta	MyAccount (PLTADM30)

Permissões Pré-configuradas

Permissões pré-configuradas são fornecidas com o sistema. Como permissões customizadas, eles fornecem acesso a diferentes módulos dentro do sistema.

Procurar Nomes de Permissão

Sobre Esta Tarefa

Para procurar uma permissão:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Permissões**.
2. Na página Permissões, conclua uma ações a seguir:
   - Em Procurar no campo **Nome da Permissão**, insira uma parte do nome da permissão ou o nome da permissão inteiro que você está procurando e clique em **Ir!** A página Permissões lista todas as permissões que correspondem aos critérios de procura.
   - Em Listar no campo **Em Ordem Alfabética**, selecione **TODOS** ou a letra com a qual começa o nome da permissão que você está procurando e clique em **Ir!** A página Permissões lista todas as permissões que correspondem aos critérios de procura.

Criar Permissões

Sobre Esta Tarefa

Se você tiver atualizado de uma versão anterior do sistema, as permissões existentes serão configuradas para Outro por padrão. Talvez seja necessário editar cada permissão para aplicar um novo tipo de permissão.

Antes de começar, você precisa saber as seguintes informações:

Campo	Descrição
ID da Permissão	ID da permissão para a permissão que você está criando. ID da permissão é o nome do processo de negócios, documento XSLT, modelo da web ou o recurso para o qual você está configurando a permissão. Inclua a extensão para o recurso após o ID. Necessário. IDs de permissão: • Devem ser exclusivos. • Fazem distinção entre maiúsculas e minúsculas. • O ID de permissão deve corresponder ao nome do processo de negócios, documento XSLT, modelo da web ou recurso. Se o ID de permissão e o nome do recurso não corresponderem exatamente, não será possível bloquear o recurso.
Nome da Permissão	Nome da permissão que você está criando. Necessário. Um nome de permissão deve ser exclusivo. Nomes de permissão fazem distinção entre maiúsculas e minúsculas, por exemplo, "Qualquer documento" e "Qualquer Documento" são dois nomes de permissão diferentes.
Tipo de Permissão	O tipo da permissão para a permissão que você está criando. Necessário. Os tipos de permissão incluem: • UI – Permite acesso a itens de menu específicos na interface. • Caixa de correio – Permite acesso a caixas de correio específicas no sistema. • Modelo – Permite acesso a modelos para web específicos. • BP – Permite acesso a processos de negócios específicos. • Rastreamento – Permite acesso a opções de rastreamento de documento específicas. • Comunidade – Permite acesso a opções de gerenciamento de comunidade específicas. • Serviço da Web • Serviço • eInvoicing • Outro – Permite acesso a recursos não identificados por um dos tipos anteriores.

Para criar uma permissão:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Permissões**.
2. Próximo de **Criar uma Nova Permissão**, clique em **Ir**!
3. Na página Permissões, insira **ID da Permissão**.
4. Insira o **Nome da Permissão**.
5. Selecione o **Tipo de Permissão**.
6. Clique em **Avançar**.
7. Revise as configurações de permissão.
8. Clique em **Concluir**.

Editar Nomes de Permissão
Sobre Esta Tarefa

Se você precisar alterar o nome de uma permissão para refletir a permissão mais de perto, edite um nome de permissão. Nomes de permissão devem ser exclusivos e fazem distinção entre maiúsculas e minúsculas. Não é possível alterar o ID da permissão. Se houver necessidade de editar o ID permissão, você deverá criar uma nova permissão.

Para editar um nome de permissão:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Permissões**.
2. Procure a permissão que deseja editar usando Procura de Nome de Permissão ou Listar em Ordem Alfabética e clique em **Ir!**
3. Próximo da Permissão que deseja editar, clique em **Editar**.
4. Insira um novo **Nome de Permissão**.
5. Atualize o tipo de permissão, se necessário, e clique em **Avançar**.
6. Revise as informações de configurações de permissões.
7. Clique em **Concluir**.

Excluir Permissões
Sobre Esta Tarefa

É possível excluir uma permissão associada a uma conta do usuário. Quando exclui uma permissão, você remove seu uso para todas as contas do usuário. Se a permissão sendo excluída for a única associada a uma conta do usuário, você deverá editar a conta do usuário para associar outra permissão. Se você não associar pelo menos uma nova permissão à conta do usuário, o usuário poderá efetuar login, mas não terá acesso a nenhum dos itens de menu.

Para excluir uma permissão:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Permissões**.
2. Procure a permissão que deseja excluir usando Procura de Nome de Permissão ou Listar em Ordem Alfabética e clique em **Ir!**
3. Na página Permissões, clique em **Excluir** para a permissão que deseja excluir.
4. Verifique se as informações de permissão correspondem à permissão que deseja excluir e clique em **Excluir**.

   O sistema exclui a permissão e exibe a mensagem:

   ```
   A atualização do sistema foi concluída com sucesso.
   ```

Revisar Nome da Permissão e ID
Sobre Esta Tarefa

Para revisar um nome de permissão e o ID:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Permissões**.
2. Procure a permissão que deseja revisar usando Procura de Nome de Permissão ou Listar em Ordem Alfabética e clique em **Ir!**

3. Selecione a permissão. O nome da permissão e o ID são exibidos.

Contas do Usuário

Contas do usuário são definidas por grupos, permissões e políticas de senha para ajudar a fornecer um ambiente seguro. Esse tipo de definição de conta do usuário é feito como um modelo de segurança baseado em função. Antes de criar quaisquer novas contas do usuário, você precisa determinar quais grupos, permissões e políticas de senha seu ambiente de negócios requer. A designação de grupos, permissões e políticas de senha é opcional.

Apenas contas com permissões de criação podem criar novas contas do usuário. Tarefas de contas do usuário incluem:

- Criar uma conta do usuário
- Procurar uma conta do usuário
- Editar uma conta do usuário
- Excluir uma conta do usuário

Permissões Padrão da Conta do Usuário

As permissões a seguir são designados automaticamente às contas de usuário:

- MyAccount (ID de permissão PLTADM30) – Permite acesso à página Minha Conta (Contas > Minha Conta).
- Permissões Admin Web App (ID de permissão WebAppAdminPermission) – Usada para acessar outros aplicativos da web.

Não remova essas permissões de contas do usuário. Se elas forem removidas acidentalmente, edite a Conta do Usuário e salve. As permissões ausentes serão restauradas.

Autenticação de Conta do Usuário

A autenticação de contas do usuário pode ser:

- Local – A autenticação é concluída com relação ao banco de dados.
- Externa – A autenticação é concluída com relação a um servidor LDAP. A autenticação externa não requer adaptador LDAP, que é usado com processos de negócios e permite a comunicação com servidores LDAP locais ou remotos usando Java Naming Directory Interface (JNDI). Se você não tiver uma licença para conexão única ou LDAP, todos os usuários que você criar serão usuários locais e autenticados com relação ao banco de dados do aplicativo. Para criar uma conta do usuário externo, você deve ter uma licença do aplicativo para conexão única ou LDAP.

Lista de Verificação de Criação de Conta do Usuário

Use esta lista de verificação para criar uma conta do usuário:

Tarefa	Lista de Verificação de Segurança Baseada em Função	Suas Notas
1	Criar novas permissões ou revisar as permissões pré-configuradas que vêm pré-instaladas.	
2	Criar novos grupos ou revisar os grupos que vêm pré-instalados.	

Tarefa	Lista de Verificação de Segurança Baseada em Função	Suas Notas
3	Criar uma política de senha customizada para designar ao usuário.	
4	Se você estiver usando autenticação externa, configure o ambiente para autenticação externa.	
5	Criar a conta do usuário e designar as permissões, os grupos e as políticas de senha.	

Configurar o Ambiente para Autenticação de Conta do Usuário Externo

Sobre Esta Tarefa

Se você estiver criando um usuário externo, é possível especificar um método de autenticação alternativo (geralmente LDAP).

Antes de criar uma conta do usuário externo, você deve:

Procedimento

1. Pare o Sterling B2B Integrator.
2. Especificar o método de autenticação alternativo incluindo ou modificando a configuração de autenticação no arquivo authentication_policy.properties.in. As propriedades precisam seguir este formato: authentication_4. = _value.*xxxxxx*
3. Insira `setupfiles.sh`.
4. Inicie o Sterling B2B Integrator.

Procurar Contas do Usuário

Sobre Esta Tarefa

Para procurar uma conta do usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Contas do Usuário**.
2. Conclua uma das ações a seguir:
   - Em Procurar no campo **Nome da Conta**, digite parte do nome ou o nome inteiro da conta do usuário que você está procurando e clique em **Ir!** A página Contas lista todas as contas de usuário que correspondem aos critérios de procura.
   - Em Listar no campo **Em Ordem Alfabética**, selecione **TODOS** ou a letra com a qual começa o nome da conta do usuário que você está procurando e clique em **Ir!** A página Contas lista todas as contas de usuário que correspondem aos critérios de procura.

criar contas do usuário

Sobre Esta Tarefa

Antes de começar, você precisa saber se está usando autenticação local ou externa:

- Local - A autenticação é concluída com relação ao banco de dados do aplicativo. Padrão.
- Externa – A autenticação é concluída com relação a um servidor LDAP. A autenticação externa não requer o adaptador LDAP, que é usado com processos de negócios e permite que o sistema se comunique com servidores LDAP locais ou remotos usando uma Java Naming Directory Interface (JNDI).

Se estiver designando uma ou mais Chaves de Usuário Autorizado a essa conta, as chaves deverão ser obtidas do parceiro comercial e registradas antes da criação da conta do usuário.

Nota: Embora diversos idiomas estrangeiros sejam suportados, uma conta de usuário não deve ser usada com mais de um idioma específico para evitar problemas de exibição de interface do usuário.

Também é necessário saber as informações a seguir:

Campo	Descrição
ID de Usuário	O ID do usuário para a conta do usuário que você está criando. O ID do usuário deve ter pelo menos cinco caracteres alfanuméricos de comprimento. Nenhum caractere ou pontuação especial é permitido. Necessário. Apenas para o banco de dados MySQL, o login não faz distinção entre maiúsculas e minúsculas. Você sempre deve usar IDs com ortografia exclusiva para que um usuário não use acidentalmente o ID de usuário de outro.
Senha (apenas Autenticação Local)	A senha para a conta do usuário que você está criando. A senha deve ter pelo menos seis caracteres alfanuméricos de comprimento. Caracteres especiais são permitidos. Necessário para usuários locais. Este campo não é exibido para usuários externos.
Confirmar Senha (apenas Autenticação Local)	Digite a senha uma segunda vez. Necessário para usuários locais. Este campo não é exibido para usuários externos.
Política (apenas Autenticação Local)	A política de senha para associar a essa conta do usuário. Na lista, selecione a política que deseja associar. Opcional. Este campo não é exibido para usuários externos. O sistema calcula a data de expiração a partir da primeira data em que o usuário efetua logon com essa senha.
Host de Autenticação (apenas Autenticação Externa)	O servidor Lightweight Directory Access Protocol (LDAP) no qual o usuário está sendo autenticado. O(s) servidor(es) listado(s) nesse campo é(são) especificado(s) no arquivo authentication_policy.properties.in.
Tempo Limite da Sessão	Quantidade de tempo em minutos que você pode ficar inativo antes de efetuar login novamente. O tempo está em minutos. Necessário.
Acessibilidade	Parte da interface com o usuário do painel à qual a conta do usuário tem acesso. Opcional. A seguir estão algumas opções de acessibilidade: • UI do Admin – Acessa apenas a área de janela Console Administrativo no painel. • UI do AS2 - Acessa apenas a interface do AS2 Edition. • UI do Painel – Acessa a interface do painel. Refine escolhendo um Tema do Painel.

Campo	Descrição
Tema do Painel	Painel predefinido ao qual a conta do usuário tem acesso. Necessário se a acessibilidade estiver configurada como UI do Painel. A seguir estão algumas opções de tema de painel: • Padrão • Operador • Participante • Patrocinador Participante • Patrocinador • AFT
Nome Dado	Nome do usuário. Necessário.
Sobrenome	Último nome do usuário. Necessário.
E-mail	Endereço de email do usuário.
Pager	Número do pager do usuário.
Idioma Preferencial	Configure o valor como **Usar Configurações de Aplicativo Cliente**. **Nota:** Esse valor instrui o Sterling B2B Integrator a usar o idioma especificado no navegador do usuário e/ou o código do idioma do sistema operacional do cliente. **Nota:** Este é o valor padrão.
ID do Gerente	ID do usuário do gerente do usuário.
Identidade	Identidade do parceiro comercial para associar à conta do usuário. Apenas um parceiro comercial pode ser associado a uma conta do usuário. Uma conta do usuário pode ser associada a vários grupos, cada um com sua própria associação de identidade de parceiro comercial. Isso permite que uma conta do usuário seja associada a mais de um parceiro comercial. O campo Identidade é usado para rotear mensagens no Mailbox. Selecione a identidade de um parceiro comercial da lista. O valor padrão é Organização Hub.

Para criar uma conta de usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Contas do Usuário**.
2. Próximo de **Criar uma Nova Conta**, clique em **Ir!**
3. Na página Nova Conta, selecione o **Tipo de Autenticação**.
4. Insira o **ID do Usuário**.
5. Insira a **Senha**.
6. Confirme a Senha.
7. Selecione **Política**.
8. Insira o **Tempo Limite da Sessão**.
9. Selecione **Acessibilidade**.

10. Selecione **Tema do Painel**.
11. Clique em **Avançar**.
12. Na página Chave do Usuário Autorizado SSH, designe uma ou mais chaves públicas. Mova as chaves para a área de janela **Disponível** para a área de janela **Designado** e clique em **Avançar**.
13. Na página Grupos, designe grupos de permissões. Mova os nomes de grupos da área de janela **Disponível** para a área de janela **Designado** e clique em **Avançar**.
14. Na página Permissões, designe permissões individuais. Mova as permissões da área de janela **Disponível** para a área de janela **Designado** e clique em **Avançar**. Por padrão, as permissões associadas aos grupos aos quais esse usuário é designado já estão selecionadas. As permissões necessárias são Permissão Admin Web App e MyAccount.
15. Na página Informações sobre o Usuário, insira o **Nome Dado**.
16. Insira o **Sobrenome**.
17. Insira o **Endereço de Email**.
18. Insira o **Número do Pager**.
19. Selecione o **Idioma Preferencial**. Selecione o valor **Usar Configurações do Aplicativo Cliente**.

    Nota: Esse valor instrui o Sterling B2B Integrator a usar o idioma especificado no navegador do usuário e/ou o código do idioma do sistema operacional do cliente.
20. Insira o **ID do Gerente**.
21. Selecione a **Identidade**.
22. Clique em **Avançar**
23. Revise as configurações da conta do usuário.
24. Clique em **Concluir**. A conta do usuário é criada e esta mensagem é exibida:

    ```
    A atualização do sistema foi concluída com sucesso.
    ```

    Se você criou um usuário externo, efetue logout do sistema e login novamente com a conta ou ID do usuário externo. O sistema autenticará o ID do usuário externo no servidor LDAP externo.

Editar Contas de Usuário

Sobre Esta Tarefa

Nota: Embora diversos idiomas estrangeiros sejam suportados, uma conta de usuário não deve ser usada com mais de um idioma específico para evitar problemas de exibição de interface do usuário.

Para editar uma conta de usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Contas do Usuário**.
2. Localize a conta de usuário que deseja editar usando as opções Procurar ou Listar.
3. Clique em **Editar** para a conta do usuário que deseja editar.
4. Faça quaisquer mudanças para o tipo de autenticação para esse usuário.

Se você alterar o tipo de autenticação de externo para local, será necessário criar uma senha para o usuário. Se você alterar o tipo de autenticação de local para externo, não será possível alterar a senha ou política de senha do usuário.

5. Faça quaisquer mudanças na **Nova Senha** e confirme a nova senha.
6. Faça quaisquer mudanças na **Política**.
7. Faça quaisquer mudanças para o **Tempo Limite da Sessão** e clique em **Avançar**.
8. Faça quaisquer mudanças para a **Chave do Usuário Autorizado SSH** e clique em **Avançar**.
9. Faça quaisquer mudanças de grupos e clique em **Avançar**.
10. Faça quaisquer mudanças de permissões e clique em **Avançar**.

    Não é possível remover a Permissão Admin Web App ou MyAccount.
11. Faça quaisquer mudanças para as informações do usuário e clique em **Avançar**.

    Nota: Para contas de usuário exibindo a interface com o usuário em uma língua estrangeira suportada, verifique se o valor Idioma Preferencial está configurado como **Usar Configurações de Aplicativo Cliente**. Esse valor instrui o Sterling B2B Integrator a usar o idioma especificado no navegador do usuário e/ou o código do idioma do sistema operacional do cliente.
12. Revise as configurações da conta do usuário.
13. Clique em **Concluir**.

Excluir Contas de Usuário

Sobre Esta Tarefa

Para excluir uma conta de usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Contas do Usuário**.
2. Localize a conta de usuário que deseja excluir usando as opções Procurar ou Listar.
3. Clique em **Excluir** para a conta do usuário que deseja excluir.
4. Clique em **OK**.
5. Revise as configurações da conta do usuário.
6. Clique em **Excluir**. A conta do usuário selecionada é excluída e esta mensagem é exibida:

   ```
   A atualização do sistema foi concluída com sucesso.
   ```

Atualizar Informações da Minha Conta

Sobre Esta Tarefa

Informações da Minha Conta são associadas ao seu nome de usuário e senha, portanto, quando você efetua login, suas informações pessoais são exibidas na página Minha Conta. É possível editar suas próprias informações de conta e alterar a página inicial que é vista quando você efetua login no sistema.

Há várias instâncias quando as informações de conta pessoal mudam que requerem que você edite as informações de conta. Além disso, talvez seja necessário alterar a senha para propósitos de segurança.

Nota: Embora diversos idiomas estrangeiros sejam suportados, uma conta de usuário não deve ser usada com mais de um idioma específico para evitar problemas de exibição de interface do usuário.

Para atualizar suas informações de conta:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Minha Conta**.
2. Se quiser atualizar sua senha de conta, no campo **Senha Antiga**, insira a senha atual e insira uma nova senha no campo **Nova Senha**. Insira a nova senha novamente no campo **Confirmar Nova Senha**.
3. Insira qualquer alteração nos campos **Nome Especificado**, **Sobrenome**, **E-mail**, ou **Pager**.
4. Para alterar as **Chaves de Usuário Autorizado SSH** para essa conta, mova as chaves das áreas de janela Disponível para Designado.
5. Para alterar **Idioma Preferencial**, selecione um idioma.

   Nota: Para contas do usuário exibindo a interface com o usuário em um idioma estrangeiro suportado, verifique se o valor está configurado para **Usar Configurações de Aplicativo Cliente**. Esse valor instrui o Sterling B2B Integrator a usar o idioma especificado no navegador do usuário e/ou o código do idioma do sistema operacional do cliente.
6. Para alterar a **Página de Boas-vindas** (Início do Console Administrativo) que é exibida quando você efetua login, selecione uma opção na lista.
7. Para alterar o número de processos exibidos de uma vez na página Processos Atuais, selecione um novo valor para **Tamanho da Página para Processos Atuais**.
8. Para alterar o número de documentos exibidos de uma vez na página Documentos Atuais, selecione um novo valor para **Tamanho da Página para Documentos Atuais**.
9. Se quiser reutilizar as janelas do navegador para ativar os atalhos, selecione **Reutilizar janelas para ativar atalhos**.
10. Se quiser que o sistema preencha procuras automaticamente com base nas sequências inseridas anteriormente, selecione **Conclusão automática para procuras**.
11. Se quiser que o sistema se lembre dos valores "procurar por", selecione **Lembrar dos valores "procurar por"**. Essa opção salva o último valor digitado em cada um dos campos Procurar.
12. Clique em **Salvar**. As novas informações da conta são salvas e esta mensagem é exibida:

    ```
    Sua atualização foi concluída com sucesso.
    ```

O usuário da conta do usuário existe para o login (V5.2.5 e superior)

O Sterling B2B Integrator fornece para o Active Directory saídas de usuário de sincronização, que podem ser usadas para gerenciar suas contas do usuário com o Active Directory, em vez da interface com o usuário do Sterling B2B Integrator. Essas saídas de usuário podem ser configuradas pelos Serviços IBM durante um IBM Services Customer Engagement. Entre em contato com seu representante de vendas IBM para obter mais informações.

Saída de usuário	Descrição
IUserLoginUserExit_preAuthenticate	Use para inserir um código customizado antes da autenticação.
IUserLoginUserExit_postAuthenticateFail	Use para inserir um código customizado após uma autenticação bem-sucedida.
IUserLoginUserExit_postAuthenticateSuccess	Use para inserir um código customizado após uma autenticação com falha.

O usuário da conta do usuário existe para efetuar logout (V5.2.6 e superior)

O Sterling B2B Integrator fornece para o Active Directory saídas de usuário de sincronização, que podem ser usadas para gerenciar suas contas do usuário com o Active Directory, em vez da interface com o usuário do Sterling B2B Integrator. Essas saídas de usuário podem ser configuradas pelos Serviços IBM durante um IBM Services Customer Engagement. Entre em contato com seu representante de vendas IBM para obter mais informações.

Saída de usuário	Descrição
ILogoutUserExit_OnSessionInvalidate	Use para inserir um código customizado antes que a sessão seja invalidada.

Conexão Única

Conexão Única

Conexão Única (SSO) é um processo de autenticação que permite que usuários acessem vários aplicativos inserindo apenas um nome de usuário e uma senha. Antes, um usuário efetuava login em cada aplicativo e tinha que gerenciar vários nomes de usuário e senhas.

A autenticação do usuário para SSO não requer o adaptador LDAP, que é usado com processos de negócios para se comunicar com servidores LDAP locais ou remotos usando uma Java Naming Directory Interface (JNDI).

Sterling B2B Integrator permite SSO por meio da integração com o Netegrity SiteMinder, ou por meio de classes de implementação customizada para plug-ins SSO em outros aplicativos e servidores de conexão única.

A conexão única é limitada aos seguintes componentes:

- Interface de Administração
- Interface do Mailbox
- Interface do Dashboard
- Interface do Advanced File Transfer (AFT)
- Interface do MyAFT

Classe Padrão do Provedor de Conexão Única

A interface SSOProviderDefault permite que o plug-in de Conexão Única (SS) manipule a função de conexão única para o Netegrity SiteMinder.

A URL de login de SSO para todas as interfaces, exceto Dashboard, é semelhante à interface de login normal. A URL da interface de Dashboard é http:Host:port/dashboard/sso.jsp. O cabeçalho da solicitação para a interface de Dashboard deve ter o valor SM_USER=SSO User Name (ou o valor pode ser configurado no arquivo security.properties em SSO_USER_HEADER).

É possível configurar a SSO para redirecionamento para uma página HTTP externa (em vez de a página de logoff Sterling B2B Integrator) após o usuário efetuar logoff na sessão de SSO. A página externa do servidor de SSO pode ser uma página de login ou logoff.

O exemplo a seguir mostra a classe SSOProviderDefault.java:

```
package com.sterlingcommerce.server_name.security.authentication;
import javax.servlet.*;
import javax.servlet.http.*;
import com.sterlingcommerce.server_name.security.SecurityManager;
import com.sterlingcommerce.server_name.util.frame.log.Logger;
import java.util.Properties;
import com.sterlingcommerce.server_name.util.frame.Manager;
import java.util.*;
/**
 * Implementação de Conexão Única padrão para ISSOProvider que usará
* Cabeçalho da Solicitação para obter SSO_USER
 *
 * Nome do desenvolvedor @author
 */
public final class SSOProviderDefault implements ISSOProvider  {
    private static final String CLASS_NAME = "SSOProviderDefault";
    private static final Logger LOG = SecurityManager.getInstance().getLogger();
    private static final Logger AUTHLOG =
            SecurityManager.getInstance().getAuthenticationLogger();
/**
* Autenticar processamento de SSO (login)
*
* @param Request : A solicitação de HTTP.
*
* @return String : O ID do usuário de SSO se a autenticação for aprovada
*                : null se a autenticação for negada
* << Nenhuma exceção lançada para o Provedor de SSO padrão - Tem valor ou é nulo >>
*/
public String authenticate(HttpServletRequest request)
                        throws SSOAuthenticationException, SSOException
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (AUTHLOG.debug) {
          AUTHLOG.logDebug(CLASS_NAME + " Authenticate user tag : " +
              SecurityManager.getInstance().getSSOAuthenticationHeader() +
              " value : " + sso_user);
    }
    return sso_user;
}
/**
 * AuthenticatePage SSO processing (Page)
 *
 * @param Request : A solicitação de HTTP.
*
 * @return boolean : True se a autenticação de SSO na Página for aprovada ou se nenhuma
 *                   autenticação de Página for necessária porque não está ativada ou
não há Usuário de SSO.
 *                 : False se a autenticação for negada
 *                   (Deve lançar SSOException se retornar false!!!!)
 */
public boolean authenticatePage(HttpServletRequest request)
```

```
                          throws SSOAuthenticationException, SSOException
{
    return true; // Sempre passar Validação de Página para SSOProviderDefault
    /*****  Remover comentário se quiser fazer verificação SSO_USER_HEADER
(SM_USER) na Página
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (sso_user != null) {
       passed = true;
    } else {
       passed = false;
       throw new
   SSOAuthenticationException(ISSOProvider.REASON_SSO_AUTHENTICATION_FAILURE);
    }
    return passed;   ******/
}
/**
 * Quando o usuário efetua logout chamando isto para não executar ações extra
*
 * @param Response : A resposta HTTP
 * @param Request : A solicitação de HTTP.
 * @param int reason : Um id para dizer de onde foi feita a chamada
* @param String : A Sequência identifica o tipo de sessão: WS, DASHBOARD, MAILBOX,
 *            AFT, MYAFT ou null se não souber
*
 * @return boolean : True para execução com sucesso,
 *           False se não for & deve usar lógica de logout padrão
 *
 */
public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
{
    HttpSession session = request.getSession(false);
    String forward = "SSO_FORWARD_URL";
    if (sessionType != null)   {
       forward = forward + ".";
       forward = forward + sessionType;
    }
    if (reason == REASON_GIS_SESSION_EXPIRED) {
       forward = forward + ".GIS_TIMEOUT";
    }
    else if (reason == REASON_LOGOUT)  {
       forward = forward + ".LOGOUT";
    }
    else {  // Outra razão : enviar tudo para VALIDATION_FAILED
       forward = forward + ".VALIDATION_FAILED";
    }
    String forwardUrl = getForwardURLParameter(forward);
    if (AUTHLOG.debug) {
       AUTHLOG.logDebug(CLASS_NAME + " Forward properties: " + forward +
" is forwardUrl: " + forwardUrl);
    }
    if (forwardUrl != null) {
       try {
           // Tempo Limite do Painel - Usar JSP para sair do IFrame
           if ((reason == REASON_GIS_SESSION_EXPIRED)&&
  (sessionType != null) &&
               (sessionType.equalsIgnoreCase(DASHBOARD_SESSION))) {
               if (AUTHLOG.debug) {
                    AUTHLOG.logDebug(CLASS_NAME + " Set ExternalSsoUrl = "
                                                + forwardUrl);  }
               request.setAttribute("ExternalSsoUrl", forwardUrl);
               return false; // Configure como false, é necessário manipular
o redirecionamento no JSP
           } else {
               response.sendRedirect(response.encodeRedirectURL(forwardUrl));
           }
```

```
        } catch (Exception e) {
            return false;
        }
        return true;
    }
    return false;   // Use a lógica padrão (isto é: GIS Logout/Login Page)
}
}
```

Componentes do Plug-in de Conexão Única

Sterling B2B Integrator permite uma classe de implementação customizada para plug-ins de Conexão Única (SSO) em outros aplicativos e servidores de conexão única. Você deve incluir uma nova classe de implementação SSO_AUTHENTICATION_CLASS.<n>=<New class entry> no arquivo security.properties para implementar um plug-in de SSO. É possível gravar classes de implementação customizada para plug-ins de SSO com base na seguinte classe de interface ISSOProvider.java.

Classe de Interface SSOProvider.java

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

Classe SSOException

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

Classe SSOAuthenticationException

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

Método de Autenticação do Usuário

O método de autenticação é inicializado durante o login. O método de autenticação retorna o ID do usuário após uma autenticação bem-sucedida. A SSOAuthenticationException é lançada para autenticação malsucedida. A exceção deve conter um código de razão apropriado e uma página de redirecionamento para manipulação se houver cabeçalhos de SSO presentes. Se não houver cabeçalhos de SSO presentes, o controle será passado de volta para a tela de login do sistema.

Método de Autenticação de Página

O método de autenticação será inicializado em cada página. Qualquer validação adicional durante a transição de página do servidor de SSO será manipulada nesse método. Por exemplo, é possível executar ping do servidor de SSO se a sessão de SSO tiver atingido o tempo limite. Para uma autenticação malsucedida, deve ser lançada uma exceção contendo um código de razão apropriado e uma página de redirecionamento.

Solicitações de SSO Inválidas

O método de invalidação é inicializado quando o usuário efetua logoff, falha ao autenticar o login ou a página ou quando a sessão expira. O método de redirecionamento HTTP deve ser executado para invalidar solicitações de SSO. Os métodos a seguir são inicializados para autenticação malsucedida:

- Se a autenticação do servidor de SSO for bem-sucedida e a autenticação do Sterling B2B Integrator for malsucedida, o método REASON_GIS_AUTHENTICATION_FAILURE será inicializado com o código de razão.
- Se a autenticação do servidor de SSO for malsucedida, o método REASON_SSO_AUTHENTICATION_FAILURE será inicializado com o código de razão.
- Se o usuário efetuar logoff, o método REASON_LOGOUT será inicializado com o código de razão.
- Se a sessão HTTP expirar, o método REASON_HTTP_SESSION_EXPIRED será inicializado com o código de razão.
- Se a sessão de SSO do usuário expirar, o método REASON_SSO_SESSION_EXPIRED será inicializado com o código de razão.

Conexão Única com Lista de Verificação do Netegrity SiteMinder

Antes de configurar a Conexão Única (SSO), você deve ter conhecimento de SSO e de Netegrity SiteMinder. Use esta lista de verificação para configurar a SSO com o Netegrity SiteMinder:

Tarefa	Conexão Única com Lista de Verificação do Netegrity SiteMinder	Observações
1	Instale o Netegrity SiteMinder e configure-o com um servidor proxy reverso.	
2	Configure os Arquivos de Propriedades para usar com Netegrity SiteMinder.	
3	Configure o Netegrity Secure Proxy Server.	
4	Crie Regiões Seguras do Servidor Netegrity.	

Para implementação customizada de plug-ins SSO para outros aplicativos e servidores de conexão única, consulte Componentes do Plug-in de Conexão Única.

Conexão única com o IBM Global High Availability Mailbox (V5.2.6 ou mais recente)

Os usuários do Sterling B2B Integrator com as permissões apropriadas podem acessar diretamente a ferramenta de gerenciamento do IBM® Global High Availability Mailbox usando a conexão única a partir do Sterling B2B Integrator para gerenciar o Global Mailbox.

Antes de Iniciar

Os usuários do Sterling B2B Integrator devem pertencer a um dos grupos a seguir para acessar diretamente a ferramenta de gerenciamento do Global Mailbox a partir do Sterling B2B Integrator:

- *CAIXA DE CORREIO*
- *Implementação*
- *Administradores da Caixa de Correio*
- *Sterling B2B Integrator Admin*

Sobre Esta Tarefa

Ao escolher acessar a ferramenta de gerenciamento do Global Mailbox por meio de conexão única, sua nova sessão do Global Mailbox será aberta em uma nova guia do navegador da web, enquanto sua sessão do Sterling B2B Integrator permanecerá disponível.

Somente é possível acessar o Global Mailbox por conexão única a partir do Sterling B2B Integrator. Se sair da ferramenta de gerenciamento do Global Mailbox, você não será desconectado da sua sessão do Sterling B2B Integrator.

Se quiser alterar sua senha do administrador do Global Mailbox, deve-se conectar diretamente à ferramenta de gerenciamento do Global Mailbox.

Restrição: Se você se conectar à ferramenta de gerenciamento do Global Mailbox por meio de conexão única, não será possível alterar sua senha do administrador do Global Mailbox e **Alterar senha** no menu **Administrador** não estará disponível.

Para acessar a ferramenta de gerenciamento do Global Mailbox por meio de conexão única:

Procedimento

1. A partir da página Console de Administração, expanda **Implementação** no Menu de Administração.
2. Expanda **Caixa de correio global**.
3. Selecione **Administração da caixa de correio**.
4. Clique no hiperlink **Ativar ferramenta de gerenciamento da caixa de correio global** para abrir uma nova sessão na ferramenta de gerenciamento do Global Mailbox.

   Lembre-se: Ao clicar no hiperlink **Ativar ferramenta de gerenciamento da caixa de correio global**, uma nova sessão do Global Mailbox é aberta em uma nova guia do navegador da web.

Configurar Arquivos de Propriedades para Conexão Única com Netegrity SiteMinder

Sobre Esta Tarefa

Para editar os arquivos neo-ui.properties e security.properties:

Procedimento

1. Pare o Sterling B2B Integrator.
2. Navegue para o */install_dir*/install/properties.
3. Abra o arquivo neo-ui.properties.
4. Inclua a entrada de SSO associada para cada interface. A amostra de código a seguir mostra a entrada associada nos mesmos sites HTTP:

```
url.host=%(host)
url.port=10200
url.cm=http://%(host):10200/communitymanagement/
url.cm.sso=http://%(host):10200/communitymanagement/
url.ob=http://%(host):10233/onboard/
url.ws=http://%(host):10200/ws/
url.ws.sso=http://%(host):10200/ws/
url.dash.sso=http://%(host):10233/dashboard/
url.ds=http://%(host):10200/datastore/
url.help=http://%(host):10200/help/index.htm?context=webhelplocal&single=true&topic=
url.help.ja=http://%(host):10200/help_ja/index.htm?context=webhelplocal&single=true& topic=
url.dash=http://%(host):10233/dashboard/
portlet.refresh.interval.seconds=60
url.aft=http://%(host):10200/aft/
url.aft.sso=http://%(host):10200/aft/
url.dmi=http://%(host):10200/dmi/
url.dmi.sso=http://%(host):10200/dmi/
```

5. Salve e feche o arquivo neo-ui.properties.
6. Abra o arquivo */install_dir*/install/properties/security.properties em um editor de texto.
7. No security.properties, localize os parâmetros de configuração ## Autenticação SSO, conforme mostrado na amostra de código a seguir:

```
## Configuração de Autenticação SSO
## ative autenticação sso (true, false) padrão=false
SSO_AUTHENTICATION_ENABLED=true
## ative autenticação sso em cada página (true, false) padrão=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false
## variável de cabeçalho http contendo ID do usuário autenticado externamente
SSO_USER_HEADER=SM_USER
## Lista de classes SSOProvider fornecidas para uso - Se Autenticação SSO estiver
## ativada, e precisar ter pelo menos uma classe, a seguinte será o padrão
## fornecido.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Tentará usar esta primeiro
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Tentará usar esta se a primeira
## falhar
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Tentará usar esta se a segunda ## também falhar
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Tentará usar esta se todas
## as primeiras classes –1 falharem
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS OProviderDefault
## Página Externa para SSO no Logout (Especifique a página externa Servidor SSO para cada um
## dos casos)
## Exemplo: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## Após o logout do Usuário de SSO do Mailbox, em vez de exibir Tela de Login do Mailbox,
## exibe a página da web da IBM.
SSO_FORWARD_URL.AFT.LOGOUT=
SSO_FORWARD_URL.MYAFT.LOGOUT=
SSO_FORWARD_URL.MAILBOX.LOGOUT=
SSO_FORWARD_URL.WS.LOGOUT=
SSO_FORWARD_URL.DASHBOARD.LOGOUT=
## Manipulação padrão para LOGOUT se não souber a origem
SSO_FORWARD_URL.LOGOUT=
## Página Externa para SSO ao atingir Tempo Limite (Especifique a página externa
Servidor SSO para cada ## do caso)
SSO_FORWARD_URL.AFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MYAFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MAILBOX.GIS_TIMEOUT=
SSO_FORWARD_URL.WS.GIS_TIMEOUT=
SSO_FORWARD_URL.DASHBOARD.GIS_TIMEOUT=
## Manipulação padrão para TIMEOUT se não souber a origem
SSO_FORWARD_URL.GIS_TIMEOUT=
## Página Externa para SSO durante falha de Validação/Autenticação (Validação de Usuário de SSO
## Falhou - No login ou Validação de Página)
SSO_FORWARD_URL.AFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=
SSO_FORWARD_URL.WS.VALIDATION_FAILED=
SSO_FORWARD_URL.DASHBOARD.VALIDATION_FAILED=
## Manipulação Padrão para VALIDATION FAILED se não souber a origem
SSO_FORWARD_URL.VALIDATION_FAILED=
```

8. Abaixo da entrada de configuração ## Autenticação SSO, faça as seguintes mudanças nos parâmetros de SSO:

Parâmetro	Descrição	Valor Fornecido	Novo Valor
SSO_AUTHENTICATION_ ENABLED	Ativa ou desativa o uso de SSO.	Falso	Verdadeiro
SSO_USER_HEADER	Nome do cabeçalho do usuário do Netegrity SiteMinder ou configuração do aplicativo SSO.	SM_USER Esse é o valor no Netegrity SiteMinder.	Deve corresponder à entrada no Netegrity SiteMinder ou aplicativo SSO.

Parâmetro	Descrição	Valor Fornecido	Novo Valor
SSO_PAGE_ AUTHENTICATION_ ENABLED	Ativa ou desativa a autenticação SSO em cada página	Falso	True - Para autenticar SSO em cada página. Altere apenas se a Classe de Provedor de SSO customizada for fornecida.
SSO_AUTHENTICATION_ CLASS.n	Classe de implementação para fornecer suporte de autenticação.	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	Selecione na lista de classes SSOProvider fornecida.
SSO_FORWARD_ URL URL	Exibe a página da URL fornecida após você efetuar logoff no Mailbox. Caso contrário, exibe o padrão.	Comentado Exibe a página padrão.	Forneça a URL.

9. Salve e feche o arquivo security.properties.
10. Inicie o Sterling B2B Integrator.

Configurar Netegrity Secure Proxy Server

Sobre Esta Tarefa

Antes de configurar o Netegrity Secure Proxy Server, você deve:

- Instalar o Sterling B2B Integrator em um servidor como acme.si.com.
- Saber o número da porta na qual a Mailbox Browser Interface (MBI) está instalada. Você deve usar essas informações nas regras de encaminhamento apropriadas.
- Saber o número da porta na qual a interface com o usuário do Painel do Sterling B2B Integrator está instalada. Você deve usar essas informações nas regras de encaminhamento apropriadas.

Para configurar o Netegrity Secure Proxy Server:

Procedimento

1. Inclua as regras de encaminhamento necessárias para Sterling B2B Integrator no arquivo /opt/netegrity/proxy-engine/conf/proxyrules.xml.

   O exemplo a seguir mostra como o arquivo proxyrules.xml concluído deve ficar após a inclusão das regras de encaminhamento para acessar os componentes do Sterling B2B Integrator:

```
<?xml version="1.0"?>
<?cocoon-process type="xslt"?>
<!DOCTYPE nete:proxyrules SYSTEM "file:////home/netegrity/proxy-engine/conf/dtd/proxyrules.dtd">
<!-- Proxy Rules-->
<nete:proxyrules xmlns:nete="http://acme.com/">
   <nete:cond criteria="beginswith" type="uri">
<nete:case value="/gbm">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/help">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/webxtools">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/mailbox">
  <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<nete:case value="/dashboard">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/portlets">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:case value="/datastore">
   <nete:forward>http://acme.gis.com:12433$0</nete:forward>
</nete:case>
<nete:default>
   <nete:forward>http://acme.portalserver.com$0</nete:forward>
</nete:default>
</nete:cond>
</nete:proxyrules>
```

2. Inclua as linhas a seguir no arquivo proxyrules.xml para desativar a verificação de Cross Server Scripting no servidor proxy seguro, já que o Sterling B2B Integrator não suporta execução de política Netegrity Cross Server Scripting.

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

3. Salve e feche o arquivo proxyrules.xml.

Criar Regiões do Netegrity Policy Server Secure

Sobre Esta Tarefa

Para o Sterling B2B Integrator trabalhar com o Netegrity Secure Proxy Server, o Netegrity Policy Server Administrator deve criar Regiões Seguras em torno de cada um dos padrões de URL sendo encaminhados pelo Servidor Proxy Seguro. Essas Regiões de Segurança devem ter as regras necessárias designadas para autenticação e autorização. Além disso, o agente da web no Servidor Proxy Seguro deve ser configurado para se comunicar com o Policy Server.

Criar uma região segura para cada padrão de URL listado:

Padrão de URL	Permite Acesso a:
/mbi/*	Interface do aplicativo Mailbox

Padrão de URL	Permite Acesso a:
/dashboard/*	Interface do aplicativo Dashboard usando o formato http://host:port/dashboard
/datastore/*	Componentes do armazenamento de dados
/portlets/*	Componentes do portlet de aplicativo na interface do Dashboard
/help/*	Componentes de ajuda contextual
/webxtools/*	Utilitários do Web Extensions
/gbm/*	Componentes do Graphical Process Modeler

Senhas

Políticas de Senha

Políticas de senha são conjuntos de decisões de segurança que você faz e aplica a diferentes contas de usuário de acordo com políticas de segurança em sua empresa. Essas opções incluem itens como número de dias durante os quais uma senha é válida e os comprimentos máximo e mínimo de uma senha.

É possível usar políticas de senha para aperfeiçoar as operações de segurança durante a inclusão de novos usuários. Em vez de incluir políticas individuais para cada usuário individual, é possível criar uma política de senha e aplicá-la a todos os usuários que requerem o mesmo acesso.

Após a criação de uma política de senha, é possível aplicá-la apenas a contas do usuário internas. Isso fornece maior flexibilidade na manutenção de suas políticas de segurança. Se você estiver usando LDAP, não será possível aplicar políticas de senha às contas externas.

Os valores padrão para política de senha são:

Parâmetro	Valor Padrão
ID de Política	default_user
Nome da Política	Política de Usuário Padrão
Número de dias válidos	60
Comprimento Mínimo	6
Comprimento Máximo	28
Número de senhas mantidas no histórico	5
Senha requer caracteres especiais	Selecionado
Mudança de senha obrigatória na primeira tentativa de login	Selecionado

Tarefas de política de senha incluem:

- Criar uma política de senha
- Procurar uma política de senha
- Editar uma política de senha
- Excluir uma política de senha
- Editar o parâmetro de bloquear

- Editar a mensagem de expiração de senha

Política de Senha Customizada

A Política de Senha Customizada do Sterling B2B Integrator é um recurso de segurança que permite incluir regras de política de senha adicionais. Essas regras de senha adicionais podem ajudar a evitar o uso de senhas fracas que podem ser facilmente descobertas por hackers e a rejeitar senhas inconformes. Para ativar essa funcionalidade, você precisa:

- Implemente algum código Java customizado por meio de um ponto de plugue. Depois de ativado, o ponto de plugue é usado para todos os usuários no sistema associado a uma política de senha (essa é uma configuração global).
- Inclua a propriedade passwordPolicyExtensionImpl no arquivo customer_overrides.properties.
- Aplique a política de senha customizada em Contas do Usuário.

A extensão de política de senha customizada é aplicada antes da política de senha padrão. Se uma senha violar mais de um requisito de política (um impingido pela classe de extensão e outro impingido pela implementação padrão), apenas a mensagem de erro retornada da classe de extensão será exibida para o usuário.

Exemplo: Exemplo de Política de Senha

Por exemplo, uma política de senha denominada Test pode ter as seguintes configurações para uma senha:

- Válido por 10 dias
- Mínimo de 10 caracteres de comprimento
- Máximo de 20 caracteres de comprimento
- Deve ter pelo menos dois caracteres especiais
- O usuário deve alterar a senha padrão durante o login inicial
- Número de senhas mantidas no histórico

Usando o exemplo anterior, o usuário recebe um nome de usuário e uma senha do administrador do sistema. O usuário efetua login usando o nome de usuário e a senha fornecidos e é solicitado que ele altere a senha. Se o usuário não fornecer uma senha com pelo menos 10 caracteres, mais de 20 caracteres ou sem pelo menos dois caracteres especiais, o sistema solicitará que o usuário faça correções. Após todas as condições configuradas na política de senha serem atendidas pelo usuário alterando a senha, o sistema salvará a nova senha e permitirá o acesso do usuário. Cada conta do usuário pode ter apenas uma política de senha associada a ela, mas é possível aplicar uma política de senha a diversas contas de usuário.

Além das mudanças de política de senha na interface, é possível alterar o número de vezes que um usuário pode não efetuar login corretamente antes de bloquear a conta do usuário que está tentando efetuar login.

Por exemplo, se o número de tentativas consecutivas de login antes da falha for configurado como três e você digitar a senha errada três vezes, não será possível efetuar login usando esse computador específico. É possível efetuar login usando qualquer outro computador que tenha acesso ao sistema.

Senha ou Passphrase de Instalação

Durante a instalação, você cria um passphrase do sistema para sua instalação do Sterling B2B Integrator. O passphrase é uma sequência altamente complexa com

mais de 16 caracteres. O passphrase do sistema é necessário para iniciar o sistema e para acessar informações do sistema protegidas. A única pessoa que pode atualizar ou alterar o passphrase é aquela que criou/instalou o software. Se você perder ou esquecer seu passphrase, não será possível iniciar o sistema. O único usuário que pode atualizar o passphrase do sistema é o usuário que executou a instalação.

O passphrase do sistema não é armazenado pelo sistema, exceto em instalações do Windows, onde ele é armazenado em um formulário ofuscado no security.properties para facilitar o sistema em execução como um serviço não interativo. Ele pode ser armazenado no claro nas outras plataformas no security.properties para que você não tenha de inseri-lo na linha de comandos ao iniciar o sistema. No entanto, o passphrase do sistema só é protegido pelo controle de acesso do arquivo do sistema operacional.

Lista de Verificação de Senha de Política Customizada

Use a lista de verificação a seguir para implementar uma política de senha do cliente:

Tarefa	Lista de Verificação de Senha de Política Customizada
1	Crie uma estrutura de diretório dentro de <SI_Install_Dir> para teste, política e extensão.
2	Crie a classe Java dentro do diretório de extensão.
3	Especifique a classe Java implementando a política de senha (propriedade passwordPolicyExtensionImpl) no arquivo customer_overrides.properties.
4	Inclua o jar da classe de implementação no caminho de classe.
5	Defina a mensagem de erro.

Exemplo - Política de Senha Customizada

Este é um exemplo de uma extensão de senha de política customizada.

A interface com.sterlingcommerce.woodstock.security.PasswordPolicyExtension foi incluída no sistema da seguinte forma:

```
public interface IPasswordPolicyExtension {
    /**
     * Implementa validação estendida em senhas e
retorna null se a
     * validação de senha for bem-sucedida. Se a validação falhar,
uma chave de mensagem de erro
     * que pode ser consultada em Login_*.properties* deve
ser retornada.
     * @param password - A sequência de senha para validar
     * @param policyId - O PWD_POLICY.POLICY_NAME da
política associada ao usuário, caso a extensão precise
dele.
     * @return String Retorna null se a validação de senha
foi bem-sucedida e a chave de mensagem de erro se a validação de senha falhar.
     */
    public String validateNewPassword (String password,
String policyName);
}
```

Retornar null do método indica que a senha foi aceita. Retornar anything else significa que a senha não era válida.

Exemplo de Implementação

```
package test.policy.extension;
import java.util.regex.Pattern;
public class PwdPolExtnImpl implements com.sterlingcommerce.woodstock.security.IPasswordPolicyExtension
{
   public String validateNewPassword(String
pwd,
                  String policyName) {
           // Verificações de validação de senha adicionais
                  boolean match=Pattern.matches(".*[a-z].*",
pwd) && Pattern.matches(".*[A-Z].*", pwd) && (Pattern.matches(".*[0-9].*",
pwd) || Pattern.matches(".*[^A-Za-z0-9].*",pwd));
                  if (match==true) return null;
                  else return "nogood";
      }

}
```

Procurar Políticas de Senha

Sobre Esta Tarefa

Para procurar uma política de senha:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Política de Senha**.
2. Na página Política de Senha, conclua uma das ações a seguir:
   - Em Procurar no campo **Nome da Política de Senha**, insira uma parte do nome ou o nome inteiro da política de senha que você está procurando e clique em **Ir!** A página Política de Senha lista todas as permissões que correspondem ao seu critério de procura.
   - Em Listar no campo **Em Ordem Alfabética**, selecione **TODOS** ou a letra com a qual começa o nome da política de senha que você está procurando e clique em **Ir!** A página Política de Senha lista todas as permissões que correspondem ao seu critério de procura.

Criar Políticas de Senha

Sobre Esta Tarefa

Você cria uma política de senha para designar a política a contas de usuário. Não é preciso associar uma política de senha a uma conta do usuário, mas isso não ajuda no gerenciamento de segurança.

Antes de começar, você precisa das seguintes informações:

Campo	Descrição
ID de Política	ID que identifica a política de senha no banco de dados.
Nome da Política	Nome da política exibido na interface com o usuário quando é feita qualquer referência à política de senha.

Campo	Descrição
Número de dias válidos	Número de dias durante os quais uma senha de usuário é válida. O padrão é 0, o que significa que a senha nunca expira. Se você fornecer um valor entre 1 e 999, o usuário receberá uma solicitação para mudar a senha quando esse período expirar. A contagem regressiva de expiração começa na primeira vez que um usuário efetua login após uma senha ser designada à conta do usuário.
Comprimento Mínimo	Comprimento mínimo que a senha deve ter. Necessário. Os valores válidos são quaisquer numerais. Esse número deve ser configurado para pelo menos 6. O valor padrão é 6. Se nenhuma política for aplicada, o sistema impõe um comprimento mínimo de 6.
Comprimento Máximo	Comprimento máximo que a senha pode ter. Necessário. Os valores válidos são quaisquer numerais. Esse número deve ser configurado para pelo menos o mesmo número que o comprimento mínimo. O valor padrão é 28.
Número de senhas mantidas no histórico	Número de senhas para manter na tabela PWD_HISTORY no banco de dados para um usuário. Após esse número de senhas ser excedido, a antiga senha é removida da tabela e pode ser reutilizada pelo usuário. O valor padrão é 0.
Senha requer caracteres especiais	Especifica que a senha deve conter pelo menos um caractere especial. Os valores válidos incluem incluem numerais, letras maiúsculas, !, @, #, $, %, ^, &, ou *.
Mudança de senha necessária na primeiro tentativa de login	Especifica que o usuário deve alterar a senha padrão após o login inicial. Isso solicita que o usuário altere a senha após efetuar login pela primeira vez.

Para criar uma política de senha:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Política de Senha**.
2. Próximo de **Criar uma Nova Política de Senha**, clique em **Ir!**
3. Na página Política de Senha, insira o **ID de Política**.
4. Insira o **Nome da Política**.
5. Insira o **Número de Dias Válidos**.
6. Insira o **Comprimento Mínimo**.
7. Insira o **Comprimento Máximo**.
8. Insira o **Número de dias que a senha é mantida no histórico**.
9. Se for obrigatório a senha conter caracteres especiais, selecione a caixa de opção.
10. Se for obrigatório o usuário alterar a mudança de senha na primeira tentativa de login, selecione a caixa de opção.
11. Clique em **Avançar**.
12. Revise as configurações de política de senha.
13. Clique em **Concluir**.

Editar Políticas de Senha

Sobre Esta Tarefa

Para editar uma política de senha:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Política de Senha**.
2. Localize a política de senha que deseja editar usando as opções Procurar ou Listar.
3. Clique em **Editar** para a política de senha que deseja editar.
4. Na página Configurações de Política de Senha, faça as mudanças apropriadas e clique em **Avançar**.
5. Revise as configurações de política de senha.
6. Clique em **Concluir**.

   A mensagem a seguir é exibida:

   ```
   A atualização do sistema foi concluída com sucesso.
   ```

Excluir Políticas de Senha

Sobre Esta Tarefa

Se você excluir uma política de senha, as contas do usuário associadas a essa política de senha específica ainda poderão efetuar login, mas o usuário não será forçado a alterar a senha. Se o usuário não alterar a senha, nenhuma validação será concluída com relação à nova senha.

Para excluir uma política de senha:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Política de Senha**.
2. Localize a política de senha que deseja excluir usando as opções Procurar ou Listar.
3. Clique em **Excluir** para a política de senha que deseja excluir.
4. Na página Confirmar, clique em **Excluir**.

   A mensagem a seguir é exibida:

   ```
   A atualização do sistema foi concluída com sucesso.
   ```

Alterar o Número de Dias para Expiração de Senha de Usuário

Sobre Esta Tarefa

O sistema notifica você de expirações de senha iminentes, colocando uma mensagem na seção Alertas do Sistema da página Início do Console Administrativo. A mensagem indica que a senha expirará em um número específico de dias. Cada dia, o número será reduzido em um, até o dia em que a senha expirar, quando será solicitado que você altere sua senha.

Os administradores do sistema podem alterar o número de dias antes da expiração no arquivo ui.properties.in. Você deve fazer todas as mudanças no arquivo ui.properties.in, e não no arquivo ui.properties. Se você fizer mudanças no arquivo ui.properties e reiniciar o sistema, as mudanças feitas no arquivo ui.properties serão sobrescritas pelo arquivo ui.properties.in.

Para alterar o número de dias para a expiração da senha:

Procedimento

1. Pare o Sterling B2B Integrator.
2. Navegue para o */install_dir*/install/properties.
3. Abra o arquivo ui.properties.in.
4. Localize a entrada MsgPwdExpires= 15.
5. Altere 15 para o novo número de dias para a expiração da senha do usuário.
6. Salve o arquivo.
7. Navegue para */install_dir*/install/bin.
8. Insira **setupfiles.sh**.
9. Reinicie o Sterling B2B Integrator. As mudanças feitas no arquivo ui.properties.in são aplicadas ao arquivo ui.properties e entrarão em vigor para todas as contas do usuário.

Reconfigurar sua Própria Senha após Bloqueio

Sobre Esta Tarefa

Se você estiver bloqueado:

- Efetue login usando outro computador que tenha acesso ao sistema.
- Espere 30 minutos e o bloqueio expirará, permitindo que você tente efetuar login usando o computador bloqueado novamente.
- Entre em contato com o administrador do sistema para ter o bloqueio removido por meio da página Gerenciador de Bloqueios. Isso permite tentar efetuar login usando o computador bloqueado novamente.

Definir Mensagem de Erro para Política de Senha Customizada

Sobre Esta Tarefa

As mensagens de erro informam o usuário das regras de senha e lista as razões para mudanças de senha rejeitadas. As mensagens de erro de senha customizada são definidas nos arquivos Login_*language_dir*.properties_*uniqueID*_ext. Se um texto específico customizado não for fornecido, a mensagem de erro padrão será retornada para o usuário. O arquivo Login_*language_dir*.properties_*uniqueID*_ext não faz parte do código do sistema padrão. Ele deve ser criado após a instalação inicial do sistema e preenchido para corresponder ao seu ambiente.

Para definir uma mensagem de erro para uma extensão de política de senha customizada:

Procedimento

1. Navegue para o diretório */install_dir*/install/properties/lang/*language_dir*. Em que *language_dir* é o idioma configurado para o código de idioma do cliente (por exemplo, en, ja, fr).
2. Edite o arquivo Login_*language_dir*.properties_*uniqueID*_ext. Em que language_dir é o idioma configurado para o código de idioma do cliente e <filename> é o identificador exclusivo para a nova extensão de senha customizada. Por exemplo: Login_en.properties_custompasswd_ext.
3. Inclua uma entrada no arquivo para a condição de erro configurada no arquivo de extensão customizado e defina a sequência descritiva para retornar ao

usuário. Por exemplo, nogood = A senha deve conter no mínimo um caractere minúsculo, um caractere maiúsculo e um dígito ou caractere especial.

4. Salve e feche o arquivo.

Especificar Extensão da Política de Senha Customizada no Arquivo customer_overrides.property

Sobre Esta Tarefa

Para conectar a implementação customizada, o nome da classe Java precisa ser especificado na propriedade passwordPolicyExtensionImpl no arquivo customer_overrides.properties.

Para especificar a classe Java que implementa a extensão de política de senha:

Procedimento

1. Navegue até o diretório de instalação.
2. Navegue para o diretório de propriedades.
3. Edite o arquivo customer_overrides.properties.
4. Inclua a propriedade passwordPolicyExtensionImpl no final do arquivo e insira o nome da classe Java que implementa a validação estendida de senhas. Por exemplo,
   security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl.
5. Salve e feche o arquivo.

Incluir JAR da Classe de Implementação no Caminho para a Política de Senha Customizada

Sobre Esta Tarefa

A classe de implementação de extensão deve ser compilada e compactada como jar da seguinte forma:

Procedimento

1. Navegue para *SI_Install_Dir*.
2. Insira o comando a seguir para compilar o arquivo de classe customizada:
   `javac -cp /SI_Install_Dir/jar/platform_ifcbase/1_3/platform_ifcbase.jar test/policy/extension/*.java`
3. Crie o arquivo JAR executando o comando a seguir de dentro de *SI_Install_Dir* :
   `jar cf any_filename.jar absolute_path_to_custom_class_file.class` em que `any_filename.jar` é o nome do novo arquivo JAR a ser criado, e em que `absolute_path_to_custom_class_file.class` é o nome do arquivo de classe Java de implementação customizada. Por exemplo: `jar cf userExit.jar test/policy/extension/PwdPolExtnImpl.class`
4. Navegue para o diretório *SI_Install_Dir*/bin.
5. Insira o comando a seguir para incluir o jar recém-criado para o caminho de classe:
   `./install3rdParty.sh userExit 1_0 -j path_to_jar_that_was_created_in_step3`
   por exemplo, `./install3rdParty.sh userExit 1_0 -j SI_Install_Dir/userExit.jar`

Autenticação LDAP

Lightweight Directory Access Protocol (LDAP) como uma ferramenta de autenticação do Sterling B2B Integrator

Lightweight Directory Access Protocol (LDAP) é um conjunto de protocolos usados para acessar informações armazenadas em um diretório de informações, que é um diretório LDAP. Um diretório LDAP é um banco de dados, mas não um banco de dados relacional, usado para gerenciar informações que são difundidas para diversos servidores em uma rede e é otimizado para o desempenho da leitura.

É possível usar o LDAP para delegar autenticação de uma conta do usuário externo a um diretório LDAP e para fornecer autenticação usando as mesmas informações de segurança usadas para outros aplicativos em sua empresa. Se sua empresa já tiver adotado LDAP, é possível usar seus diretórios LDAP existentes.

A autenticação de conta do usuário não requer o adaptador LDAP, que é usado com processos de negócios para se comunicar com servidores LDAP locais ou remotos usando uma Java Naming Directory Interface (JNDI).

Se seu servidor LDAP não estiver funcionando, os usuários que têm contas internas reterão o acesso; no entanto, os usuários que têm contas externas não terão acesso até que o servidor LDAP esteja funcionando.

Antes de poder configurar o LDAP com o Sterling B2B Integrator, você deve ter:

- Conhecimento de LDAP
- Acesso a um servidor LDAP instalado e configurado contendo informações sobre o usuário
- O local do servidor LDAP
- (Para SSL) Instalado certificados de segurança no Keystore e Armazenamento Confiável
- Criado as contas do usuário externo para cada usuário que será autenticado por meio de seu servidor LDAP
- (Para SSL) O local do Keystore e do Armazenamento Confiável

Exemplo: Parâmetros de Configuração de Autenticação LDAP

O exemplo a seguir mostra os parâmetros de configuração da Autenticação LDAP:

```
## Configuração da Autenticação GIS/LDAP
## propriedades de sistema java (jsse) de ssl opcional para localizar e usar
## o armazenamento confiável e o keyStore
## um conjunto de propriedades de keystore e armazenamento confiável
para toda configuração LDAP.
# LDAP_SECURITY_TRUSTSTORE=/home/applications/properties/cacerts
# LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# LDAP_SECURITY_KEYSTORE=/home/applications/properties/keystore
# LDAP_SECURITY_KEYSTORE_PASSWORD=password
#########################################################################
#
# Configuração de Autenticação GIS
#
#########################################################################
authentication_0.className=com.sterlingcommerce.woodstock.security
.GISAuthentication
authentication_0.display_name=GIS Authentication
#########################################################################
#
```

```
# Para Configuração de Autenticação de Servidor LDAP adicional,
# copie-cole o conjunto de propriedades a seguir e remova o comentário de
# todas as propriedades que começam com "authentication_<number>".
# Substitua a tag <number> pelo número adicional do método de
# autenticação. Por exemplo, se o último método de autenticação for
# "authentication_0", você deverá substituir a tag <number> por "1"
# para seu próximo novo método de autenticação LDAP.
# Em seguida, você tem que alterar cada propriedade com informações
do servidor properLDAP.
#
# Você pode comentar a linha ou deixar em branco o "authentication_<number>
# .security_protocol"
# se você não for usar SSL para protocolo de segurança.
#
# As propriedades de autenticação LDAP authentication_1 seriam substituídas se
# o cliente já usou autenticação LDAP como configurado em security
# .properties.
#
########################################################################
########################################################################
#
# Configuração de Autenticação do <number> do Servidor LDAP
#
########################################################################
# authentication_<number>.className=com.sterlingcommerce.woodstock.security
# .LDAPAuthentication
# authentication_<number>.display_name=LDAP Serveragrona <number>
## enable ldap authentication  (true, false) default=false
# authentication_<number>.enabled=true
## jndi parameters for ldap connections
# authentication_<number>.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
# authentication_<number>.server=acme.inc.com
# authentication_<number>.port=636
# authentication_<number>.security_type=simple
# authentication_<number>.principle=cn=Manager,dc=acme,dc=inc,dc=com
# authentication_<number>.credentials=SecretPassword
## comente a linha ou deixe em branco essa propriedade se o servidor não for
## usar SSL para o protocolo de segurança.
#authentication_<number>.security_protocol=ssl
## parâmetros de procura para senha do usuário
# authentication_<number>.password_attribute=userPassword
# authentication_<number>.search_root=dc=acme,dc=inc,dc=com
# authentication_<number>.search_filter=(uid=<userid>)
# authentication_<number>.with_user_bind=falseBelow the ##LDAP Authentication
```

Lista de Verificação de Configuração de Autenticação LDAP

Use esta lista de verificação para configurar LDAP com Sterling B2B Integrator:

Tarefas	Lista de Verificação de Configuração LDAP
1	Configurar LDAP em um dos seguintes modos: • Modo de Comparação de Senha • Modo Binário de Senha
2	Configurar LDAP com Sterling B2B Integrator
3	Verificar configuração LDAP
4	Opcional. Criptografar senhas LDAP.

Configurar LDAP no Modo de Ligações de Senha

Sobre Esta Tarefa

Para configurar LDAP em um modo de ligações de senha:

Procedimento

Insira seu **ID do usuário** e sua **senha** da conta do usuário externa. O sistema:

- Tenta se ligar ao repositório LDAP com credenciais ativando a execução das consultas necessárias.
- Procura o usuário no diretório LDAP com o ID do usuário adequado.
- Recupera o nome distinto (DN) do usuário do diretório LDAP.
- Tenta se ligar ao repositório LDAP usando o DN e a senha do usuário.
- Êxito – O sistema se liga ao repositório LDAP como um usuário.
- Falha – O sistema não pode se ligar ao repositório LDAP como um usuário.

Configurar LDAP no Modo de Comparação de Senhas

Sobre Esta Tarefa

Para configurar LDAP em um modo de comparação de senhas:

Procedimento

1. Insira seu **ID do usuário** e sua **senha** da conta do usuário externa.
2. O sistema tenta se ligar ao repositório LDAP com credenciais ativando a execução de consultas necessárias.
3. O sistema procura o usuário no diretório LDAP com o ID do usuário adequado.
4. O sistema recupera a senha de usuário do diretório LDAP.
5. O sistema compara a senha fornecida pelo usuário com a senha recuperada do diretório LDAP. Se as senhas corresponderem, você será autenticado e terá permissão de acesso ao sistema. Se as senhas não corresponderem, você não será autenticado e não terá o acesso permitido.

Configurar LDAP com Sterling B2B Integrator

Sobre Esta Tarefa

Para configurar o Sterling B2B Integrator para usar o LDAP, você deve editar o arquivo authentication_policy.properties.in. Também é possível usar o arquivo customer_overrides.properties para configurar os valores de propriedade que não serão sobrescritos por uma instalação de correção.

Para configurar a autenticação LDAP:

Procedimento

1. Pare o Sterling B2B Integrator.
2. Navegue até o diretório de instalação.
3. Navegue para o diretório de propriedades.
4. Abra o arquivo authentication_policy.properties.in.
5. Em authentication_policy.properties.in, localize a entrada de configuração ## Autenticação GIS/LDAP.
6. Abaixo da entrada de configuração ## Autenticação GIS/LDAP, faça as seguintes mudanças nos parâmetros LDAP:

Parâmetro	Descrição	Valor Fornecido	Alterar para
#LDAP_SECURITY_ TRUSTSTORE	Caminho para o armazenamento confiável local. Você deve ter os certificados requerido pelo LDAP armazenados no armazenamento confiável. Não é possível usar certificados de parceiros comerciais. Opcional. Use somente se você estiver usando SSL.	Caminho inativo	Caminho completo para o armazenamento confiável local.
#LDAP_SECURITY_ TRUSTSTORE_ PASSWORD	Senha que permite acesso ao armazenamento confiável. Opcional. Use somente se você estiver usando SSL.	changeit	Senha que permite acesso ao truststore local.
#LDAP_SECURITY_ KEYSTORE	Caminho para o keystore local. Você deve ter os certificados LDAP necessários armazenados no keystore. Não é possível usar certificados de parceiros comerciais. Opcional. Use somente se você estiver usando SSL.	Caminho inativo	Caminho completo para o keystore local.
#LDAP_SECURITY_ KEYSTORE_ PASSWORD	Senha que permita acesso ao keystore. Opcional. Use somente se você estiver usando SSL.	password	Senha que permite acesso ao keystore local.
#authentication_ <number>. enabled	Ativa ou desativa o uso de LDAP. False – Todos os usuários que são criados a partir desse host de autenticação serão desativados (falha de login). True – Cada usuário pode ser acessado ou internamente ou externamente, mas não das duas formas, desde que cada ID do usuário seja exclusivo. Esse valor não é verificada quando é para autenticação interna.	Falso	Verdadeiro
#authentication_<number> .jndi_factory	Nome de classe da classe de factory que cria o contexto inicial para o provedor de serviços LDAP. Essa é a factory de contexto padrão enviada com o JDK.	com.sun. jndi.ldap. LdapCtx Factory	Sem mudança
#authentication_ <number>.server	URL especificando o nome do host do servidor LDAP.	Caminho inativo	URL do host do LDAP local.

Parâmetro	Descrição	Valor Fornecido	Alterar para
#authentication_ <number>.port	O número da porta do servidor LDAP.		
#authentication_ <number>. security_type	Método de autenticação para o provedor usar. O sistema suporta apenas autenticação simples.	simples	Sem mudança
#authentication_ <number>. princípio	Identidade do princípio de autenticação, que permite que o sistema execute consultas. Esse parâmetro é o componente de nome em uma solicitação de ligação LDAP ASN.1.	cn=Manager, dc=amr, dc=stercomm, dc=com	Informações de nomenclatura locais.
#authentication_ <number>. credenciais	Configuração de senha no repositório LDAP para o princípio de LDAP que permite que o sistema execute consultas.	SecretPassword	Senha local que acompanha o princípio local.
#authentication_ <number>. security_protocol	Objeto especificando qual protocolo de segurança o provedor deve usar.	SSL	Nenhuma mudança. Esse parâmetro não ficará visível se você tiver optado por não usar SSL.
#authentication_ <number>. password_attribute	Nome do atributo LDAP que contém a senha do usuário. Esse parâmetro só será usado se #LDAP_ AUTHENTICATE_ WITH_USER_BIND estiver configurado como false.	userPassword	Atributo local que contém a senha.
#authentication_ <number>. search_root	Objeto especificando a raiz a partir da qual a consulta do usuário é baseada.	dc=amr, dc=stercomm, dc=com	Caminho da procura local.
#authentication_ <number>.search_filter	Objeto especificando o modelo a ser usado na procura. O valor <userid> é substituído dinamicamente no momento da solicitação pelo ID do usuário solicitando autenticação.	(uid=<userid>)	Um servidor Windows Active Directory pode usar uma entrada como (sAMAccount Name=<userid>)

Parâmetro	Descrição	Valor Fornecido	Alterar para
#authentication_ <number>. with_user_bind	Especifica se você deve autenticar um usuário de acordo com uma ligação bem-sucedida. False – O sistema extrai o valor da senha de usuário do servidor LDAP e executa uma comparação com as credenciais do usuário fornecidas. True – O sistema se liga ao servidor LDAP usando o nome distinto do usuário e as credenciais fornecidas. Uma ligação bem-sucedida significa uma autenticação bem-sucedida.	falso	Altere para true se quiser autenticar com ligação de usuário.

7. Salve o arquivo authentication_policy.properties.in.
8. Insira */install_dir*/install/bin/setupfiles.sh (UNIX) ou *install_dir*\install\bin\setupfiles.cmd (Windows) para atualizar entradas LDAP no arquivo authentication_policy.properties a partir do arquivo authentication_policy.properties.in.
9. Inicie o Sterling B2B Integrator.

   As mudanças no arquivo authentication_policy.properties são aplicadas e agora é possível começar a usar o servidor LDAP para autenticar usuários.

   Após a inicialização, o sistema identifica servidores LDAP a partir do arquivo authentication_policy.properties. O sistema autentica usuários externos quando eles efetuam login.

Verificar Configuração de LDAP

Sobre Esta Tarefa

Para verificar se você configurou o LDAP corretamente com o Sterling B2B Integrator, revise o arquivo Authentication.log em Autenticação de Usuário para assegurar que o sistema aceita a configuração do LDAP.

Se houver problemas na conexão com o diretório LDAP ou se a autenticação LDAP falhar, verifique as instruções de log DEBUG no arquivo Authentication.log para resolver o problema. O arquivo Authentication.log registra todas as tentativas de login, sejam elas bem-sucedidas ou malsucedidas.

Criptografar Senhas LDAP

Sobre Esta Tarefa

É possível ocultar senhas relacionadas ao LDAP nos arquivos de propriedades criptografanda-os no arquivo customer_overrides.property.

Os parâmetros / propriedades a seguir podem ser usados para criptografarem as senhas do LDAP no arquivo customer_overrides.properties:

Parâmetro/Propriedade	Descrição
authentication_policy.authentication _1.credentials	Este parâmetro ou propriedade administra a senha principal necessária para acessar uma instância LDAP. Ele deve ser protegido, já que nenhuma senha que controla a segurança e o acesso deve ser exposta em texto simples.
authentication_policy. LDAP_SECURITY_ TRUSTSTORE_PASSWORD	Este parâmetro ou propriedade controla a senha para o armazenamento confiável (formato JKS) usado para proteger as conexões LDAP. O passphrase para este JKS deve ser fornecido para que o armazenamento confiável possa ser acessado, já que é um arquivo criptografado.
authentication_policy. LDAP_SECURITY_KEYSTORE_PASSWORD	Esst parâmetro ou propriedade controla a senha se a autenticação SSL baseada no cliente for usada para proteger conexões para uma determinada instância LDAP.

Para criptografar senhas do LDAP:

Procedimento

1. Navegue até o diretório bin.
2. Use encrypt_string.[sh/cmd] para determinar o valor real da propriedade/parâmetro que deseja criptografar.
3. Atualize os parâmetros/propriedades no arquivo customer_overrides.properties para ter as entradas a seguir. Substitua todos os <ENCVAL> pelo valor criptografado da não sequência criptografada comentada para essa propriedade usando bin/encrypt_string.sh (ou .cmd). Por exemplo:

```
authentication_policy.LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/../
woodstock2/com/sterlingcommerce/woodstock/security/units/cacerts
# não criptografado
#authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# criptografado
authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=<ENCVAL>
authentication_policy.LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/../woodstock2/
com/sterlingcommerce/woodstock/security/units/keystore
# não criptografado
#authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=password
# criptografado
authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=<ENCVAL>
authentication_policy.authentication_2.display_name=LDAP Server agrona 2
authentication_policy.authentication_2.enabled=true
authentication_policy.authentication_2.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
authentication_policy.authentication_2.server=agrona.sci.local
authentication_policy.authentication_2.port=18100
authentication_policy.authentication_2.security_type=simple
authentication_policy.authentication_2.principle=cn=Manager,dc=amr,dc=stercomm,dc=com
# não criptografado
#authentication_policy.authentication_2.credentials=Sterling
# criptografado
authentication_policy.authentication_2.credentials=<ENCVAL>
authentication_policy.authentication_2.security_protocol=ssl
authentication_policy.authentication_2.password_attribute=userPassword
authentication_policy.authentication_2.search_root=dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_2.search_filter=(uid=<userid>)
authentication_policy.authentication_2.with_user_bind=false
authentication_policy.authentication_2.className=com.sterlingcommerce.woodstock.security
.LDAPAuthentication
```

Notícias do Usuário

Notícias do Usuário

O recurso Notícias do Usuário permite postar mensagens nas páginas Início do Console Administrativo. As notícias do usuário possibilitam informar os usuários sobre mudanças ou lembrá-los de eventos e tarefas importantes. Mensagens podem ser postadas:

- Para todos os usuários
- Para um usuário específico
- Para diversos usuário

O item de notícias é exibido com base em uma data efetiva e em uma data de expiração. Também é possível configurar a mensagem como:

Tipo de Mensagem	Símbolo	Descrição
Aviso		Fornece informações de anúncio gerais ou de baixa prioridade.
Alerta		Fornece informações de anúncio de alta prioridade.

Você deve ter permissões de gravação para Contas para criar mensagens de notícias do usuário. A exclusão de antigas mensagens reduz requisitos de armazenamento e a quantidade de esforço necessária para recuperar mensagens específicas.

As tarefas de notícias do usuário incluem:

- Criar uma Mensagem de Notícias do Usuário para Usuários Específicos
- Criar uma Mensagem de Notícias do Usuário para todos os Usuários
- Procurar uma Mensagem de Notícias do Usuário
- Editar uma Mensagem de Notícias do Usuário
- Excluir uma Mensagem de Notícias do Usuário

Criar Mensagens de Notícias do Usuário para Todos os Usuários

Sobre Esta Tarefa

Antes de iniciar, você precisa saber as seguintes informações:

Campo	Descrição
Tipo	Tipo de mensagem que você está criando. Os valores válidos são Aviso e Alerta.
Assunto	Assunto da mensagem que você está criando.
Mensagem	Corpo da mensagem que você está criando.

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Notícias do Usuário**.
2. Próximo de **Nova Mensagem**, clique em **Ir!**
3. Insira o **Tipo**.

4. Insira **Assunto**.
5. Insira **Mensagem**.
6. Clique em **Avançar**.
7. Selecione **TODOS Usuários** e clique em **Avançar**.
8. Insira **Data Efetiva** da mensagem (dd-mm-aaaa).
9. Insira **Data de Expiração** da mensagem (dd-mm-aaaa).
10. Clique em **Avançar**.
11. Revise Novas Configurações de Mensagem.
12. Clique em **Concluir**.

Criar Mensagens de Notícias do Usuário para Usuários Específicos

Sobre Esta Tarefa

Antes de iniciar, você precisa saber as seguintes informações:

Campo	Descrição
Tipo	Tipo de mensagem que você está criando. Os valores válidos são Aviso e Alerta.
Assunto	Assunto da mensagem que você está criando.
Mensagem	Corpo da mensagem que você está criando.

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Notícias do Usuário**.
2. Próximo de **Nova Mensagem**, clique em **Ir!**
3. Insira o **Tipo**.
4. Insira **Assunto**.
5. Insira **Mensagem**.
6. Clique em **Avançar**.
7. Selecione **Usuários Selecionados**.
8. Selecione o nome de cada usuário que você quer que receba essa mensagem.
9. Clique em **Avançar**.
10. Insira **Data Efetiva** da mensagem (dd-mm-aaaa).
11. Insira **Data de Expiração** da mensagem (dd-mm-aaaa).
12. Clique em **Avançar**.
13. Revise Novas Configurações de Mensagem.
14. Clique em **Concluir**.

Procurar Mensagens de Notícias do Usuário

Sobre Esta Tarefa

Para procurar uma mensagem de notícias do usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Notícias do Usuário**.
2. Use uma das opções Procurar a seguir:

Opções Procura de Notícias do Usuário	Ação
por ID do Usuário	Selecione TODOS ou o usuário específico da lista.
por Assunto	Insira uma parte do texto da mensagem.
por Intervalo de Data Efetiva	Insira o intervalo de data (dd/mm/aaaa).

3. Clique em **Vá!** A página Notícias do Usuário lista todas as mensagens que correspondem ao critério de procura.

Editar Mensagens de Notícias do Usuário

Sobre Esta Tarefa

Para editar uma mensagem de notícias do usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Notícias do Usuário**.
2. Procure a mensagem de notícias do usuário que deseja editar.
3. Clique em editar para a mensagem de notícias do usuário que deseja editar.
4. Atualize o tipo de mensagem, assunto ou mensagem, se necessário.
5. Clique em **Avançar**.
6. Atualize os usuários que receberão essa mensagem, se necessário, e clique em **Avançar**.
7. Atualize a **Data Efetiva** da mensagem (dd-mm-aaaa), se necessário.
8. Atualize a **Data de Expiração** da mensagem (dd-mm-aaaa), se necessário.
9. Clique em **Avançar**.
10. Revise Novas Configurações de Mensagem.
11. Clique em **Concluir**.

Excluir Mensagens de Notícias do Usuário

Sobre Esta Tarefa

Para excluir uma mensagem de notícias do usuário:

Procedimento

1. No **Menu de Administração**, selecione **Contas** > **Notícias do Usuário**.
2. Procure a mensagem de notícias do usuário que deseja excluir.
3. Clique em **Excluir** para a mensagem de notícias que deseja remover.
4. Revise Novas Configurações de Mensagem.
5. Clique em **Excluir**. A mensagem a seguir é exibida:

   ```
   A atualização do sistema foi concluída com sucesso.
   ```

Criptografia de Documento

Visão Geral do Recurso de Criptografia de Documento

A criptografia de documentos é um recurso fornecido com o Sterling B2B Integrator. Esse recurso permite a configuração de uma camada adicional de segurança além das permissões tradicionais de arquivo e banco de dados. Se você tiver integrado o Sterling File Gateway ao Sterling B2B Integrator, ele usará o

mesmo recurso de criptografia de documento para proteger dados inativos. O Sterling File Gateway é um aplicativo para transferência de arquivos segura entre parceiros que usam protocolos, convenções de nomenclatura de arquivo e formatos de arquivo diferentes.

O recurso de criptografia de documento é destinado à proteção de dados inativos contra espionagem. O recurso permite que você criptografe os dados de carga útil armazenados no banco de dados e/ou sistema de arquivos. Ele também é projetado para evitar que alguém de fora do sistema visualize os dados de carga útil acessando diretamente o banco de dados ou sistema de arquivos.

Aspectos importantes de criptografia de documento:

- A configuração padrão na instalação é sem criptografia. Se quiser que seus documentos sejam criptografados, você precisará ativar esse recurso.
- É possível ativar esse recurso a qualquer momento, mas somente documentos recebidos após a criptografia ser ativada serão criptografados.
- Quando você ativa esse recurso, a criptografia serve para todas as cargas úteis no sistema inteiro.
- Apenas os dados de carga útil de documento são criptografados, e **não** os metadados.
- A mesma chave de criptografia é usada para criptografar e decriptografar.
- O sistema usa um certificado predefinido (doccrypto) para criptografar documentos. É possível criar um certificado do sistema diferente. Se o fizer, você precisará atualizar o valor de CERT_NAME no arquivo customer_overrides.properties.

Apesar de o desempenho ser afetado quando a criptografia é ativada, cada cliente verá impactos de desempenho diferentes dependendo do hardware, do número e do tamanho dos documentos sendo processados e da quantidade relativa de tempo de processamento gasto por um determinado servidor fazendo persistência de documentos e recuperação com relação a outras atividades.

Chave de Criptografia para Criptografia de Documento

A mesma chave de criptografia é usada para criptografar e decriptografar documentos do banco de dados ou do sistema de arquivos. O certificado digital é usado para gerar e criptografar as chaves, e o passphrase do sistema é usado para criptografar os certificados digitais. A criptografia de documento cria uma chave por documento, e essa chave é armazenada junto com o documento como parte dos metadados. Os certificados digitais são armazenados como qualquer outro certificado do sistema.

O sistema usa um certificado predefinido (doccrypto) para gerar e criptografar as chaves que são usadas para criptografar os documentos. É possível criar um certificado do sistema diferente. Se o fizer, você precisará atualizar o valor de CERT_NAME no arquivo customer_overrides.properties.

Designar um Certificado Diferente para Criptografia de Documento

Sobre Esta Tarefa

O sistema usa um certificado predefinido (doccrypto) para criptografar documentos. É possível criar um certificado do sistema diferente a ser usado para

criptografar documentos, por exemplo, se o certificado anterior estiver expirando. Ao fazer isso, deve-se atualizar o valor do CERT_NAME no arquivo customer_overrides.properties.

CUIDADO: Não exclua ou renomeie o certificado do sistema anterior. O certificado anterior é necessário para decriptografar documentos que foram criptografados por ele anteriormente. O novo certificado do sistema não consegue decriptografar esses documentos, pois não foi usado para criptografá-los.

Antes de executar esse procedimento, você precisa:

- Gerar o novo certificado
- Saber o nome do certificado

Para atualizar o valor de CERT_NAME:

Procedimento

1. Navegue para o diretório de instalação.
2. Navegue para o diretório de propriedades.
3. Abra o arquivo customer_overrides.properties.
4. Inclua a seguinte linha no arquivo:
   `security.CERT_NAME=name_of_new_system_certificate`
5. Salve e feche o arquivo customer_overrides.properties.
6. Pare e reinicie o Sterling B2B Integrator.

Ativar Criptografia de Documento para Documentos do Sistema de Arquivos e do Banco de Dados

Sobre Esta Tarefa

Para criptografar documentos de um sistema de arquivos e de um banco de dados:

Procedimento

1. Navegue para o diretório de instalação.
2. Navegue para o diretório de propriedades.
3. Abra o arquivo customer_overrides.properties.
4. Inclua a seguinte linha no arquivo.
   `security.ENC_DECR_DOCS=ENC_ALL`
5. Salve e feche o arquivo customer_overrides.properties.
6. Pare e reinicie o Sterling B2B Integrator.

Ativar Criptografia de Documento para Documentos do Banco de Dados

Sobre Esta Tarefa

Para criptografar documentos do banco de dados:

Procedimento

1. Navegue para o diretório de instalação.
2. Navegue para o diretório de propriedades.
3. Abra o arquivo customer_overrides.properties.

4. Inclua a seguinte linha no arquivo.
   `security.ENC_DECR_DOCS=ENC_DB`
5. Salve e feche o arquivo customer_overrides.properties.
6. Pare e reinicie o Sterling B2B Integrator.

Ativar Criptografia de Documento para Documentos do Sistema de Arquivos

Sobre Esta Tarefa

Para criptografar documentos do sistema de arquivos:

Procedimento

1. Navegue para o diretório de instalação.
2. Navegue para o diretório de propriedades.
3. Abra o arquivo customer_overrides.properties.
4. Inclua a seguinte linha no arquivo.
   `security.ENC_DECR_DOCS=ENC_FS`
5. Salve e feche o arquivo customer_overrides.properties.
6. Pare e reinicie o Sterling B2B Integrator.

Desativar Criptografia de Documento para Documentos

Sobre Esta Tarefa

A configuração padrão na instalação é sem criptografia.

Para desativar a criptografia de documento:

Procedimento

1. Navegue para o diretório de instalação.
2. Navegue para o diretório de propriedades.
3. Abra o arquivo customer_overrides.properties.
4. Atualize o valor de ENC_DECR_DOCS para NONE. Por exemplo:
   `security.ENC_DECR_DOCS=NONE`
5. Salve e feche o arquivo customer_overrides.properties.
6. Pare e reinicie o Sterling B2B Integrator.

Certificados

Certificados Digitais

Use o Utilitário de gerenciamento de chave IBM (iKeyman) para ajudar a gerenciar seus certificados digitais.

O sistema usa os seguintes tipos de certificados digitais:

- Certificados de CA e confiável – Certificados digitais para os quais o sistema não tem chaves privadas. Esses certificados são armazenados em formato DER padrão.
- Certificados do sistema - Um certificado digital para o qual a chave privada é mantida no sistema. Esses certificados são armazenados com a chave privada em um formato seguro.

A seguir há algumas informações básicas sobre como certificados digitais são usados:

- Cada organização trocando documentos seguros deve ter um certificado. Use o iKeyman para gerar o certificado ou ele pode ser gerado externamente. Para obter informações sobre o iKeyman, consulte o "Utilitário de gerenciamento de chave IBM (iKeyman)" na página 60.
- Cada perfil comercial para um parceiro comercial com quem você troca documentos assinados e criptografados deve ter um certificado.
- Uma organização ou perfil comercial pode ter apenas um certificado ativo por vez. No caso de certificados duais, uma organização pode ter um par de certificados ativo; uma para assinatura, um para criptografia.
- Um organização ou perfil comercial deve ter um certificado ativo para trocar com êxito documentos assinados e criptografados.
- Uma organização ou perfil comercial pode ter diversos certificados válidos.
- Certificados podem ser usados para assinar documentos que você transmite por todos os métodos de transporte.
- O comprimento da chave para um certificado não tem que ser igual ao do certificado do parceiro comercial.
- Antes de configurar o período de validade do certificado, é recomendável ler e aplicar as recomendações de melhor prática do Microsoft PKI Quick Guide. Para obter informações sobre as recomendações de boas práticas para usar certificados, consulte http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html.

Certificados Digitais Suportados

Sterling B2B Integrator suporta a versão 3 X.509 de certificados digitais. Certificados digitais podem ser autoassinados ou assinados por CA:

- Um certificado autoassinado é um certificado digital assinado com a chave privada que corresponde à chave pública no certificado, demonstrando que o emissor tem a chave privada que corresponde à chave pública no certificado.
- Um certificado assinado por CA é um certificado digital que é assinado com o uso de chaves mantidas por autoridades de certificação. Antes de emitir um certificado, a CA normalmente avalia o solicitante de um certificado para determinar se o solicitante é, de fato, o portador do certificado referido no certificado.

Certificados CA

Um certificado de CA é um certificado digital emitido por uma autoridade de certificação (CA). A CA verifica certificados confiáveis para raízes confiáveis. Raízes confiáveis são a base sobre a qual cadeias de confiança são construídas em certificados. Confiar em uma raiz de CA significa confiar em todos os certificados emitidos por essa CA. Se você não quiser confiar em uma raiz de CA, o Sterling B2B Integrator não confiará em nenhum certificado emitido por essa CA.

Certificados de CA contêm uma chave pública correspondente a uma chave privada. A CA possui a chave privada e a usa para assinar os certificados que emite. Para validar um certificado confiável, primeiro você deve efetuar o registro de entrada em um certificado de CA.

Certificados raiz de CAs comuns estão contidos em um keystore Java (JKS) na JVM fornecida com o Sterling B2B Integrator. Isso permite que os usuários estabeleçam alguns relacionamentos de confiança baseados em autoridade mais facilmente do que se tivessem que procurar e obter certificados do web site da CA.

Certificados de CA são armazenados separadamente dos certificados confiáveis no produto.

Na interface com o usuário, é possível efetuar o registro de entrada dos certificados raiz de CA que se originam de qualquer uma das seguintes origens:

- Certificados raiz de CA comuns fornecidos com o Sterling B2B Integrator no keystore JKS.
- Apenas certificados e certificados confiáveis são reconhecidos. Certificados e chaves privadas não ficam visíveis na UI.
- Certificados SSL importados de parceiros comerciais.
- Outros certificados obtidos externamente.

Com base nas políticas de segurança em seu site, os certificados de CA no keystore JKS também podem ser registrados por meio do console. Embora certificados de CA sejam documentos públicos, você deve ter cuidado sobre quem tem direitos de incluí-los. Uma pessoa mal intencionada poderia incluir um certificado de CA falso para verificar certificados de usuário final falsos.

Nomes de Certificados de CA

O nome do certificado de CA não faz parte do conteúdo do certificado. Geralmente eles são integrados ao Nome Distinto Relativo (RDN) e ao número de série do certificado. No entanto, certificados do keystore JKS são nomeados com uma sequência arbitrária.

Como o nome do certificado é armazenado no banco de dados do sistema e é usado como o alias para referir-se ao certificado na GUI, você pode desejar renomear certificados com nomes mais curtos ou mais significativos com base nas convenções de nomenclatura de arquivo. Certificados podem ser renomeados quando registrados ou editados.

Benefícios de Certificados Digitais Autoassinados e Assinados por CA

Quando você e seus parceiros comerciais estiverem decidindo se devem gerar um certificado autoassinado ou adquirir um certificado assinado de uma CA, considere o seguinte:

- É possível criar facilmente certificados autoassinados usando Sterling B2B Integrator. No entanto, esses certificados autoassinados não são verificados por um terceiro confiável.
- A principal vantagem de usar os certificados de uma CA é que a identidade do portador do certificado é verificada por um terceiro confiável. As desvantagens incluem custo extra e esforço administrativo. Se você decidir usar um certificado de terceiros, obtenha-o de uma CA.
- Uma CA fornece uma origem centralizada para postar e obter informações sobre certificados, incluindo informações sobre certificados revogados.

Por padrão, o sistema confia em todos os certificados de CA e certificados autoassinados gerados pelo aplicativo. No entanto, é possível especificar se todos ou alguns dos certificados emitidos por uma CA específica deve ser confiável. Também é possível não confiar explicitamente em um certificado autoassinado de um parceiro comercial.

Datas de Expiração para Certificados

Se um adaptador e um servlet forem usados para comunicações de entrada (por exemplo, o recebimento de dados AS2 de parceiros comerciais), você deverá monitorar as datas de expiração dos certificados do sistema para assegurar que os certificados sejam válidos. Antes de os certificados expirarem, eles devem ser substituídos por certificados válidos.

Definições de Parâmetro do Certificado do Sistema

Se um adaptador e um servlet forem usados para comunicações de entrada (por exemplo, o recebimento de dados AS2 de parceiros comerciais), você deverá monitorar as datas de expiração dos certificados do sistema para assegurar que os certificados sejam válidos. Antes de os certificados expirarem, eles devem ser substituídos por certificados válidos.

Parâmetro	Descrição
alias	O nome da chave armazenado no HSM. Use apenas nomes de alias contendo caracteres a-z, A-Z, 0-9 ou hífen (-) e cujo comprimento total não excede o comprimento do GUID do sistema.
certname	Nome para designar ao certificado do sistema no banco de dados.
Certtype	O tipo de certificado para importar. Quatro tipos de arquivos de certificado são suportados: pkcs12, pkcs8, pem e keystore. O Sterling B2B Integrator suporta apenas chaves pem criptografadas com DES ou 3DES. Use keystore para listar ou importar keystore.
arquivo	Nome do arquivo para importar.
keypass	PIN para o slot no dispositivo Eracom.
keystoretype	Tipo de keystore para importar. O valor válido é CRYPTOKI.
keystoreprovider	Tipo de provedor. Eracom é o único tipo de provedor suportado por HSM. Os valores válidos são: • ERACOM • ERACOM.n (se você estiver importando certificados em um slot diferente da primeira posição)
password	Passphrase de armazenamento para o arquivo de certificado.
pkcs12file	Nome do arquivo PKCS12 para importar.
pkcs12storepass	Passphrase de armazenamento usado para a geração do arquivo PKCS12.
pkcs12keypass	Passphrase válido para o arquivo PKCS12.
storepass	PIN para o slot no dispositivo Eracom onde o keystore reside.
systempass	Passphrase do sistema.

Utilitário de gerenciamento de chave IBM (iKeyman)

O Utilitário de gerenciamento de chave IBM (iKeyman) é um componente do IBM SDK que gera chaves, solicitações de certificação e certificados autoassinados.

É possível usar o iKeyman para criar certificados a fim de proteger comunicações, criptografar e decriptografar dados. Em uma transferência segura usando o SSL, os certificados fornecem um nível de segurança incluído.

No Sterling B2B Integrator, é possível usar o iKeyman para criar:

- Certificate Signing Requests (CSRs) – Um arquivo para ser enviado por email para uma autoridade de certificação para solicitar um certificado X.509.
- Certificados-chave – uma combinação de um certificado codificado por ASCII e uma chave privada criptografada PKCS12 codificada por ASCII. Se você gerar certificados-chave usando o formato padrão com determinadas cifras, o certificado de saída apresentará um erro quando importado para o Sterling B2B Integrator. PKCS12 é o formato recomendado para os certificados-chave.

Para obter mais informações sobre como configurar e usar o iKeyman, consulte iKeyman Overview for IBM SDK, Java Technology Edition 7.0.0

Tarefas de Certificado

Criar um Certificado Autoassinado

Sobre Esta Tarefa

Para criar um certificado autoassinado:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Próximo de **Criar Certificado Autoassinado**, clique em **Ir!**
3. Insira o **Nome** do certificado autoassinado.
4. Insira o nome da **Organização** de origem.
5. Selecione o **País** ou a origem do certificado autoassinado.
6. Insira um endereço de **email** do contato para a pessoa responsável pelos certificados na organização e clique em **Avançar**.
7. Insira o **Número de Série** para o certificado. O número de série é aquele que você quer designar ao certificado autoassinado.
8. Insira o número de dias (**Duração**) durante os quais o certificado autoassinado será válido.

   Nota: Na V5.2.6.2 ou posterior, a data de expiração máxima é *Jan 1, 2080*. Qualquer período inserido, que poderá resultar em uma data de expiração posterior a Jan 1, 2080, será padronizada para *Jan 1, 2080*. Em liberações anteriores, não há limite máximo.
9. Insira os **Endereços IP** das interfaces de rede que deseja associar ao certificado como o campo SubjectAltName.
10. Insira os **Nomes DNS** das interfaces de rede que deseja associar ao certificado como o campo SubjectAltName.
11. Selecione o **Comprimento da Chave**. Selecione um dos comprimentos de chave a seguir:
    - 512
    - 1024
    - 2048

Nota: O comprimento de chave 1024 fornece um bom equilíbrio entre segurança, interoperabilidade e eficiência. O comprimento de chave 2048 é o mais seguro, mas também o mais lento, e pode não funcionar em alguns aplicativos.

Nota: Se selecionar o comprimento da chave 512, deve-se também usar o JDK 7 SR5. O JDK 7 SR7 FP1 não suporta comprimentos da chave abaixo de 1024.

12. Selecione o **Algoritmo de Assinatura**.
13. Selecione a opção **Validar Quando Usado**. As opções de validação são:
    - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
    - Cadeia de Autenticação – Constrói uma cadeia de confiança para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
14. Configure **Bit de Assinatura de Certificado** selecionando a caixa de opção.
15. Clique em **Avançar**.
16. Revise as informações sobre o certificado certificado autoassinado.
17. Clique em **Concluir**.

Obter Certificado Confiável Automaticamente dos Parceiros Comerciais

Sobre Esta Tarefa

O Utilitário de Captura de Certificado automatiza o processo de obtenção de um certificado SSL de um parceiro comercial. Este método de obtenção de informações de certificado permite que um parceiro se conecte e salve facilmente um certificado. Se for desejado, uma verificação de segurança fora da banda pode ser feita antes de o certificado ser verificado no sistema como um certificado de CA ou Confiável.

Antes de iniciar:

- Verifique se o sistema host do parceiro é ativado por SSL.
- Obtenha informações da porta e do host para o servidor do parceiro comercial.
- Se o modo FTPS for usado, determine se o modo será explícito ou implícito.
- Configure a instância do serviço SSLCertGrabberAdapter padrão para usar o servidor de perímetro apropriado e servidor proxy (apenas HTTPS). Consulte a documentação do adaptador para obter detalhes.

Para obter o certificado SSL automaticamente de um parceiro comercial:

Procedimento

1. No **Menu de Administração**, selecione **Parceiro Comercial > Certificados Digitais > Utilitário de Captura de Certificado**.
2. Próximo de **Capturar Certificado de Parceiro**, clique em **Ir!**
3. Selecione o tipo de conexão para o servidor e clique em **Avançar**.
    - FTPS
    - HTTPS
4. Insira o **Nome do Host** ou **Endereço IP**.

5. Insira o número da **Porta**.
6. Selecione o modo de conexão para FTPS (se estiver usando HTTPS, ignore esta etapa):
   - Explícito - a negociação do SSL ocorre após a conexão de FTP ser estabelecida. Padrão.
   - Implícito - a negociação do SSL ocorre antes de a conexão FTP ser estabelecida.
7. Clique em **Avançar**. O sistema tenta se conectar e recuperar certificados.
8. Após a captura ser concluída, revise as informações de resumo e decida quais certificados deseja salvar.
9. Selecione um método de codificação para cada certificado e clique em **Salvar**. Os formatos de codificação são:
   - BASE64 – Usa codificação BASE64 no certificado DER padrão. Padrão.
   - DER – Formato padrão para certificados digitais aceito pela maioria dos aplicativos.
10. Clique em **Salvar** e navegue para o local onde deseja salvar o arquivo.
11. Aceite o nome do arquivo padrão ou edite-o de acordo com as convenções de nomenclatura de arquivo e clique em **Salvar**.
12. Após o salvamento, os certificados podem ser registrados no sistema. Se você decidir registrar um certificado no sistema:
    a. Verifique se cada certificado é válido e confiável.
    b. Registre o certificado como um certificado de CA ou Confiável, dependendo da função. Para confiança baseada em Autoridade de Certificação, você pode precisar efetuar o registro de entrada da cadeia de certificados, excluindo o certificado do usuário final. Para confiança direta, efetue o registro de entrada do certificado do usuário final.

Configurar Informações de Status em Resumos de Certificado

Sobre Esta Tarefa

Por padrão, as informações de status do certificado são fornecidas no final da janela pop-up de resumo quando um nome de certificado com hyperlink for selecionado. Você tem a opção de incluir ou excluir as informações de status. Como as informações de status são compiladas em tempo real, talvez você não queira incluí-las.

A propriedade VerificationOnPopupInfo controla se informações de status são exibidas no resumo do certificado. Essa propriedade está no arquivo ui.properties. Os valores para a propriedade VerificationOnPopupInfo são:

- true - incluir informações de validação (padrão)
- false - não compilar ou exibir informações de validação na janela pop-up
- (qualquer outro valor) - incluir informações de validação

Para evitar a compilação e a exibição das informações de status:

Procedimento

1. Abra o arquivo ui.properties.
2. Atualize o valor de VerificationOnPopupInfo para false. Exemplo:
   ```
   VerificationOnPopupInfo=false
   ```
3. Salve e feche o arquivo.
4. Reinicie o Sterling B2B Integrator.

Configurar Exibições de Impressão Digital

Sobre Esta Tarefa

Além do hash SHA1 pré-calculado, impressões digitais de certificados adicionais podem ser incluídas nas telas de exibição do certificado, de confirmação e de resumo. Cálculos de hash são feitos sob demanda quando uma exibição é gerada.

Impressões digitais adicionais são exibidas em telas de GUI, mas não têm efeito sobre a manipulação de mensagens ou comunicação do sistema.

Para configurar o sistema para calcular e exibir impressões digitais de certificados adicionais:

Procedimento

1. No arquivo ui.properties, modifique esta linha:

   ```
   AddtlCertThumbprintAlgs=hash_algorithm
   ```

   Para exibir mais de um hash adicional, separe os valores com vírgulas. Exemplo:

   ```
   AddtlCertThumbprintAlgs=SHA384,SHA512
   ```

Parâmetro	Descrição
hash_algorithm	Nome de um algoritmo de hash a ser aplicado à impressão digital do certificado. Os valores válidos são: • SHA-256 • SHA-384 • SHA-512

2. Salve e feche o arquivo ui.properties.
3. Reinicie o Sterling B2B Integrator.

Procurar Certificados de CA

Sobre Esta Tarefa

Para procurar um certificado de CA:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial > Certificados Digitais > CA**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Conclua uma das ações a seguir e clique em **Ir!**
   - Em Procurar no campo **Por Nome de Certificado**, insira uma parte do nome ou o nome inteiro do certificado de CA que você está procurando. A página Certificados Digitais de CA lista todos os certificados de CA que correspondem ao seu critério de procura.
   - Em Listar no campo **Em Ordem Alfabética**, selecione **TODOS** ou a letra com a qual começa o nome do certificado de CA que você está procurando. A seleção de TODOS lista todos os certificados de CA. A página Certificados Digitais de CA lista todos os certificados de CA que correspondem ao seu critério de procura.

Visualizar Informações Resumo do Certificado de CA

Sobre Esta Tarefa

Quando uma lista de certificados é exibida, é possível clicar no nome do certificado para visualizar informações de resumo sobre esse certificado. Os campos a seguir são configuráveis no sistema.

Campo Resumo do Certificado	Descrição
Nome do Sistema	O Nome do Certificado é o rótulo do banco de dados. Ele é usado para referir-se a esse certificado na GUI e armazena esse nome em seu banco de dados. O nome padrão para um certificado do keystore JKS é uma sequência arbitrária. Os nomes de outros certificados são construídos a partir do nome distinto relativo (RDN) do emissor e o número de série do certificado. É possível alterar um nome de certificado para um nome mais curto ou mais reconhecível durante o registro ou a edição do certificado.
Impressão Digital	Informações para o hash SHA1 são incluídas por padrão. Para configurar o cálculo e a exibição de informações de impressão digital, edite o arquivo ui.properties.
Status	Uma verificação em tempo real do status atual, indicando se as datas do certificado são válidas e se o certificado foi verificado. Para configurar se essas informações são ou não calculadas no momento da exibição, edite o arquivo ui.properties.

Embora essas informações se apliquem às informações de resumo para um certificado de CA, campos semelhantes aparecem nas telas de resumo e confirmação para outros tipos de certificados.

Registro de Entrada de Certificados de CA da Interface com o Usuário

Sobre Esta Tarefa

Com base nas políticas de segurança em seu site, os certificados de CA no keystore JKS também podem ser registrados por meio do console.

Antes de começar, salve quaisquer certificados de CA que você tenha obtido externamente em um arquivo local.

Para efetuar o registro de entrada em um certificado de CA:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial > Certificados Digitais > CA**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Próximo de **Efetuar o Registro de Entrada do Novo Certificado**, clique em **Ir!**
3. Selecione um método para importar certificados:

Método de importação	Próximas etapas
Importar da JVM – Importa do keystore JKS	1. Clique em **Importar** em **JVM**. 2. Aceite a senha padrão que aparece no campo de senha e clique em **Avançar**. A senha do keystore padrão é fornecida pela Sun Microsystems. Se o campo de senha estiver vazio, o sistema ainda usará a senha padrão.
Importar do Arquivo – Importa certificados salvos como um arquivo em uma unidade local	1. Clique em **Importar** do **Arquivo**. 2. Insira o Nome do Arquivo ou clique em **Navegar** para selecionar um arquivo de certificado de CA. Clique em Avançar. Você pode ignorar a senha que aparece no campo de senha. Não é necessário apagar a entrada.

Os certificados disponíveis são listados com um resumo das informações de identificação. Todos os certificados são selecionados por padrão.

4. Clique nas caixas de seleção à esquerda de cada entrada para selecionar ou cancele a seleção dos certificados para importar.
5. Para cada certificado selecionado, aceite o Nome do Certificado sugerido ou edite-o com base nas convenções de nomenclatura de arquivo.
6. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:
   - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
   - Cadeia de Autenticação – Tenta construir uma cadeia de confiança até a raiz para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
7. Se você receber uma mensagem declarando que o certificado duplica um certificado que já está no banco de dados, insira S ou N para indicar se deseja importar a duplicata.

   Essa verificação é feita apenas em certificados únicos. Ela não acontece durante o registro de entrada de um ou mais certificados de um arquivo.

   Certificados são identificados por um hash SHA1 com o propósito de determinar duplicatas. Mais de uma cópia de um certificado pode estar presente no banco de dados, desde que cada uma preencha uma linha diferente e tenha um ID de objeto distinto. O certificado existente não é sobrescrito.
8. Revise as informações de certificado de CA.
9. Clique em **Concluir**.

Registro de Entrada de Certificados de CA do Console

Sobre Esta Tarefa

Certificados de CA comuns estão contidos em um keystore JKS que faz parte da JVM fornecida com o Sterling B2B Integrator. O keystore JKS está localizado em /install_dir/jdk/jre/lib/security/cacerts. Você também pode obter certificados externamente.

Para importar certificados no repositório confiável do Sterling B2B Integrator, modifique o comando em /install_dir/install/bin/ImportCACerts.sh (UNIX) ou \install_dir\install\bin\ImportCACerts.cmd (Windows).

Antes de iniciar, salve quaisquer certificados de CA obtidos externamente em um arquivo local.

Para efetuar o registro de entrada de um certificado de CA no console:

Procedimento

1. Navegue até o diretório de instalação.
2. Navegue até o diretório bin.
3. Insira este comando:

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   Todos os certificados no arquivo são listados, um por vez, com estas exceções:
   - Entradas contendo chaves privadas ou simétricas não são processadas ou listadas.
   - Apenas o primeiro certificado em um arquivo em formato DER é processado e listado.
4. Após os prompts, insira S (sem distinção entre maiúsculas e minúsculas) para qualquer certificado que você deseja importar.
5. Para cada certificado aceito, aceite o Nome do Certificado sugerido ou edite-o com base nas convenções de nomenclatura de arquivo.
6. Se o rótulo do certificado duplicar um rótulo que já está no banco de dados, insira `S` ou `N` (sem distinção entre maiúsculas e minúsculas) para indicar se você deseja alterar o rótulo. Embora geralmente os certificados não sejam identificados por um rótulo e o banco de dados permita duplicatas de rótulo, alguns serviços procuram certificados por rótulo. Evite rótulos duplicados para evitar a possibilidade de comportamento inesperado.
7. Se o certificado duplicar um certificado que já está no banco de dados (conforme indicado pelo hash SHA1 do certificado), especifique com S ou N se deseja importar a duplicata.

   Certificados são identificados por um hash SHA1 com o propósito de determinar duplicatas. Mais de uma cópia de um certificado pode estar presente no banco de dados, desde que cada uma preencha uma linha diferente e tenha um ID de objeto distinto. O certificado existente não é sobrescrito.

Editar Certificados de CA

Sobre Esta Tarefa

Para editar um certificado de CA:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial > Certificados Digitais > CA**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Usando Procurar ou Listar, localize o certificado de CA que deseja editar e clique em **Ir!**
3. Próximo do **Certificado de CA** que deseja editar, clique em **Editar**.

4. Insira o Nome do Certificado.
5. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:
   - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
   - Cadeia de Autenticação – Constrói uma cadeia de confiança para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
6. Revise as informações de certificado de CA.
7. Clique em **Concluir**.

Excluir Certificados de CA

Sobre Esta Tarefa

Para excluir um certificado de CA:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial > Certificados Digitais > CA**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Próximo de **Alfabeticamente**, clique em **Ir!**
3. Próximo do certificado de CA que deseja excluir, clique em **Excluir**.

Procurar Certificados do Sistema

Sobre Esta Tarefa

Para procurar um certificado do sistema:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Nos certificados do sistema, conclua uma das ações a seguir e clique em **Ir!**
   - Em Procurar no campo **Por Nome de Certificado**, insira uma parte do nome ou o nome inteiro do certificado do sistema que você está procurando. A página Certificados do Sistema lista todos os certificados do sistema que contêm o nome completo ou parcial digitado.
   - Em **Listar** no campo **Em Ordem Alfabética**, selecione **TODOS** ou a letra com a qual começa o nome do certificado de CA que você está procurando. A seleção de TODOS lista todos os certificados do sistema. A página Certificados do Sistema lista todos os certificados do sistema que correspondem aos critérios de procura.

Editar Certificados do Sistema

Sobre Esta Tarefa

Para editar um certificado do sistema:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Usando ou Procurar ou Listar, localize o **Certificado do Sistema** que deseja editar e clique em **Ir!**
3. Próximo do certificado do sistema que deseja editar, clique em **Editar**.
4. Insira o **Nome do Certificado**.
5. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:
   - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
   - Cadeia de Autenticação – Constrói uma cadeia de confiança para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
6. Revise as informações do certificado do sistema.
7. Clique em **Concluir**.

Identificar Certificados do Sistema no Sterling B2B Integrator

Sobre Esta Tarefa

Para identificar um certificado do sistema:

Procedimento

1. No **Menu de Administração**, selecione **Implementação > Serviços > Configuração**.
2. Na seção Listar, selecione o tipo aplicável de serviço ou adaptador da lista **Por Tipo de Serviço** e clique em **Ir!**
3. Na lista de configurações, escolha a configuração.
4. Clique no **Nome do Serviço** para visualizar informações de configuração.
5. Revise informações de resumo do certificado.

Verificar Data de Expiração de um Certificado do Sistema

Sobre Esta Tarefa

Se um adaptador e um servlet forem usados para comunicações de entrada (por exemplo, o recebimento de dados AS2 de parceiros comerciais), você deverá monitorar as datas de expiração dos certificados do sistema para assegurar que os certificados sejam válidos.

Para verificar a data de expiração de um certificado do sistema:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Para visualizar todos os certificados do sistema, selecione **Todos** na lista suspensa Alfabético e clique em **Ir!**
3. Selecione o nome do certificado do sistema que deseja visualizar. O Resumo do Certificado é exibido.
4. Na seção **Descrição** do Resumo do Certificado, revise as informações fornecidas no campo **Datas Válidas**.
5. Revise as informações fornecidas na seção **Status** para saber se as datas são válidas e se o certificado foi verificado.

Exportar Certificados do Sistema no Sterling B2B Integrator

Sobre Esta Tarefa

Este comando de exportação é aplicável apenas aos certificados do sistema Sterling B2B Integrator. Não é possível usar esse comando para exportar certificados do sistema no HSM.

Para exportar um certificado do sistema, digite o seguinte comando com os parâmetros apropriados:

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

Parâmetro	Descrição
keyname	Nome da chave do sistema para exportação.
pkcs12filename	Nome do arquivo que contém informações exportadas.
pkcs12storepass	Senha de armazenamento que protege o armazenamento.
pkcs12keypass	Senha da chave que protege a chave.

Excluir Certificados de Sistema no Sterling B2B Integrator

Sobre Esta Tarefa

Você deve exportar uma cópia do certificado do sistema para seu disco local antes de excluí-lo. OpsDrv, OpsKey e UIKeys são certificados do sistema que não podem ser excluídos.

Para excluir um certificado do sistema:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração do AS2**, selecione **Certificados**.
2. Próximo de **Alfabeticamente**, clique em **Ir!**
3. Próximo do certificado do sistema que deseja excluir, clique em **Excluir**.
4. Clique em **Excluir** na página Confirmar.

Registro de Saída de Certificados do Sistema
Sobre Esta Tarefa

Para exportar um certificado do sistema, você deve efetuar o registro de saída do certificado. O procedimento a seguir exporta apenas o certificado público, não a chave privada, e fornece a você um certificado público para enviar para um parceiro comercial.

Para efetuar o registro de saída de um certificado do sistema:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Usando Procurar ou Listar, localize o certificado do sistema do qual deseja efetuar o registro de saída.
3. Próximo do certificado do sistema do qual deseja efetuar o registro de saída, clique em **Efetuar o Registro de Saída**.
4. Na caixa de diálogo **Registro de Saída do Certificado do Sistema**, selecione o formato do certificado e, em seguida, clique em **Ir!**:
   - PKCS12 - Esta opção formata o certificado digital como um arquivo PKCS12. Você também tem a opção de inserir uma Senha de Chave Privada e Senha de Armazenamento de Chaves.
   - BASE64 - Esta opção usa codificação BASE64 no certificado DER padrão.
   - DER - Este formato padrão para certificados digitais é aceito pela maioria dos aplicativos.
5. Na caixa de diálogo **Download de Arquivo**, clique em **Salvar**.
6. Na caixa de diálogo **Salvar Como**, selecione o local onde deseja salvar o certificado e, em seguida, clique em **Salvar**. A opção para abrir o certificado não é suportada. Você deve abrir o certificado dentro do sistema operacional. Se você receber a mensagem de erro, Este é um arquivo de Certificado de Segurança inválido, abra o arquivo em um editor de texto e exclua quaisquer linhas em branco antes de -----BEGIN CERTIFICATE-----. Salve o arquivo editado e tente abrir o arquivo.
7. Clique em **Fechar** na caixa de diálogo Registro de Saída do Certificado do Sistema. A página Certificado do Sistema é exibida.

Procurar Certificados Confiáveis
Sobre Esta Tarefa

Para procurar um certificado confiável:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Confiáveis**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Na página Certificados Digitais Confiáveis, conclua uma das ações a seguir e, em seguida, clique em **Ir!**:

- Em Procurar no campo **Por Nome de Certificado**, insira uma parte do nome ou o nome inteiro do certificado confiável que você está procurando. A página Certificados Digitais Confiáveis lista todos os certificados confiáveis que correspondem ao seu critério de procura.
- No campo **Listar em Ordem Alfabética**, selecione **TODOS** ou a letra com a qual começa o nome do certificado confiável que você está procurando. A página Certificados Digitais Confiáveis lista todos os certificados confiáveis que correspondem ao seu critério de procura.

Registro de Entrada de Certificados do Sistema Confiáveis

Sobre Esta Tarefa

Certificados confiáveis podem se originar das seguintes origens:

- Certificados SSL importados dos parceiros comerciais
- Outros certificados obtidos externamente

Antes de começar, salve o certificado do sistema confiável em um arquivo em seu computador local.

Para efetuar o registro de entrada de um certificado do sistema confiável:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Confiáveis**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Próximo de **Efetuar o Registro de Entrada do Novo Certificado**, clique em **Ir!**
3. Insira o **Nome do Arquivo** ou clique em **Navegar** para selecionar o nome do arquivo do certificado confiável e clique em **Avançar**.
4. Insira o **Nome do Certificado**.
5. Verifique o nome do certificado confiável do qual está efetuando o registro de entrada. Para cada certificado selecionado, o campo Nome do Certificado mostra um nome sugerido, seguido por um resumo das informações de identificação no certificado. É possível alterar o nome com base nas convenções de nomenclatura do arquivo.
6. Se você tiver mais de um certificado confiável contido no arquivo selecionado, marque a caixa de seleção à esquerda de cada certificado para efetuar o registro de entrada de cada certificado.
7. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:
   - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
   - Cadeia de Autenticação – Tenta construir uma cadeia de confiança até a raiz para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
   - Cache de CRL - Controla se o Cache de CRL é consultado cada vez que o certificado do sistema é usado.
8. Revise as informações de certificado confiável.

9. Clique em **Concluir**.

Editar Certificados Confiáveis
Sobre Esta Tarefa

Para editar um certificado confiável:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Confiáveis**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Usando Procurar ou Listar, localize o certificado confiável que deseja editar e clique em **Ir!**
3. Clique em **Editar** próximo do certificado confiável que deseja editar.
4. Insira o **Nome do Certificado**.
5. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:
   - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
   - Cadeia de Autenticação – Tenta construir uma cadeia de confiança até a raiz para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
   - Cache de CRL - Controla se o Cache de CRL é consultado cada vez que o certificado do sistema é usado.
6. Revise as informações de certificado.
7. Clique em **Concluir**.

Excluir Certificados do Sistema Confiáveis
Sobre Esta Tarefa

Para excluir um certificado do sistema confiável:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Confiáveis**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Próximo de **Alfabeticamente**, clique em **Ir!**
3. Próximo do certificado confiável que deseja excluir, clique em **Excluir**.

Importar Certificados do Sistema PKCS12
Sobre Esta Tarefa

Para importar um certificado do sistema PKCS12:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira:

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

Registro de Entrada de Certificados do Sistema PKCS12

Sobre Esta Tarefa

Antes de iniciar, você precisa salvar o certificado do sistema PKCS12 em um arquivo em seu computador local.

Para efetuar o registro de entrada em um certificado do sistema PKCS12:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Na página Certificados do Sistema, em Efetuar o Registro de Entrada, próximo de **Certificado PKCS12**, clique em **Ir!**
3. Insira o **Nome do Certificado** PKCS12.
4. Insira a **Senha da Chave Privada**. Essa é a senha usada para criptografar o certificado PKCS12.
5. Insira a **Senha do Armazenamento de Chaves**. É a senha para o objeto PKCS12. Pode ser a mesma que a senha da chave privada.
6. Insira **Nome do Arquivo** ou clique em **Navegar** para selecionar o nome do arquivo do certificado PKCS12 e clique em **Avançar**.
7. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:
   - Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
   - Cadeia de Autenticação – Constrói uma cadeia de confiança para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.
8. Revise as informações do certificado do sistema PKCS12.
9. Clique em **Concluir**.

Importar Certificados do Sistema Pem

Sobre Esta Tarefa

Apenas chaves pem criptografadas com DES ou 3DES são suportadas.

Para importar um certificado do sistema pem:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira:

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

Importar Certificados do Sistema de Chaves

Sobre Esta Tarefa

Para importar um certificado do sistema de chaves:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira:

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

Importar Certificados do Sistema de Keystore

Sobre Esta Tarefa

Para gerar um certificado do sistema de keystore em um HSM:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira:

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

Registro de Entrada de Certificados do Sistema de Chave

Sobre Esta Tarefa

Antes de começar, salve o certificado do sistema de chave em um arquivo no computador local.

Para efetuar o registro de entrada em um certificado do sistema de chave:

Procedimento

1. Escolha uma das opções a seguir:
   - Se você usar o Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiro Comercial >Certificados Digitais>Sistema**.
   - Se você usar o AS2 Edition, no menu **Administração de AS2**, selecione **Certificados**.
2. Próximo de **Certificado de Chave**, clique em **Ir!**
3. Insira o **Nome do Certificado**.
4. Insira a **Senha da Chave Privada**. Esta é a senha usada para criptografar a chave privada.
5. Insira o **Nome do Arquivo** ou clique em **Navegar** para selecionar o nome do arquivo do certificado de chave e clique em **Avançar**.
6. Selecione a opção **Validar Quando Usado** e clique em **Avançar**. As opções de validação são:

- Validade – Verifica se as datas no período de validade do certificado ainda estão em vigor. Se as datas não estiverem em vigor, o certificado não é usado.
- Cadeia de Autenticação – Constrói uma cadeia de confiança para os certificados que não são autoassinados. Se uma cadeia de confiança não pode ser construída usando certificados válidos, o certificado não é usado. Se o certificado é autoassinado, esta opção verifica apenas a assinatura do certificado.

7. Revise as informações de certificado de chave.
8. Clique em **Concluir**.

Online Certificate Status Protocol (OCSP)

Suporte do Online Certificate Status Protocol (OCSP) no Sterling B2B Integrator

O Online Certificate Status Protocol (OCSP) é um conjunto de estruturas de dados definidas ASN.1 para solicitação e recebimento de informações sobre status de revogação de certificado. Essas estruturas de dados podem ser enviadas e recebidas por muitos protocolos de transporte em princípio. Na prática, o HTTP é usado.

Um cliente do OCSP envia perguntas e processa respostas. Um respondente do OCSP responde às perguntas e gera respostas.

Funcionalidade do Cliente do OCSP

Uma implementação do cliente do OCSP consiste em:

- Estruturas de dados para gerenciar informações sobre respondentes do OCSP
- Funcionalidade para gerar solicitações do OCSP
- Funcionalidade para processar respostas do OCSP
- Funcionalidade para transmitir solicitações do OCSP e receber respostas do OCSP

Como o Sterling B2B Integrator Executa uma Verificação do OCSP

Sobre Esta Tarefa

Uma verificação do OCSP para um certificado no Sterling B2B Integrator é determinada quando a verificação do OCSP dentro do Sterling B2B Integrator é implementada como parte de APIs do sistema interno usado por serviços para obter certificados e chaves do banco de dados. Verificações do OCSP são desempenhadas pelo Sterling B2B Integrator quando métodos são chamados para obter certificados e chaves dos objetos que as contêm no banco de dados.

As etapas a seguir descrevem como a verificação do OSCSP é implementada no Sterling B2B Integrator:

Procedimento

1. O sistema examina o objeto que contém o certificado para determinar se a verificação do OCSP está ativada. Isso permite que o sistema decida, sem chamadas de banco de dados adicionais, se deve tentar uma verificação do OCSP.
2. Se verificação do OCSP estiver ativada, o sistema obterá o nome do emissor codificado a partir de um certificado.

3. O sistema executa hash no nome do emissor codificado com SHA1.
4. O sistema tenta localizar uma autoridade configurada no sistema que tenha um nome cujo hash corresponda ao do certificado.
5. Se nenhuma autoridade for localizada, nenhuma verificação será executada.
6. Se uma autoridade for localizada, o sistema verificará a política do OCSP para a autoridade. Se a política permitir ou requerer verificações do OCSP, consulte a tabela CERT_AUTHORITY para obter informações adicionais. O sistema tenta localizar um respondente do OCSP para a autoridade.
7. Se nenhum respondente do OCSP for localizado para a autoridade, uma das opções a seguir acontece:
   - Se a política de autoridade estiver configurada para sempre verificar, uma exceção será lançada e a verificação falhará.
   - Se a política de autoridade for a única verificação quando um respondente estiver configurado, nenhuma verificação será executada.
   - Se um respondente do OCSP for localizado para a autoridade, ocorrerá uma tentativa de verificação do OCSP.

Tabelas de Banco de Dados

Duas novas tabelas de banco de dados foram incluídas para gerenciar informações relacionadas ao OCSP:

- CERT_AUTHORITY
- OCSP_RESPONDER

CERT_AUTHORITY

A tabela CERT_AUTHORITY mantém informações sobre autoridades de certificação.

Coluna	Tipo	Descrição
OBJECT_ID	VARCHAR (255)	Este é um GUID que constitui um ID exclusivo para um registro. Esta é a chave primária. Não pode ser nulo.
NAME	VARCHAR (255)	Um nome para um registro. Nulo permitido.
CREATE_DATE	DATETIME	Uma data de criação de um registro.
MODIFIED_DATE	DATETIME	A data em que um registro foi modificado pela última vez.
MODIFIED_BY	VARCHAR(255)	As informações sobre quem modificou um registro.
ISSUER_NAME	BLOB	O RDN da autoridade obtido de seu certificado.
HASH_ALG	VARCHAR(128)	O algoritmo hash usado para calcular o nome e os hashes de chave. Apenas SHA1 é suportado.
RDN_HASH	VARCHAR(255)	Hash SHA1 codificado como BASE64 do RDN do emissor codificado como DER obtido do certificado da autoridade. Essa coluna é indexada.
KEY_HASH	VARCHAR(255)	Hash SHA1 codificado como BASE64 da chave pública codificada no certificado do emissor.

Coluna	Tipo	Descrição
CERT_OID	VARCHAR(255)	O OBJECT_ID do certificado de autoridade na tabela CA_CERT_INFO. Cada autoridade deve ter um certificado de CA no banco de dados. Nulos não são permitidos.
OCSP_POLICY	VARCHAR(128)	A política do OCSP para a autoridade. Ela consiste em dois valores separados por vírgulas. Os valores descrevem quando usar OCSP e o que verificar. Os valores possíveis são: **OCSP_When** • never – nunca usar OCSP • resp – usar apenas OCSP se um respondente estiver configurado quando uma solicitação for feita • always – sempre usar OCSP quando uma solicitação for feita. Isso requer que um respondente seja configurado e fará com que a verificação de certificado falhe se nenhum respondente for configurado **OCSP_What** • none – nunca verificar nenhum certificado • end-user- verificar apenas certificados do usuário final • both – verificar certificados do usuário final e intermediários. Atualmente não suportado • Nulo não é permitido nesta coluna
CRL_POLICY	VARCHAR(128)	Atualmente não usado.

OCSP_RESPONDER

A tabela OCSP_RESPONDER mantém informações sobre respondentes do OCSP.

Coluna	Tipo	Descrição
OBJECT_ID	VARCHAR (255)	Este é um GUID que constitui um ID exclusivo para um registro. Esta é a chave primária. Não pode ser nulo.
NAME	VARCHAR (255)	Um nome para um registro. Nulo permitido.
CREATE_DATE	DATETIME	Uma data de criação de um registro.
MODIFIED_DATE	DATETIME	A data em que um registro foi modificado pela última vez.
MODIFIED_BY	VARCHAR(255)	As informações sobre quem modificou um registro.
ISSUER_NAME	BLOB	O RDN da autoridade obtido de seu certificado.

Coluna	Tipo	Descrição
HASH_ALG	VARCHAR(128)	O algoritmo hash usado para calcular o nome e os hashes de chave. Apenas SHA1 é suportado.
RDN_HASH	VARCHAR(255)	Hash SHA1 codificado como BASE64 do RDN do emissor codificado como DER obtido do certificado da autoridade. Essa coluna é indexada.
KEY_HASH	VARCHAR(255)	Hash SHA1 codificado como BASE64 da chave pública codificada no certificado do emissor.
CERT_OID	VARCHAR(255)	O OBJECT_ID do certificado de autoridade na tabela CA_CERT_INFO. Cada autoridade deve ter um certificado de CA no banco de dados. Nulos não são permitidos.
CACHE_TTL	VARCHAR(64)	O tempo em segundos que respostas do OCSP podem viver no cache de resposta interno Se a coluna for NULL, respostas do OCSP só serão armazenadas em cache por 1 segundo, o que na prática significa zero.
TRANS_PROF_OID	VARCHAR(255)	OBJECT_ID de um perfil no banco de dados GIS. É necessário criar um perfil para o respondente do OCSP que inclua a URL correta para o respondente.
COMM_BP	VARCHAR(255)	Nome de um processo de negócios para usar para comunicação com o respondente do OCSP. Ele deve ser um processo de negócios que realize uma comunicação HTTP. Serviços no processo de negócios têm que ser configurados para não requererem ou apresentarem cabeçalhos HTTP durante envio e recebimento, respectivamente. O processo HTTPClientSend fornecido com o sistema pode ser usado e é recomendado
COMM_WAIT	VARCHAR(24)	O número de segundos que você deve esperar para a comunicação com o respondente do OCSP ocorrer antes de concluir que algo está errado.

Configuração do OCSP

Sobre Esta Tarefa

Ao a configuração do sistema, é possível criar quantas autoridades e respondentes você quiser.

Para configurar o sistema para usar OCSP:

Procedimento

1. Verifique o certificado para a autoridade de certificação que emite os certificados que você quer verificar no OCSP no Sterling B2B Integrator para verificar se ele é um certificado de CA.

2. Liste os certificados de CA no sistema e obtenha o ID do objeto para o certificado instalado.
3. Se o certificado de assinatura de resposta do OCSP da autoridade for diferente do certificado emitido da autoridade, marque o certificado de assinatura de resposta do OCSP da autoridade no Sterling B2B Integrator como um certificado confiável.

   Nota: Com 5.2.4.2 e superior, é possível marcar o certificado raiz que emitiu o certificado respondente como CA, ao invés do certificado respondente como um Certificado Confiável. Uma vez que o certificado respondente muda frequentemente, dependendo da CA, ele pode fazer o OCSP falhar até que o certificado seja substituído por um válido. Você deve sempre marcar um certificado raiz a partir de agora como uma melhor prática, já que ele raramente muda. No entanto, ambos os tipos continuarão a ser permitidos.
4. Se você registrou um certificado de assinatura do OCSP adicional, liste os certificados de CA no sistema e obtenha o ID do objeto para o certificado que acabou de instalar.
5. Acesse o diretório bin da instalação do Sterling B2B Integrator.
6. Inicie o banco de dados se necessário.
7. Inicie o shell bash ou sh.
8. Defina a origem do arquivo tmp.sh
9. Crie uma autoridade usando o utilitário no com.sterlingcommerce.security.ocsp.SCICertAuthority da classe.
10. Criar um respondente do OCSP usando o utilitário no com.sterlingcommerce.security.ocsp.SCIOCSPResponder da classe
11. Atualize os certificados para a autoridade ou certificados individuais para ativar o OCSP. O utilitário com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo configurará todos os certificados confiáveis e de sistema para uma autoridade. O utilitário com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo configurará um certificado de sistema. O utilitário com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo configurará um certificado confiável.

Scripts de Configuração do OCSP

Os seguintes scripts foram incluídos com o hotfix do OCSP para executar os utilitários de configuração do OCSP. Há uma versão do UNIX/Linux e Windows de cada script. Os scripts usam os mesmos argumentos de linha de comandos que os programas utilitários que eles chamam. Os scripts estão localizados no diretório bin da instalação do produto. As informações sobre argumentos de linha de comandos são essencialmente repetidas nesta seção descrevendo os scripts.

ManageCertAuthority.sh e ManageCertAuthority.cmd

Argumento	Descrição

-a, -r, -d	Operação a ser executada: -a add -l list -d delete A opção –l não tem argumentos adicionais. A opção –d tem um único argumento: o ID do objeto do registro a ser excluído
Nome	Nome da autoridade. Requerido com –a.
Modified_by	Usuário que modificou ou criou a identidade. Requerido com –a.
Hash_alg	Algoritmo hash para a autoridade. Apenas o valor “SHA1” é suportado. Requerido com –a.
Certificate_id	ID do objeto do certificado de CA associado à autoridade. Requerido com –a.
OCSP_policy	A sequência de políticas do OCSP para a autoridade. Essa é uma sequência delimitada por vírgulas conforme descrito na seção na tabela CERT_AUTHORITY. Requerido com –a. Para o primeiro elemento da sequência, o seguinte é permitido: • never – nunca usar OCSP • resp – usar apenas OCSP se um respondente estiver configurado quando uma solicitação for feita • always – sempre usar OCSP quando uma solicitação for feita. Isso requer que o respondente seja configurado e faça a verificação de certificado falhar se nenhum respondente estiver configurado Para o segundo elemento da sequência, o seguinte é permitido: **OCSP What** • none – nunca verificar nenhum certificado • end-user- verificar apenas certificados do usuário final • both – verificar certificados do usuário final e intermediários. Atualmente não suportado. Exemplos: • never,none • always,end-user
Crl_policy	Sequência de políticas CRL para a autoridade. Requerido com –a. Um valor é requerido para esse argumento, mas não é usado atualmente. “None” é aceitável.

Object_ID	Um ID de objeto a ser usado durante a criação desse registro. Opcional com -a.

ManageOCSPResponder.sh e ManageOCSPResponder.cmd

Argumento	Descrição
-l	Obtém uma lista de respondentes de OCSP atualmente configurados. Essa opção não usa argumentos adicionais.
-d	Exclui o respondente do OCSP configurado com o ID de objeto fornecido para os dados de configuração de respondentes. Essa opção usa object_id como um argumento adicional.
-u2	Atualiza registros existentes no banco de dados com as informações corretas sobre a chave pública do certificado de autoridade e o DN do assunto do certificado de autoridade. Ele precisa ser executado com relação a todos os registros existentes para Respondentes do OCSP e de Autoridade de Certificação ou você precisará excluir e recriar os registros para obter as informações adequadas no banco de dados. Essa opção usa object_id como um argumento adicional.
-a	Inclui dados de configuração para um novo Respondente do OCSP a ser usado para verificar o status de certificados emitidos pela autoridade fornecida. Os argumentos adicionais são name, modified_by, hash_alg, authority_cert_oid, response_signing_cert_oid, resp_signing_cert_in_ca_store, cache_ttl, trans_prof_oid, comm_bp, comm_wait, send_nonce, require_nonce e object_id.
name	(Requerido com -a) Nome da autoridade.
modified_by	(Requerido com -a) Usuário que modificou ou criou a identidade.
hash_alg	(Requerido com -a) Algoritmo hash para a autoridade. Apenas o valor “SHA1” é suportado.
authority_cert_oid	(Requerido com -a) ID de objeto do certificado de CA associado à autoridade.

response_signing_cert_oid	(Requerido com -a) ID de objeto do certificado que o provedor de serviços do OCSP usou para assinar a resposta fornecendo o status para o certificado. Esse certificado deve ser incluído no armazenamento de Certificado Digital de CA ou no armazenamento de Certificado Digital Confiável. Esse é o ID do Certificado do Sistema para o certificado como ele aparece no armazenamento.
resp_signing_cert_in_ca_store	(Requerido com -a) Sinalizador indicando se o valor anterior do argumento response_signing_cert_oid está localizado no Armazenamento de Certificado Digital de CA no Sterling B2B Integrator.
cache_ttl	(Requerido com -a) O tempo de vida em segundos para respostas do OCSP no cache interno.
trans_prof_oid	(Requerido com -a) O ID de objeto de um transporte configurado para comunicação com o respondente do OCSP.
comm_bp	(Requerido com -a) Nome de um processo de negócios a ser usado para se comunicar com o respondente do OCSP. Ele deve ser um processo de negócios que realize uma comunicação HTTP. Serviços no processo de negócios têm que ser configurados para não requererem ou apresentarem cabeçalhos HTTP durante envio e recebimento, respectivamente. O processo HTTPClientSend que é fornecido com o sistema pode ser usado e é recomendado.
comm_wait	(Requerido com -a) O número de segundos que deve ser aguardado para a comunicação com o respondente até se concluir que ocorreu um erro.
send_nonce	(Requerido com -a) Indica se um valor NONCE será enviado para o serviço do OCSP. O valor NONCE é usado para evitar ataques de reprodução por alguns provedores do OCSP.
require_nonce	(Requerido com -a) Indica se o servidor deve requerer que o serviço do OCSP forneça um valor NONCE na resposta.
object_id	(Opcional com -a) Um ID de objeto a ser usado durante a criação desse registro.

SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd

Esse utilitário configurará as informações do OCSP no banco de dados para um único certificado do sistema

Argumento	**Descrição**

Esse utilitário configurará as informações do OCSP no banco de dados para um único certificado do sistema

-o, -n	Como interpretar o segundo argumento: -o object_ID -n name
Object_ID/Name	ID ou nome do objeto da autoridade, conforme determinado pelo argumento 1.

SetSystemCertOCSPInfo.sh e SetTrustedCertOCSPInfo.cmd

Esse utilitário configurará as informações do OCSP no banco de dados para um único certificado do sistema

Argumento	**Descrição**
-o, -n	Como interpretar o segundo argumento: -o object_ID -n name
Object_ID/Name	ID ou nome do objeto da autoridade, conforme determinado pelo argumento 1.

Executar um Script OCSP

Sobre Esta Tarefa

Use o exemplo a seguir para aprender como executar os scripts de configuração do OCSP. Esses scripts assumem que você já tenha registrado os certificados de CA para a autoridade, iniciado o banco de dados, que você esteja no diretório bin da instalação do Sterling B2B Integrator e tenha especificado a origem do arquivo tmp.sh no diretório bin.

Depois de obter o ID do objeto do certificado de CA da autoridade, no Sterling B2B Integrator, no **Menu de Administração**, selecione **Parceiros Comerciais > Certificados Digitais - CA**. Selecione um certificado. A caixa de diálogo Resumo do Certificado aparece com as informações do certificado, incluindo seu ID de objeto.

Conclua as seguintes etapas para executar um Script OCSP. Para obter uma lista integral de comandos de script OCSP, consulte “Scripts de Configuração do OCSP” na página 80.

Procedimento

1. Execute um comando semelhante ao seguinte para criar uma autoridade no sistema:

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

2. Depois de criar uma autoridade, e de criar um perfil para comunicação com um respondente do OCSP, execute um comando semelhante ao seguinte para criar um respondente do OCSP no sistema:

```
./ManageOCSPResponder.sh -a CertAuth_TestOCSP admin SHA1
"kenny:node1:13727b3f8e4:29762" "kenny:node1:13727275fd9:40698" false (use
true se o certificado de assinatura marcado
for o mesmo do certificado de resposta, que é, marcado para a
autoridade de certificação na etapa 3) "2400" "14ffd4a0:1371823040d:-77c8"
HTTPClientSend 3600 false false
```

3. Executar um comando semelhante ao seguinte para listar todas as autoridades no sistema:

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

   A saída de retorno para cada autoridade é exibida:

   ```
   CERT_AUTHORITY:
   OBJECT_ID: sedna:1ded0fd:11dc9d22929:-7fbd
   NAME: VPCA
   CREATE_DATE: 2008-11-23
   MODIFIED_DATE: 2008-11-23
   MODIFIED_BY: null
   ISSUER_NAME: Country=US, StateOrProvince=Dublin, OrganizationUnit=GIS
    Development, Organization=Sterling,
   CommonName=Test CA
   HASH_ALG: SHA1
   RDN_HASH: 24E63F8AE9F51497529EA0CC34467A4680737A9F
   ENCODED_RDN_HASH: JOY/iun1FJdSnqDMNEZ6RoBzep8=
   KEY_HASH: C96F2FF442EBFA07672DCEC49B729D4D24898313
   ENCODED_KEY_HASH: yW8v9ELr+gdnLc7Em3KdTSSJgxM=
   CERT_OID: sedna:a1807c:11dc6d53ba4:-7b4b
   OCSP_WHEN_POLICY: always
   OCSP_WHAT_POLICY: end-user
   CRL_POLICY: null
   ```

4. Use um comando semelhante ao seguinte para ativar o OCSP para todos os certificados confiáveis e do sistema emitidos pela autoridade:

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

Lógica de Verificação do OCSP

Sobre Esta Tarefa

As etapas a seguir descrevem a lógica de verificação do OCSP no Sterling B2B Integrator:

Se o status do certificado estiver ok, a verificação do OCSP foi bem-sucedida. Caso contrário, ela falhou.

Procedimento

1. Se uma resposta existente cujo tempo de vida não expirou for localizada, a resposta será usada como a resposta do OCSP.
2. Se nenhuma resposta existente for localizada no cache ou o tempo de vida tiver expirado para uma resposta no cache, uma solicitação do OCSP será criada.
3. Se o sistema criar uma solicitação do OCSP, ele ativará o processo de negócios configurado para o respondente do OCSP enviar a solicitação e receber a resposta. As solicitações incluirão um valor nonce se o respondente foi configurado para ter um enviado.
4. Se o processo de negócios for concluído com sucesso, o sistema tentará analisar seu documento primário como uma resposta do OCSP. O processo de negócios usado para enviar solicitações do OCSP e receber respostas do OCSP remove os cabeçalhos HTTP da resposta.
5. Se o documento primário puder ser analisado como uma resposta do OCSP, o sistema verificará o status da resposta.

6. Se o status da resposta indicar que a solicitação gerou uma resposta válida, o sistema tentará verificar a assinatura na resposta do OCSP usando o certificado configurado para o respondente do OCSP.
7. Se a assinatura for verificada e o respondente foi configurado para requerer um nonce, o sistema tentará obter e verificar o nonce da resposta.
8. Se todas as outras verificações forem aprovadas, o sistema procurará informações de status de certificado para o certificado para o qual a solicitação foi construída e enviada.
9. Se as informações de status forem localizadas, o sistema atualizou o cache interno para uma resposta do OCSP existente para o certificado.

Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) 140-2

Para conformidade com os requisitos de segurança do FIPS 200, os aplicativos devem usar módulos criptográficos certificados pelo Cryptographic Module Validation Program e compatíveis com FIPS 140-1 ou 140-2. Os requisitos mínimos para uso de criptografia validada por aplicativos são:

- Todas as operações criptográficas, incluindo a geração de chaves, devem ser desempenhadas por módulos criptográficos validados.
- Apenas funções de segurança aprovadas são permitidas.
- Apenas técnicas de estabelecimento de chave aprovadas são permitidas.

FIPS 140-2 com Sterling B2B Integrator

O Certicom Government Service Edition (GSE) é um módulo criptográfico certificado do FIPS 140-2 Nível 1 distribuído com Sterling B2B Integrator. GSE é um kit de ferramentas criptográfico de nível inferior gravado em Java que implementa uma variedade de funções de segurança, incluindo funções de segurança não aprovadas.

No modo FIPS, ele executa as seguintes tarefas:

- Ativa a máquina de estado GSE FIPS e chama power-on self-tests.
- Afunila chamadas de função criptográficas do sistema principal para o GSE.

Ativar FIPS Durante a Instalação

Sobre Esta Tarefa

Durante uma instalação nova, quando perguntado se você deseja executar no modo FIPS, selecione TRUE.

Ativar o Modo FIPS Manualmente

Sobre Esta Tarefa

É possível ativar o modo FIPS manualmente após a instalação do Sterling B2B Integrator.

Antes de começar, você deve verificar se possui uma licença para operar no modo FIPS antes que ele seja ativado. Isso verificará sua licença na inicialização e mas não inicializará se o modo FIPS estiver ativado, mas não licenciado.

Para ativar manualmente o modo FIPS:

Procedimento

1. Navegue para */install_dir*/properties/.
2. Localize o arquivo security.properties.
3. Abra o arquivo security.properties em um editor de texto. Se você fizer mudanças no arquivo security.properties, certifique-se de que fazer as mesmas mudanças no arquivo security.properties.in. Isso evitará que as definições customizadas sejam sobrescritas. Você deve usar o arquivo de propriedades de segurança para customizar o FIPS em vez de editar arquivos de propriedade diretamente.
4. Especifique as seguintes configurações: FIPSMode=true
5. Salve e feche o arquivo security.properties.
6. Reinicie o Sterling B2B Integrator. Isso é necessário para as mudanças serem reconhecidas no sistema.

Desativar Modo FIPS

Sobre Esta Tarefa

Para desativar manualmente o modo FIPS:

Procedimento

1. Navegue para */install_dir*/properties/.
2. Localize o arquivo security.properties.
3. Abra o arquivo security.properties em um editor de texto.
4. Especifique as configurações a seguir: FIPSMode=false
5. Salve e feche o arquivo security.properties.
6. Reinicie o Sterling B2B Integrator. Isso é necessário para as mudanças serem reconhecidas no sistema.

Servidores Proxy

Servidores Proxy

Servidores Proxy aprimoram a segurança do seu sistema.

Configurar Servidor Proxy HTTP

Sobre Esta Tarefa

Para configurar um servidor proxy HTTP:

Procedimento

1. No **Menu de Administração**, selecione **Operações** > **Servidores Proxy**.
2. Clique em **incluir**.
3. Insira o **Nome** do servidor proxy.
4. Selecione **HTTP** como o **Tipo**.
5. Insira o nome do **Host**. Os endereços de IPV6 devem ser colocados entre colchetes retos.
6. Insira o número da **Porta**.
7. Insira a **Contagem de Novas Tentativas**.
8. Clique em **Avançar**.
9. Se quiser requerer autenticação básica para o usuário:

- Selecione **Sim** e clique em **Avançar**.
- Se selecionar Não (padrão), clique em **Avançar** e vá para a Etapa 13.

10. Insira **ID do Usuário de Autenticação**.
11. Insira **Senha de Autenticação**.
12. Clique em **Avançar**.
13. Revise as Configurações do Servidor Proxy.
14. Clique em **Concluir**.

Configurar Servidor Proxy SSP

Sobre Esta Tarefa

Para configurar um servidor proxy SSP:

Procedimento

1. No **Menu de Administração**, selecione **Operações** > **Servidores Proxy**.
2. Clique em **incluir**.
3. Insira o **Nome** do servidor proxy.
4. Selecione **SSP** como o **Tipo**.
5. Insira o nome do **Host**. Os endereços de IPV6 devem ser colocados entre colchetes retos.
6. Insira o número da **Porta**.
7. Insira a **Contagem de Novas Tentativas**.
8. Clique em **Avançar**.
9. A autenticação básica é necessária para o usuário? Selecione Sim ou Não.
10. O SSL é necessário? Selecione Sim ou Não.
11. Clique em **Avançar**.
12. Se selecionou autorização básica para este usuário, você deverá inserir o **ID do Usuário de Autenticação** e a **Senha de Autenticação** e clicar em **Avançar**. Se você não exigiu essa autorização, esta página não será exibida.
13. Se selecionar Sim para SSL necessário, você deverá selecionar **Força da Criptografia**, **Certificados de CA** e **Certificados de Chave** e clicar em **Avançar**. Se você não exigiu SSL, esta página não será exibida.
14. Clique em **Avançar**.
15. Revise as Configurações do Servidor Proxy.
16. Clique em **Concluir**.

Configurar um Servidor Proxy para SSL

Sobre Esta Tarefa

Se decidir usar SSL com a configuração do servidor proxy SSP, você deve:

Procedimento

1. Criar um certificado SSL ou importar o certificado da autoridade de certificação no Sterling B2B Integrator.
2. Configurar o campo **Usar SSL** na configuração de adaptador apropriada para **Deve**.

Editar Servidores Proxy

Sobre Esta Tarefa

Para editar uma configuração do servidor proxy:

Procedimento

1. No **Menu de Administração**, selecione **Operações** > **Servidores Proxy**.
2. Clique em **Editar** para o servidor proxy que deseja editar.
3. Atualize os campos, conforme necessário.
4. Clique em **Avançar**.
5. Revise as Configurações do Servidor Proxy.
6. Clique em **Concluir**.

Excluir Servidores Proxy

Sobre Esta Tarefa

A exclusão de uma configuração do servidor proxy pode causar erros em alguns recursos do Sterling B2B Integrator. Talvez seja necessário reconfigurar adaptadores e serviços específicos para trabalharem adequadamente sem uma configuração do servidor proxy específico.

Para editar uma configuração do servidor proxy:

Procedimento

1. No **Menu de Administração**, selecione **Operações** > **Servidores Proxy**.
2. Clique em **Excluir** para o servidor proxy que deseja editar.
3. Revise as Configurações do Servidor Proxy.
4. Clique em **Excluir**.

SSL

Sobre a implementação do SSL no Sterling B2B Integrator

O Secure Sockets Layer (SSL) fornece comunicação segura através da internet. Ele usa criptografia simétrica e assimétrica.

O protocolo de segurança SSL fornece autenticação de servidor e autenticação de cliente no Sterling B2B Integrator:

- A autenticação de servidor é executada quando um cliente se conecta ao servidor. Após o handshake inicial, o servidor envia seu certificado digital para o cliente. O cliente valida o certificado do servidor ou a cadeia de certificados.
- A autenticação de cliente é executada quando um servidor envia uma solicitação de certificado para um cliente durante o handshake. Se o certificado de cliente ou cadeia forem verificados e a mensagem de verificação de certificado for verificada, o handshake continuará.
- Um autenticação adicional opcional é executada verificando o nome comum no certificado com relação ao nome completo do domínio do servidor a partir de uma consulta de Servidor de Nomes de Domínio (DNS) reversa na qual o nome completo do domínio do servidor pode ser obtido.

Tipos de Confiança

Dois tipos de confiança para os certificados SSL são suportados no Sterling B2B Integrator:

- Confiança de CA – Confiança hierárquica com base em um certificado raiz usado para emitir outros certificados. Esse é o modelo de confiança de certificado SSL padrão.
- Confiança Direta - Confiança direta de certificados autoassinados tidos como distribuídos por meio mecanismos seguros fora da banda. Os certificados autoassinados e a confiança direta não fazem parte dos padrões de SSL, mas são usados com frequência em certas comunidades comerciais.

Certificados SSL

Para comunicar usando SSL, configure os sistemas envolvidos para suportar tanto a autenticação de servidor como a autenticação do cliente/servidor. Para executar autenticação com relação a um servidor, você precisa de um certificado de Autoridade de Certificação (CA) raiz e do conjunto de certificados intermediários na cadeia ou, se o servidor usar um certificado autoassinado, de uma cópia do certificado autoassinado.

Para suportar autenticação de cliente/servidor, você precisa de um certificado autoassinado ou de CA e de um certificado do sistema.

É possível obter um certificado SSL de uma CA confiável fornecendo um Certificate Signing Request (CSR) para a CA. O certificado SSL liga a chave pública e o cliente ou servidor SSL.

Caso pretenda usar autenticação de cliente/servidor, configure um certificado do sistema. É possível criar certificados do sistema das seguintes formas:

- Efetue check-in em um arquivo de certificado-chave existente ou arquivo PKCS12
- Gere um certificado do sistema autoassinado
- Use o Utilitário de gerenciamento de chave (iKeyman) para gerar um CSR e obter um certificado a partir de uma CA. Para obter informações sobre o iKeyman, consulte o “Utilitário de gerenciamento de chave IBM (iKeyman)” na página 60.

Conjuntos de criptografia

Antes de usar o Sterling B2B Integrator, deve-se revisar as listas de cifras disponíveis, predefinidas e customizá-las de acordo com os requisitos de segurança da sua empresa.

Os conjuntos de criptografia do IBM SDK, Java Technology Edition, Versão 7 podem ser localizados aqui: http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html. Para outros JDKs suportados no Sterling B2B Integrator, consulte a documentação do fornecedor JDK para uma lista de conjuntos de criptografia suportados.

A intensidade da cifra é configurada no `security.properties` ou no `customer_overrides.properties`. Os níveis dos conjuntos de criptografia disponíveis são:

- AllCipherSuite (A seleção da UI é **TODOS**) - inclui tudo que está listado em FRACO e FORTE.
- WeakCipherSuite (A seleção da UI é **FRACO**) - Inclui os conjuntos de criptografia fracos suportados que você deseja usar com o Sterling B2B Integrator
- StrongCipherSuite (A seleção da UI é **FORTE**) - Inclui os conjuntos de criptografia fortes suportados que você deseja usar com o Sterling B2B Integrator
- CipherSuiteDefault (disponível na V5.2.6 e superior) - por padrão, inclui um subconjunto de cifras suportadas para o IBM JDK7. Usado se WeakCipherSuite e StrongCipherSuite estiverem vazios.

Adaptadores Clientes para SSL

Os adaptadores clientes a seguir suportam SSL:

- Adaptador Cliente FTP
- Adaptador Cliente HTTP
- Adaptador do solicitante Sterling Connect:Direct FTP+ (com Secure+ Option)

Os parâmetros para SSL podem ser configurados no perfil do parceiro comercial ou para o adaptador. Para o adaptador cliente FTP, esses parâmetros são configurados no serviço Sessão Inicial do Cliente de FTP. Para o adaptador cliente HTTP, esses parâmetros são configurados no serviço Sessão inicial do Cliente HTTP. Os parâmetros configurados no serviço Sessão Inicial substituem as configurações em um perfil do parceiro comercial.

Os parâmetros na tabela a seguir controlam SSL a partir de uma perspectiva de cliente. Consulte a documentação para o adaptador ou serviço específico que você está configurando.

Parâmetro	Descrição
SSL	Determina a negociação de soquete SSL.
CACertificateId (trusted_root)	Lista de certificados públicos de CA confiáveis. Nos dados do processo, esse parâmetro é exibido como um ID do objeto.
CipherStrength	O nível de criptografia a ser aplicado aos dados que fluem pela conexão do soquete.
SystemCertificateId	Selecione na lista de certificados do sistema disponíveis. Esse certificado confirma a identidade do cliente para o servidor.

Adaptadores para Servidor para SSL

Os adaptadores para servidor a seguir suportam SSL:

- Adaptador para Servidor FTP
- Adaptador para Servidor HTTP
- Adaptador para servidor Sterling Connect:Direct (com Secure+ Option)
- Adaptador de envio SMTP

Os parâmetros na tabela a seguir controlam SSL a partir de uma perspectiva do servidor. Consulte a documentação para o adaptador ou serviço específico que você está configurando.

Parâmetro	Descrição
SSL	Se o SSL está ativo.
Passphrase do Certificado de Chave	Senha que protege o certificado de chave do servidor. Esse passphrase é usado internamente pelo sistema para inicializar as bibliotecas SSL.
CipherStrength	Força dos algoritmos usados criptografar dados.
Certificado de Chave (Armazenamento do Sistema)	Chave privada e certificado para autenticação de servidor.
Certificado de CA	Certificado usado, se houver algum, para validar o certificado de um cliente.

Registro de Entrada de um Certificado

Sobre Esta Tarefa

Para suportar autenticação de cliente/servidor, você precisa de um certificado autoassinado ou de CA e de um certificado do sistema.

É possível efetuar o registro de entrada de um certificado de CA ou certificado autoassinado em um armazenamento de certificados de CA selecionando **Parceiro Comercial** > **Certificados Digitais** > **CA** > **Registro de Entrada do Novo Certificado** no **Menu de Administração**.

Criar Certificados Autoassinados para Teste

Sobre Esta Tarefa

Para teste, é possível usar certificados autoassinados. Eles podem ser gerados e gerenciados no Sterling B2B Integrator.

Para criar um certificado autoassinado:

Procedimento

1. Selecione **Parceiros Comerciais** > **Certificados Digitais** > **Certificados do Sistema** > **Criar Certificado Autoassinado**.
2. Após ele ser criado, localize-o e registre sua saída em um arquivo.
3. Efetue o registro de entrada do certificado novamente no Sterling B2B Integrator como um certificado de CA selecionando **Parceiros Comerciais** > **Certificados Digitais** > **CA** > **Registro de Entrada do Novo Certificado**.

Renegociação de SSL/TLS (V5.2.6 ou posterior)

O Sterling B2B Integrator usa parâmetros do IBM JSSE para controlar o nível de restrição da renegociação de SSL/TLS. Os seguintes parametros estão disponíveis para atualização no arquivo `security.properties`.

Nome do Parâmetro	Definição	Valores Válidos
com.ibm.jsse2.estendido.renegotiation.indicator	Use essa propriedade para forçar todas as negociações a requererem RFC 5746, não apenas as renegociações. Essa negociação seria praticável somente após todos os parceiros de comunicação necessários terem implementado RFC 5746. A configuração padrão é OPTIONAL.	Os valores válidos são: • BOTH - Faz com que o IBM JSSE2 Server ou o IBM JSSE2 Client conectem-se somente se o peer tiver indicado suporte para renegociação de RFC 5746. Nota: configurar a propriedade para BOTH causa problemas de interoperabilidade com clientes ou servidores que não foram atualizados para suportar RFC 5746. • CLIENT - Faz com que o IBM JSSE2 Client conecte-se somente se o servidor tiver indicado suporte para renegociação de RFC 5746. Nota: configurar a propriedade para CLIENT causa problemas de interoperabilidade com servidores que não foram atualizados para suportar RFC 5746. • OPTIONAL - Esta configuração é a padrão. Usar esta opção significa que o IBM JSSE2 Server ou o IBM JSSE2 Client não requerem o indicador de renegociação durante o handshake inicial. • SERVER - Faz com que o IBM JSSE2 Server conecte-se somente se o cliente tiver indicado suporte para renegociação de RFC 5746. Nota: configurar a propriedade para SERVER causa problemas de interoperabilidade com clientes que não foram atualizados para suportar RFC 5746.

Nome do Parâmetro	Definição	Valores Válidos
com.ibm.jsse2.renegotiate	Use essa propriedade para mudar a capacidade de renegociação do IBM JSSE2. O valor padrão é NONE.	Os valores válidos são: • ABBREVIATED - Esta configuração substitui e permite o handshake abreviado não protegido durante a renegociação quando a continuidade da sessão for comprovada. Renegociações de RFC 5746 são permitidas. • ALL - Esta configuração substitui e permite o handshake integral não protegido e o handshake abreviado não protegido durante a renegociação. Renegociações de RFC 5746 são permitidas. • DISABLED - Esta configuração substitui e desativa todas as renegociações não protegidas e de RFC 5746. • NONE - Esta configuração é a padrão. Nenhuma renegociação de handshake não protegido é permitida. Somente renegociações de RFC 5746 são permitidas.
com.ibm.jsse2. renegociação .peer.cert.check	Use essa propriedade para mudar a capacidade de renegociação do IBM JSSE2 para requerer o suporte de peer especificação em RFC 5746. Esse requisito é praticável somente após todos os parceiros de comunicação necessários terem implementado RFC 5746. O valor padrão é OFF.	Os valores válidos são: • OFF - Esta configuração é a padrão. Para o IBM JSSE2 Client ou o IBM JSSE2 Server que está executando uma verificação de identificação com relação ao certificado do peer. O resultado é permitir que o certificado do peer mude durante a renegociação. • ON - Esta configuração faz com que o IBM JSSE2 Client ou o IBM JSSE2 Server execute uma comparação com relação ao certificado do peer. A razão é assegurar que o certificado não mude durante a renegociação. A comparação é aplicável a renegociações seguras e não seguras.

Resolução de Problemas de SSL

Mensagens de Erro de Certificado Corrompido ou Inutilizável

Se você receber a mensagem de erro a seguir:

```
FATAL Alert:BAD_CERTIFICATE - Um certificado corrompido ou inutilizável foi
recebido.
```

As informações do log Perímetro serão as seguintes:

```
ERROR <HTTPClientAdapter_HTTPClientAdapter_node1-Thread-19>
HTTPClientAdapter_HTTPClientAdapter_node1-Thread-172105824724com.
sterlingcommerce.perimeter.api.conduit.SSLByteDataConduit@4c2b95c6:
Doing reset3 c
om.certicom.net.ssl.SSLKeyException: FATAL Alert:BAD_CERTIFICATE -
A corrupt or unusable certificate was received.
 at com.certicom.tls.d.b.a(Unknown Source)
 at com.certicom.tls.d.b.do(Unknown Source)
```

Ao efetuar o registro de entrada do certificado, o Sterling B2B Integrator mostra um valor de Status de "Assinatura Inválida" na tela de nomenclatura. Se um processo de negócios que executa um POST HTTP de saída com SSL falhar no serviço Método de HTTP com erro, a seguinte mensagem será exibida:

```
Código de Status HTTP: -1
Frase-razão HTTP: Erro Interno: Conexão foi encerrada no
lado do perímetro com erro: CloseCode.CONNECTION_RESET
```

Obtenha o certificado de CA apropriado para o parceiro comercial. Se o parceiro comercial estiver usando um certificado autoassinado, o certificado em si poderá ser usado como o certificado de CA.

Confiança Direta e de CA

Quando o Sterling B2B Integrator é o cliente, se o servidor tem um certificado emitido por uma CA e esse certificado tem o nome DNS do servidor no assunto Nome Distinto Relativo (RDN), é possível colocar o certificado de CA raiz no armazenamento de CA e confiar nele. Se o SSL ainda não funcionar, tente a confiança direta. Coloque o certificado do servidor no armazenamento de CA e confie nele.

Se o servidor estiver usando um certificado autoassinado, coloque-o no armazenamento de CA e confie nele. Você está usando confiança direta nesse caso também.

Uso de SSL Sem Certificado

Não é possível usar adaptadores ativados por SSL sem ter o certificado do sistema ou certificado necessário.

SSL não funciona com um conjunto de criptografia baseado em CBC

Se você selecionou o conjunto de criptografia de modo CBC e o SSL não funcionar, deve-se desligar a proteção CBC.

Para a V5.2.5 e inferior, execute as etapas a seguir:

1. Abra o arquivo tmp.sh para editar.

2. Localize a sinalização do servidor para o sistema operacional que você está configurando e inclua o valor a seguir:

   ```
   -DDisableSSLEmptyRecords=true
   ```

3. Salve e feche o arquivo.

Para a V5.2.6 e superior, execute as etapas a seguir:

1. No diretório *<B2Bi Install>*/bin, localize `InstallNoappsWindowsService.cmd.in` e `InstallContainerWindowsService.cmd.in` para o Windows; localize `tmp.sh_platform_ifcresources_ext.in` para todos os outros sistemas operacionais.
2. Edite o arquivo para alterar todas as ocorrências da propriedade a seguir para falso:

   ```
   jsse.enableCBCProtection=true
   ```

3. Execute o script `setupfiles`.

Configuração HTTPS para GPM

O acesso HTTP seguro via SSL já é suportado para a maioria dos aplicativos da web no Sterling B2B Integrator na porta HTTP + 1 base. Esse aprimoramento de SSL:

- Ativa HTTPS (HTTP com criptografia de SSL) para Graphical Process Modeler (GPM)
- Ativa a desativação e o redirecionamento de aplicativos da web na porta HTTP base para outra porta (usando HTTPS)
- Suporta acesso seguro a aplicativos da web implementando os aplicativos da web em uma instância do adaptador para servidor HTTP segura
- Reduz riscos de segurança

Se você usar esse recurso, será necessário configurar o Graphical Process Modeler (GPM) para se comunicar com o aplicativo da web Dashboard usando HTTPS em vez de HTTP. O acesso a aplicativos da web implementados via um adaptador para servidor HTTP seguro pode ser mais lento do que o acesso na porta base.

Nota: No V5.2.6 e superior, o protocolo de segurança padrão é TLS 1.2 (para a porta HTTP base + 1.). Se necessário, é possível alterar isto para o TLS 1.1 ou TLS 1.0 atualizando o parâmetro **`jsseProtocol`** no `properties_platform_ifcresources_ext`. Os valores válidos incluem os parâmetros a seguir:

- **`TLS1-TLS1.1`** - para TLS1.0 e TLS1.1
- **`TLS1.1-TLS1.2`** - para TLS1.1 e TLS1.2
- **`TLS1`** - somente para TLS1.0
- **`TLS1.1`** somente para TLS1.1
- **`TLS1.2`** - somente para TLS1.2

Novos Parâmetros de SSL

Vários novos parâmetros foram incluídos no SSL aprimorado. Você precisará configurar esses parâmetros para facilitar a comunicação SSL entre o Graphical Process Modeler (GPM) e o servidor. Esses novos parâmetros devem ser definidos em seus respectivos arquivos de propriedades.

Todas as propriedades customizadas para seu ambiente devem ser configuradas no arquivo customer_overrides.properties para não serem sobrescritas durante um

upgrade ou instalação de correção. As propriedades definidas no arquivo sandbox.cfg não devem ser definidas em customer_overrides.properties, já que serão ignoradas em customer_overrides.properties. Essas propriedades são as únicas que não estão definidas em customer_overrides.properties.

A tabela a seguir descreve os novos parâmetros SSL e fornece o nome do arquivo de propriedades onde o parâmetro pode ser localizado.

Nome do Parâmetro	**Definição**	**Arquivo de propriedades**
WEBAPP_LIST_PORT	Identifica a porta que o cliente GPM deve usar para comunicação com o servidor. Ele é padronizado para a porta base durante a instalação. Se os aplicativos da web Dashboard e GPM tiverem sido implementados em uma instância do adaptador para servidor HTTP segura, esse parâmetro deverá ser modificado para corresponder à porta da instância do adaptador para servidor HTTP segura. Se a porta SSL base (porta HTTP +1 base) estiver sendo usada para implementação segura do GPM e Dashboard, esse parâmetro deverá ser modificado para corresponder à porta SSL base (SSL_PORT em sandbox.cfg).	Arquivo sandbox.cfg
WEBAPP_PROTOCOL	Identifica o protocolo a ser usado para comunicação com o aplicativo da web Dashboard (http/https).	Arquivo sandbox.cfg

Nome do Parâmetro	Definição	Arquivo de propriedades
SKIP_BASEPORT_ DEPLOYMENT_WARS	Indica quais aplicativos da web devem ser ignorados durante a implementação do war na porta base. A lista de wars é delimitada por vírgulas, faz distinção entre maiúsculas e minúsculas e não tem o sufixo .war. O padrão é não ignorar nenhum war. Após os aplicativos da web Dashboard e GPM serem implementados com êxito em um Adaptador para Servidor HTTP seguro, esse parâmetro pode ser configurado como =admin,dashboard,gbm para remover acesso àqueles aplicativos da web na porta base. A lista completa de aplicativos da web inclui: • myaft • portlets O valor ALL pode ser usado como curinga para indicar que todos os wars implementados na porta base HTTP devem ser ignorados. Isso pode não ser necessário se a porta base estiver bloqueada para acesso externo. O valor ALL não deve ser usado com nenhum outro valor.	customer_overrides.properties
HTTPS_REDIRECT_WARS	Indica os wars que serão redirecionados automaticamente da porta base HTTP para o adaptador para servidor HTTP seguro ou porta base SSL. O valor ALL pode ser usado para redirecionar todos os wars ignorados na porta HTTP base para HTTPS_LIST_PORT (o adaptador para servidor HTTP seguro ou porta SSL base). O valor ALL não deve ser usado com nenhum outro valor.	customer_overrides.properties
HTTPS_LIST_PORT	Indica a porta de destino redirecionada para solicitações feitas com relação à porta HTTP base. Deve ser configurado para o valor do adaptador para servidor HTTP seguro ou porta base SSL.	customer_overrides.properties

Nome do Parâmetro	Definição	Arquivo de propriedades
HTTPS_CLIENT_CERTS	Uma lista separada por vírgulas de certificados do sistema cujas chaves públicas precisam ser incluídas no armazenamento confiável padrão. Esses certificados são usados para verificação do lado do cliente durante o handshake SSL quando chamadas HTTPS são iniciadas a partir de um servidor Application Server-Independent (ASI) de volta para si mesmo. Esse parâmetro requer chaves de certificado do servidor com **SubjectAltName**. Se você usar chaves existentes sem esse parâmetro, essa funcionalidade falhará com mensagens muito obscuras. **Nota:** O certificado configurado para HTTPS na porta +1 (sslCert) é incluído automaticamente no armazenamento confiável e não precisa ser incluído nessa lista.	customer_overrides.properties

Durante a configuração desse recurso, se você definir apenas SKIP_BASEPORT_DEPLOYMENT_WARS, mas não HTTPS_REDIRECT_WARS e HTTPS_LIST_PORT, os aplicativos da web ficarão inacessíveis na porta base e o usuário não será automaticamente redirecionado para a porta HTTPS. Esse é um cenário válido, caso o usuário prefira não redirecionar automaticamente por razões de segurança. Os aplicativos da web continuam disponíveis quando acessados no adaptador para servidor HTTP seguro ou porta base SSL.

Ativar Autorredirecionamento para HTTPS

Sobre Esta Tarefa

Foi incluído suporte para permitir um redirecionamento automático para HTTPS a ser configurado para os aplicativos da web que são implementados em uma porta segura (Adaptador para Servidor HTTP ou porta SSL base) e ignorados na porta base. Essa é uma configuração opcional, porém altamente recomendada.

Nota: Todas as propriedades customizadas para seu ambiente devem ser configuradas no arquivo customer_overrides.properties para não serem sobrescritas durante um upgrade ou instalação de correção.

Para ativar redirecionamento automático para HTTPS:

Procedimento

1. Navegue para `/<install_dir>/install/properties`.
2. Abra o arquivo customer_overrides.properties e configure os seguintes valores de parâmetro conforme mostrado:

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

   Esses parâmetros são configurados para redirecionar automaticamente um usuário para a ocorrência HTTPS do aplicativo da web.

Nota: O arquivo customer_overrides.properties não faz parte do código do sistema padrão. Ele deve ser criado após a instalação inicial do sistema e preenchido para corresponder ao seu ambiente.

3. Salve e feche o arquivo.

Implementação de Exemplo

A implementação de exemplo no arquivo customer_overrides.properties:

```
 ## Identifica wars para redirecionamento automático para a porta https.
Use uma lista separada por vírgula
## para especificar diversos wars
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica a porta https para wars redirecionados. Se for especificada, ela
## deve corresponder ao WEBAPP_LIST_PORT no sandbox.cfg
HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_port>
```

Nota: Se você estiver usando uma instância do adaptador para servidor HTTP segura, a configuração exigirá que todos os wars especificados como HTTPS_REDIRECT_WARS sejam implementados na mesma instância do adaptador para servidor HTTP.

HTTPS_CLIENT_CERTS

Se uma instância do adaptador para servidor HTTP segura for usada, o certificado SSL usado para configurar a instância do adaptador para servidor HTTP segura deverá ser incluído na lista de certificados confiáveis. Isso é necessário porque algumas telas do Dashboard fazem chamadas https de volta para o servidor ASI. Para essas chamadas concluírem o handshake SSL com sucesso, os certificados devem ser configurados no armazenamento confiável no servidor ASI. Isso é feito especificando o nome do certificado na lista HTTPS_CLIENT_CERTS.

Esses certificados do sistema devem ter os nomes de DNS e endereço(s) IP especificados como nomes alternativos quando o certificado do sistema é criado. A verificação do nome do host SSL padrão fornecida pelo JDK requer que o nome do certificado apresentado pelo servidor SSL corresponda ao nome do host usado na url http ou a uma das sequências no atributo "SubjectAltName" no certificado. Algumas telas no Dashboard não funcionarão sem a configuração "SubjectAltName".

Nomes alternativos são configurados por meio dos campos "Lista de Endereços IP Separados por Vírgula" e "Lista de Nomes DNS Separados por Vírgula" no assistente de criação Certificado do Sistema (**Parceiro Comercial** > **Certificados Digitais** > **Sistema**).

Suporte HTTPS para o GPM

O Java Web Start (JavaWS) é usado para ativar o Graphical Process Modeler (GPM) usando HTTP. Ele suporta HTTPS e a importação dinâmica de certificados semelhantes nos navegadores. Durante o handshake SSL, o servidor fornece seu certificado e o JavaWS manipula a verificação de confiança. Se o certificado não puder ser verificado pelo JavaWS, será solicitado que o usuário o aceite ou rejeite. Os certificados SSL não podem ser verificados automaticamente pelo JavaWS e devem ser verificados por usuários.

Importar Certificados para o Java Web Start

Sobre Esta Tarefa

Se quiser evitar um prompt de certificado não confiável durante a operação Java Web Start (JavaWS), é possível importar os certificados no armazenamento de máquina local antes de ativar o Graphical Process Modeler (GPM). Isso pode evitar confusão para o usuário caso o certificado SSL associado ao adaptador para servidor HTTP seguro ou porta SSL base não seja confiável para a máquina local do usuário.

Para importar certificados raiz confiáveis no JavaWS:

Procedimento

1. Salve o certificado de raiz confiável em um arquivo no computador local.
2. Abra **Painel de Controle Java** no computador local (javaws.exe em `jre\bin`).
3. Abra a guia **Segurança** e clique em **Certificados**.
4. Clique em **Importar** para navegar para um certificado de raiz confiável e selecioná-lo.
5. Clique em **Abrir** para importar o novo certificado de raiz confiável. Após o certificado de raiz confiável ser registrado, o JavaWS o usará para verificação de confiança durante um handshake SSL.

Alternar de HTTP para HTTPS Usando Porta SSL Base

Sobre Esta Tarefa

Para alternar de HTTP para HTTPS usando a porta SSL base:

Procedimento

1. Navegue até o `/install_dir/install/properties`.
2. Abra o arquivo sandbox.cfg.
3. Modifique os seguintes parâmetros:

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

   Esses parâmetros são usados pelo Graphical Process Modeler (GPM) para comunicação com o servidor.
4. (Opcional, Recomendado) Se quiser desativar o acesso aos aplicativos da web Dashboard e GPM na porta base, e configurar o redirecionamento automático para a porta HTTPS, especifique os seguintes parâmetros em um arquivo customer_overrides.properties:

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

Por exemplo:

```
## Identifica os arquivos war a serem ignorados durante a implementação na porta base.
## Use uma lista separada por vírgula para especificar diversos wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica wars para redirecionamento automático para a porta https.
## Use uma lista separada por vírgula para especificar diversos wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica a porta https para wars redirecionados. Se for especificada, ela
## deve corresponder ao WEBAPP_LIST_PORT no sandbox.cfg
noapp.HTTPS_LIST_PORT=<base_port + 1>
```

5. Salve e feche o arquivo.
6. Navegue para `/install_dir/install/bin`.
7. Pare o Sterling B2B Integrator.
8. Aplique as mudanças de configuração. Insira `./setupfiles.sh`.
9. Implemente a nova configuração. Insira `./deployer.sh`.
10. Inicie o Sterling B2B Integrator.
11. (Opcional) Se você desativou o acesso aos aplicativos da web Dashboard e GPM na porta base (Etapa 4), verifique as mudanças feitas. Por exemplo, é possível verificar:
    - O acesso ao aplicativo da web Dashboard em http://host:baseport/dashboard está inacessível ou é redirecionado para https://host:<base_port + 1>/dashboard automaticamente.
    - O acesso ao aplicativo da web GPM em http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp está inacessível ou é redirecionado para https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp automaticamente.

Alternar do Modo HTTP para HTTPS Usando um Adaptador para Servidor HTTP Seguro

Sobre Esta Tarefa

Para alternar do modo HTTP para HTTPS:

Procedimento

1. Crie uma nova instância do adaptador para servidor HTTP com SSL ativado. Você deve configurar os parâmetros a seguir conforme especificado:
   - **Autenticação do Usuário Necessária** é configurada para **Não**
   - **Usar SSL** é configurada para **Deve**
2. Implemente os arquivos WAR necessários na instância do adaptador para servidor HTTP com SSL ativado.

   Nota: Todos os arquivos WAR devem ser selecionados do diretório `/install_dir/install/noapp/deploy` durante a configuração da instância do adaptador para servidor HTTP. Além disso, o nome do contexto do aplicativo da web admin deve corresponder ao parâmetro ADMIN_CONTEXT_PATH no arquivo `/install_dir/install/properties/sandbox.cfg`. Para todos os outros aplicativos da web, o nome do contexto deve ser o nome do arquivo war sem a extensão ".war".

   Isso é necessário para que quaisquer mudanças feitas via uma correção ou hotfix sejam refletidas automaticamente na implementação do adaptador para servidor HTTP.

   Os arquivos WAR necessários incluem:

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

Arquivos WAR adicionais podem ser necessários para o suporte da nova funcionalidade incluída no Dashboard.

3. Abra o arquivo sandbox.cfg e modifique os seguintes parâmetros:

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

Esses parâmetros são usados pelo GPM para comunicação com o servidor.

4. (Opcional, Recomendado) Se quiser desativar a implementação dos aplicativos da web Dashboard e GPM na porta base, especifique os seguintes parâmetros em um arquivo customer_overrides.properties:

```
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

Por exemplo:

```
## Identifica os arquivos war a serem ignorados durante a implementação na porta base.
## Use uma lista separada por vírgula para especificar diversos wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica wars para redirecionamento automático para a porta https.
## Use uma lista separada por vírgula para especificar diversos wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifica a porta https para wars redirecionados.
## Se especificado, deve corresponder a WEBAPP_LIST_PORT em sandbox.cfg
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

5. Se você deseja usar um certificado diferente para essa funcionalidade, modifique `/install_dir/install/properties/customer_overrides.properties` para incluir a seguinte linha: *noapp.sslCert={mention_name_of_your_own_cert}*. Se você não especificar um certificado diferente, a funcionalidade usa ASISslCert.
6. (Opcional) Se você deseja enviar cookies a partir do navegador usando um protocolo seguro como HTTPS, navegue até `/install_dir/install/properties` e especifique o seguinte parâmetro em um arquivo customer_overrides.properties:

```
## enviando cookies como seguros sobre https
http.useSecureCookie=true
```

7. Navegue para `/install_dir/install/bin`.
8. Pare o Sterling B2B Integrator.
9. Aplique as mudanças de configuração. Insira `./setupfiles.sh`.
10. Implemente a nova configuração. Insira `./deployer.sh`.
11. Inicie o Sterling B2B Integrator.
12. 11. Verifique se o aplicativo da web Dashboard é acessível via o adaptador para servidor HTTP acessando https://host:<*secure_http_server_adapter_port*>/dashboard.
13. Verifique se o aplicativo da web GPM é acessível através do adaptador para Servidor HTTP seguro acessando https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp.
14. Salve e feche o arquivo.

15. Se você desligou a implementação dos aplicativos da web Dashboard e GPM na porta base (Etapa 4), verifique o seguinte:
    - O acesso ao aplicativo da web Dashboard em http://host:baseport/dashboard é redirecionado para https://host:<*secure_http_server_adapter_port*>/dashboard automaticamente.
    - O acesso ao aplicativo da web GPM em http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp é redirecionado para https://host:<*secure_http_server_adapter_port*>/gbm/pmodeler/ProcessModeler.jnlp automaticamente.

Alternar do Modo HTTPS para HTTP

Sobre Esta Tarefa

Para alternar do modo HTTPS para o HTTP:

Procedimento

1. Navegue até o `/install_dir/install/properties`.
2. Abra o arquivo **sandbox.cfg**.
3. Modifique os seguintes parâmetros:

   ```
   WEBAPP_PROTOCOL=http
   WEBAPP_LIST_PORT=<base_port>
   ```
4. Salve e feche o arquivo.
5. (Opcional) Se a implementação dos aplicativos da web Dashboard e GPM na porta base foi desativada durante a alternação para o modo HTTPS, você deverá abrir o arquivo customer_overrides.properties e comentar a linha dos seguintes parâmetros para que eles não sejam aplicados:

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

6. (Opcional) Salve e feche o arquivo.
7. Navegue para `/install_dir/install/bin`.
8. Pare o Sterling B2B Integrator.
9. Aplique as mudanças de configuração. Insira `./setupfiles.sh`.
10. Implemente a nova configuração. Insira `./deployer.sh`.
11. Inicie o Sterling B2B Integrator.
12. Verifique o seguinte:
    - O aplicativo da web Dashboard está acessível em http://host:baseport/dashboard
    - O aplicativo da web GPM está acessível em http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp
13. (Opcional) Remova a implementação dos aplicativos da web da instância do adaptador para servidor HTTP ativada por SSL.

Hardware Security Module (HSM)

Hardware Security Module (HSM)

HSM é um dispositivo de segurança baseado em hardware que gera, armazena e protege chaves criptográficas. É possível armazenar certificados do sistema em um banco de dados usando Sterling B2B Integrator ou no HSM.

Sterling B2B Integrator suporta os seguintes dispositivos HSM:

- SafeNet Eracom ProtectServer Orange External
- Dispositivos ProtectServer Gold PCI

É possível usar o HSM para:

- Criar certificados do sistema no HSM
- Importar certificados do sistema do Sterling B2B Integrator
- Exportar certificados do sistema do Sterling B2B Integrator
- Remover certificados do sistema do HSM
- Visualizar detalhes de certificado do sistema no HSM

Recursos do Sterling B2B Integrator para Suporte HSM

Uma entrada é armazenada na tabela CERTS_AND_PRI_KEY pelo Sterling B2B Integrator para cada par de chaves e certificado. Essa entrada contém informações sobre:

- Chaves e certificados, incluindo o período de validade, número de série, restrições de uso, emissor e assunto usados pela UI para exibir para o usuário sem a necessidade de realmente acessar a chave ou o certificado.
- Normalizações do nome distinto usado pelo sistema nas procuras.
- Modificações no registro.
- Informações de status da revogação de certificado.
- Tipo de keystore.
- Referências a um objeto de keystore binário armazenado em DATA_TABLE. Quando um keystore de software é usado, o objeto de referência pode conter o material chave. No caso de um HSM, ele contém informações de referência (nCipher) ou um marcador (Eracom).

Parâmetros do Certificado do Sistema HSM

A tabela a seguir fornece os parâmetros para os comandos CreateSystemCert, ImportSystemCert e ExportSystemCert.

Parâmetro	Descrição
autogen	Se você deve ou não usar as informações geradas pelo sistema para controlar o acesso à chave e ao keystore. Deve ser configurado como false para chaves em HSMs.
alias	O nome da chave armazenado no HSM. Somente nomes de alias contendo caracteres a-z, A-Z, 0-9 ou hífen (-) e cujo comprimento total não exceda o comprimento do GUID do sistema.
Certtype	O tipo de certificado para importar. Quatro tipos de arquivos de certificado são suportados: pkcs12, pkcs8, pem e keystore. Sterling B2B Integrator suporta apenas chaves pem criptografadas com DES ou 3DES. Use o keystore para listar ou importar o keystore.
certname	O nome para designar o certificado no banco de dados do Sterling B2B Integrator.
arquivo	Keycert ou arquivo PEM para importar.
keyname	O nome da chave do sistema do Sterling B2B Integrator para criar.

Parâmetro	Descrição
keypass	O PIN do token protegendo o SafeNet Eracom HSM onde o keystore reside.
passphrase de chave	O passphrase para a chave privada. Esse valor é opcional na linha de comandos. Se você não fornecê-lo, será solicitado que o forneça. O PIN para o token no SafeNet Eracom HSM onde o keystore reside.
keysize	O comprimento, em bits, do módulo RSA. Os valores válidos são 768, 1024, 2048, 3072 ou 4096
keystoretype	O tipo de keystore para importar. O valor válido é CRYPTOKI.
keystoreprovider	O tipo de provedor. SafeNet Eracom é o único HSM suportado. ERACOM ou ERACOM.n se você estiver importando certificados em um slot diferente do slot padrão 0.
keytype	O algoritmo de chave pública. RSA é o único algoritmo suportado.
ObjectID	O ID do certificado do sistema.
pkcs12file	O arquivo pkcs12 para importar.
password	Passphrase de armazenamento para o keycert ou arquivo PEM.
pkcs12storepass	Passphrase de armazenamento para o arquivo PKCS12.
pkcs12keypass	Passphrase de chave usado para criptografar a chave privada no arquivo PKCS12.
provedor	O provedor do tipo de keystore. ERACOM ou ERACOM.n se você estiver importando certificados em um slot diferente do slot padrão 0.
rfc1779rdnsequence	O campo de sequência de nome distinto contém qualquer um dos campos identificados na coluna Valores Válidos. Apenas o campo CN é obrigatório. Separe cada campo com uma vírgula. Informações válidas: • CN = Nome Comum • O = Organização • OU = Unidade de Organização • L = Local • ST = Estado • C = País (forneça um código alfa 2 de duas letras ISO3166-1)
storetype	O tipo de keystore. CRYPTOKI é o único tipo de keystore suportado.
signingbit	Configura o bit de uso de chave de sinal para o certificado autoassinado. Os valores válidos são true ou false.
serial	O número de série do certificado.
passphrase do sistema	A passphrase do sistema Sterling B2B Integrator. Esse valor é opcional na linha de comandos.
passphrase de armazenamento	O passphrase para acessar o keystore. O PIN para o token no SafeNet Eracom HSM onde o keystore reside. Esse valor é opcional na linha de comandos.
systempass	A passphrase do sistema Sterling B2B Integrator.
storepass	O PIN do token protegendo o SafeNet Eracom HSM onde o keystore reside.
totrusttable	Determina se o certificado é incluído na tabela de certificados confiável. Os valores válidos são true ou false.

Parâmetro	Descrição
validityindays	Duração do tempo em dias em que o certificado é válido.

SafeNet Eracom HSM

Antes de poder usar o HSM com Sterling B2B Integrator, você deve configurar o Sterling B2B Integrator para usar e reconhecer o SafeNet Eracom HSM. Para instalar e configurar o SafeNet Eracom HSM, siga as instruções fornecidas pelo fornecedor; assegure-se de instalar o Java Runtime. Use o provedor para o slot no qual as chaves do Sterling B2B Integrator serão armazenadas quando você configurar e usar os utilitários. Após criar um PIN para o slot do SafeNet Eracom, não altere o PIN. O Sterling B2B Integrator não poderá acessar uma chave do HSM se você alterar o PIN.

A arquitetura SafeNet Eracom divide o HSM em diversos slots. Instale e configure placas ou HSMs de acordo com as instruções do fornecedor. Cada slot tem um provedor de segurança associado e pode ser protegido por um Número de Identificação Pessoal (PIN) separado. É possível criar um slot separado no HSM para Sterling B2B Integrator e proteger o slot com um PIN exclusivo. O provedor para o slot padrão 0 é ERACOM. Os provedores para slots adicionais são denominados ERACOM.*n*, em que *n* é o número do slot. Assegure-se de que os componentes do Java Runtime estejam disponíveis para interagirem com o dispositivo.

Configurar Sterling B2B Integrator para Usar SafeNet Eracom HSM

Sobre Esta Tarefa

Para configurar o Sterling B2B Integrator para usar o HSM do SafeNet Eracom:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Inclua as seguintes linhas nos arquivos tmp.sh e tmp.sh.in:

   ```
   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib
   export LD_LIBRARY_PATH
   ```
3. Se você estiver configurando um servidor baseado em rede, inclua as seguintes linhas nos arquivos tmp.sh e tmp.sh.in, em que *network_device_IP_OR_hostname* é o endereço IP ou o nome completo do domínio do servidor baseado em rede SafeNet Eracom:

   ```
   ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
   export ET_HSM_NETCLIENT_SERVERLIST
   ```
4. Copie jprov.jar do diretório /opt/Eracom/lib no diretório */install_dir*/install/jdk/jre/lib/ext.
5. Inclua uma definição para cada provedor de segurança no arquivo */install_dir*/install/bin/jdk/jre/lib/security/java.security. Para incluir uma definição, identifique o número designado ao provedor Certicom e designe n+1 ao provedor SafeNet Eracom. Para todos os outros provedores identificados após o provedor SafeNet Eracom, aumente o número do security.provider em 1.

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

   Se estiver usando um slot diferente de 0 no SafeNet Eracom HSM, especifique o slot da seguinte forma, em que *x* é o número do slot:

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

6. Defina TLSProviderPolicy no arquivo */install_dir*/install/properties/security.properties.
   - Se o provedor estiver definido no slot 0, assegure-se de que a única linha não comentada para o parâmetro TLSProviderPolicy será a seguinte:

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

   - Se o provedor estiver definido em um slot diferente de 0, modifique o parâmetro TLSProviderPolicy da seguinte forma, em que *x* é o slot que você está configurando:

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

7. Defina o comando KeyStoreProviderKey no arquivo */install_dir*/install/properties/security.properties:
   - Se o provedor estiver definido no slot 0, assegure-se de que KeyStoreProviderMap esteja definido como:

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

   - Se o provedor estiver definido em qualquer slot diferente de 0, modifique o parâmetro KeyStoreProviderMap da seguinte forma, em que *x* é o número do slot:

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

nCipher e SafeNet/Eracom Network e Dispositivos PCI Suportados

Sterling B2B Integrator suporta atualmente placa PCI Safenet/Eracom ProtectServer Orange e dispositivo de rede Orange External, além de nCipher.

As opções a seguir são suportadas:

Fabricante	Tipos de Dispositivos Suportados
nCipher	• Série nShield de placas PCI • Dispositivos de rede NetHSM
Safenet/Eracom	• Placa PCI ProtectServer Gold • Placa PCI ProtectServer Orange • Dispositivo de rede ProtectServer Orange External

Usar Hardware Security Module

Criar Certificados do Sistema para Armazenar no HSM

Antes de Iniciar

Antes de iniciar:

- Pare o Sterling B2B Integrator.

- Assegure-se de que o banco de dados do Sterling B2B Integrator esteja em execução.

Sobre Esta Tarefa

Para criar um certificado do sistema autoassinado para armazenar no HSM:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira: `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase]  [store passphrase] [key passphrase]`
3. Se você não forneceu o passphrase do sistema, passphrase do armazenamento e passphrase de chave na linha de comandos, será solicitado que você os digite.

Listar Certificados do Sistema Armazenados no HSM

Sobre Esta Tarefa

Para listar informações sobre certificados do sistema armazenados no HSM:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

Exemplo

A seguir está um exemplo de saída de comando:

```
Key exists with alias rayado-e5305c3-10d8f4bde7f--7fc1
Certificate Subject Info CN=test, OU=test, O=test, L=test, ST=Alabama, C=US
Certificate Issuer Info CN=Pythagoras, OU=System Verification, O=Sterling, L=Dublin,
ST=OH, C=US, EMAILADDRESS=caussuer@company.com
```

Importar Certificado do Sistema HSM no Banco de Dados do Sterling B2B Integrator

Sobre Esta Tarefa

Use este procedimento quando uma chave e um certificado já existirem no HSM e tiverem sido incluídos no HSM independentemente do Sterling B2B Integrator. Você deve importar as informações para um certificado do sistema armazenado em um HSM para o banco de dados antes que ele possa ser usado pelo Sterling B2B Integrator.

Dependendo do método usado para incluir a chave privada e o certificado no HSM, a função listar pode exibir entradas duplicadas para um único par de chaves e certificados.

Você deve obter o alias de certificado do sistema antes de poder importar informações sobre um certificado do sistema no banco de dados.

Para importar o certificado do sistema:

Procedimento

1. Navegue para */install_dir*/install/bin.

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

Remover Certificados do Sistema Armazenados no HSM

Sobre Esta Tarefa

Este procedimento exclui permanentemente o certificado do sistema do HSM. Os dados da chave privada que ele contém não podem ser recuperados.

Para remover um certificado do sistema armazenado no HSM:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira: `./RemoveSystemCert.sh -r` *xxxx*

   Em que *xxxx* é o ID do objeto do certificado que deseja remover.

Exportação de Certificados do Sistema

Sobre Esta Tarefa

Certificados do sistema em um HSM não podem ser exportados usando ExportSystemCert.sh.

Para exportar certificados do sistema do Sterling B2B Integrator para que eles possam ser importados no HSM:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Insira a sua passphrase.

Exemplo: Certificado do Sistema HSM

É possível importar um certificado do sistema para o HSM em formato keycert, pkcs12 ou pem. A importação de um certificado do sistema inclui a chave e o certificado no HSM e cria uma entrada correspondente no banco de dados do Sterling B2B Integrator. Se você importar um certificado do tipo pem e uma chave, certifique-se de que a chave privada seja criada no formato criptografado DES- ou triple-DES.

A seguir há uma amostra de chave privada pem criada em formato triple-DES:

```
-----INÍCIO DA CHAVE PRIVADA RSA-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6EROcbo8fMXnMaRM/JcKIc3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sdllKpnIXYg63Y+egn8DsxdGUCqnC+HDUlRVHX0NWKJ3FwXukr9iN
WP4MBr+NXMSETaBA0O0B4oSRCWvxelc2U2GItvUqJsOjLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+bOwFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraBl1cmJ3vL
0RTnkwZnnyJ1Brc/WynlVfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAy5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF4OXL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilpqVsYSt1g6
lO805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+4O8sGqHA1zMwuqErorUvwxD6ZNnlc
DTmKIt826oows4Gtw48aEwjV4lk8FXQsWQjDWJHjFNNvGiyszPJjvPvM8zL1EwxO
```

```
mJFeNxBb0U3zgLs5aK/HHRn1/gzOBHwtr8bdFFBkpLoVGnbW+mRVxmJOvvPe7Zo+
sJXLEWC8Bm4klV8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHabk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEIlIQ==
-----FIM DA CHAVE PRIVADA RSA-----
```

Gerenciar Utilitários de Certificado do Sistema

Pares de Chaves do HSM e Certificate Signing Requests

O utilitário GenCSR gera um par de chaves em um HSM e cria um Certificate Signing Request (CSR) PKCS10 com a chave pública desse par de chaves. É possível enviar o CSR para uma Autoridade de Certificação (CA). Quando você receber um certificado emitido pela CA, use GenCSR para atualizar o certificado. O certificado do sistema não fica disponível no Sterling B2B Integrator até ser atualizado com o certificado emitido pela CA.

Também é possível usar esse utilitário para visualizar uma lista de CSRs, gravar informações sobre um CSR para um arquivo, excluir um CSR ou gravar informações sobre um certificado emitido pela CA armazenado no HSM para um arquivo. Informações sobre CSRs são mantidas no banco de dados do Sterling B2B Integrator, enquanto que as chaves reais são armazenadas no HSM.

Para usar o utilitário, primeiro determine qual ação deseja executar. Em seguida, use o utilitário GenCSR e identifique a ação na linha de comandos. Para cada ação, forneça os argumentos necessários para a ação no arquivo de propriedades. Um arquivo de propriedades de amostra chamado csr.properties.sample é fornecido no diretório */install_dir*/install/properties.

O utilitário GenCSR pode ser localizado no diretório */install_dir*/install/bin.

A sintaxe do comando é: `GenCSR.sh -a ACTION -p PROPERTIES`

Parâmetros GenCSR

A tabela a seguir fornece os parâmetros usados durante a execução do script GenCSR:

Parâmetro	Descrição	Valores Válidos
-a ACTION	A ação a ser executada.	As ações válidas são: • CREATE • UPDATE • LIST • DELETE • GETPCKS10 • GETCACERT
-p PROPERTIES	O arquivo de propriedades que contém parâmetros adicionais necessários para as ações. Você precisa incluir o caminho para o arquivo de propriedades.	Nome do arquivo de propriedades. Por exemplo: `csr_create.properties`

Atualizar Keystore HSM com Certificados Emitidos pela CA

Sobre Esta Tarefa

Use o utilitário GenCSR com o argumento de atualização para incluir informações de certificado emitido pela CA no keystore HSM.

Procedimento

1. Assegure-se de que o arquivo csr_update.properties esteja configurado corretamente.

   A tabela a seguir descreve os parâmetros necessários no arquivo csr_update.properties para o argumento de atualização.

Parâmetro	Descrição	Valores Válidos
provedor	Nome do provedor de keystore.	ERACOM ou ERACOM.n
keystoretype	Nome do keystore usado.	CRYPTOKI
certificate.request.Name	Nome do CSR para atualizar.	Nome designado a um CSR
add.trusted	Identifica se as informações de certificado são incluídas na tabela de certificado confiável.	True | false
ca.cert.file	Caminho e nome do arquivo no qual gravar informações sobre o certificado emitido pela CA.	O nome do arquivo e o caminho válidos de um arquivo de certificado emitido pela CA

2. Atualize o keystore HSM.

   A sintaxe de comando é: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

Listar Certificate Signing Requests

Sobre Esta Tarefa

Use o utilitário GenCSR com o argumento de lista para exibir CSRs no banco de dados do HSM. Nenhuma configuração de arquivo de propriedades é necessária para o argumento de lista.

A sintaxe de comando é: `./GenCSR.sh -a list`

Excluir uma Solicitação de Assinatura de Certificado

Sobre Esta Tarefa

Use o utilitário GenCSR com o argumento de exclusão para excluir um CSR. Esse utilitário exclui apenas o CSR. Ele não exclui certificados do sistema que são atualizados com um certificado emitido por CA.

Procedimento

1. Assegure-se de que o arquivo cacert.properties esteja configurado corretamente. Você deve configurar o arquivo de propriedades antes de usar o argumento de exclusão. A tabela a seguir descreve os parâmetros necessários no arquivo cacert.properties para o argumento de exclusão.

Parâmetro	Descrição	Valores Válidos
certificate.request.Name	Nome do CSR para excluir.	Nome de um CSR
keystoretype	Nome do keystore usado.	CRYPTOKI
provedor	Nome do provedor de keystore.	ERACOM[.N]

2. Exclua o CSR. A sintaxe de comando é `./GenCSR.sh -a delete -p ../properties/cacert.properties`

Gravar Informações de CSR em um Formato pkcs10

Sobre Esta Tarefa

Use o utilitário GenCSR com o argumento getpkcs10 para gravar um CSR em formato pkcs10 no arquivo especificado.

Procedimento

1. Assegure-se de que o arquivo csr_getpkcs10.properties esteja configurado corretamente.

   A tabela a seguir descreve os parâmetros necessários no arquivo csr_getpkcs10.properties para o argumento getpkcs10. Você deve configurar o arquivo de propriedades antes de usar o argumento getpkcs10.

Parâmetro	Descrição	Valores Válidos
certificate.request.Name	Nome do CSR.	Nome designado a um CSR
keystoretype	Nome do keystore usado.	CRYPTOKI
csr.file	Caminho completo para o arquivo no qual gravar informações sobre o CSR.	Caminho e nome do arquivo no qual gravar informações do CSR

2. Grave o CSR em um arquivo.

   A sintaxe de comando é `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

Mover Certificados do Sistema para o HSM

Sobre Esta Tarefa

É mais seguro gerar novamente chaves e certificados usando CreateSystemCert.sh ou GenCSR.sh.

Para mover certificados autoassinados ou certificados emitidos pela CA do banco de dados para o HSM:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Pare o Sterling B2B Integrator.
3. Inicie o banco de dados.
4. Exporte o certificado do sistema para um arquivo PKCS12:

   `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
5. Localize o ID do objeto do certificado do sistema a ser removido. Insira:

   `./RemoveSystemCert.sh -l.`
6. Remova o certificado do sistema do banco de dados. Insira:

   `RemoveSystemCert.sh -r` *xxxx*, em que *xxxx* é o ID do objeto do certificado que deseja remover.
7. Para importar o certificado do sistema que você exportou para o HSM e criar uma entrada de banco de dados correspondente:

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

Nota: Se você mover OpsDrv, OpsKey e UIKey para o HSM, use o nome exato. Caso contrário, o Sterling B2B Integrator não funcionará corretamente. Para todos os outros certificados do sistema, o nome não é crítico. Quando você move os certificados do sistema diferentes de OpsDrv, OpsKey e UIKey, o ID do objeto que é usado por serviços e adaptadores muda. Reconfigure quaisquer serviços que usem os certificados do sistema que foram movidos.

Gravar Certificado Emitido pela CA em um Arquivo

Sobre Esta Tarefa

Use o utilitário GenCSR com o argumento getcacert para gravar o certificado emitido pela CA em um arquivo.

Procedimento

1. Assegure-se de que o arquivo getcacert.properties esteja configurado corretamente.

   A tabela a seguir descreve os parâmetros necessários no arquivo getcacert.properties para a ação getcacert. Você deve configurar o arquivo getcacert.properties antes de usar o argumento getcacert.

Parâmetro	Descrição	Valores Válidos
certificate.request.Name	Nome do CSR.	Nome do certificado
keystoretype	Nome do keystore usado.	CRYPTOKI
ca.cert.file	Caminho completo para o arquivo no qual gravar informações sobre o certificado de CA.	Nome e caminho de um arquivo de certificado de CA

2. Grave o certificado em um arquivo.

   A sintaxe de comando é `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

Gerar Certificados do Sistema Interno (OpsDrv, OpsKey, UIKey) no HSM

Sobre Esta Tarefa

Há três certificados do sistema instalados com o Sterling B2B Integrator para proteger operações internas. Pouco benefício de segurança é fornecido com sua mudança para o HSM. Sua política de segurança pode requerer que todos os certificados que contêm chaves privadas sejam armazenados em HSM. Ao gerar os certificados do sistema interno Sterling B2B Integrator chamados OpsDrv, OpsKey e UIKey no HSM, use os nomes exatos. Caso contrário, o Sterling B2B Integrator não funcionará corretamente.

Para gerar certificados do sistema interno:

Procedimento

1. Navegue para */install_dir*/install/bin.
2. Insira `./RemoveSystemCert.sh -l` para visualizar certificados no banco de dados. Observe o ID do objeto para cada certificado do sistema.

3. Para excluir os certificados do sistema do banco de dados executando o seguinte comando para cada certificado: `./RemoveSystemCert.sh -r xxxx`, em que *xxxx* é o ID do objeto do certificado que deseja remover.
4. Gere o certificado do sistema no HSM para cada certificado; insira:

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

Usar nCipher e SafeNetEracom

Mapa do Provedor de Armazenamento de Chaves

Como o Sterling B2B Integrator possui o tipo de keystore que é exclusivo em provedores de serviços criptográficos, é possível definir um mapeamento entre os tipos de keystore e os provedores necessários para implementar o objeto keystore em si, algoritmos de assinatura e algoritmos de transporte de chaves.

A chave e o objeto de abstração de informações chave contêm essas informações com uma referência a um com.sterlingcommerce.security.PrivateKeyInfo.

Isso permite que o Sterling B2B Integrator use uma combinação de chaves em HSMs e em armazenamentos de software no banco de dados ao mesmo tempo, sem configuração adicional além do carregamento inicial da chave ou informações chave no banco de dados. Para o Sterling B2B Integrator, todas as chaves são iguais, independentemente de onde são armazenadas.

O mapeamento é implementado como uma propriedade denominada KeyStoreProviderMap em security.properties. Ele consiste em um conjunto de entradas delimitadas por pontos e vírgulas (;). Cada entrada possui seis elementos delimitados por vírgulas e segue este formato:

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

Os elementos são descritas na tabela a seguir:

Elemento	Descrição	Informações Adicionais
KeyStoreType	O tipo de sequência do keystore	
KeyStoreProvider	O nome do provedor de serviços criptográficos que implementa o keystore	
DoesAliasMatter	Se o alias das chaves deve ser exclusivo para esse tipo de keystore	Pode ser true ou false. Chaves precisam ter alias exclusivos no caso de haver apenas um keystore por dispositivo.
SignatureProvider	O nome do provedor de serviços de criptografia a ser usado para criar assinaturas usando chaves do keystore	
EncryptionProvider	O nome do provedor de serviços de criptografia a ser usado na decriptografia de informações usando chaves no keystore	Isso é principalmente para operações de transporte de chave RSA

Elemento	Descrição	Informações Adicionais
KeyOnHSM	Se o keystore está em um HSM	

A sequência nula é um valor aceitável e será tratada como se nenhum provedor tivesse sido especificado. Uma entrada deve ter pelo menos dois valores. Se uma entrada contiver menos de seis valores, os valores serão designados da esquerda para a direita para o provedor de keystore, se o alias for importante durante o armazenamento da chave, provedor de assinatura, provedor de criptografia e se a chave estiver em um HSM para o tipo KeyStore. Os outros serão tratados como nulos e nenhum provedor específico será solicitado para operações com chaves desse tipo.

O KeyStoreProviderMap padrão é atualmente:

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

Gerenciar Chaves HSM e Informações Chave

Sterling B2B Integrator tem vários scripts java para gerenciar chaves no HSMs. Os programas java são listados abaixo.

Programa	Propósito
com.sterlingcommerce.db.RemoveSystemCert	Ambos listam e excluem os certificados do sistema Sterling B2B Integrator. Durante uma exclusão, o programa faz o melhor esforço para limpar a chave do keystore e sobrescrever o objeto keystore no banco de dados.
com.sterlingcommerce.db.CreateCertEx	Gera um par de chaves em um HSM e um certificado autoassinado contendo a chave pública do par de chaves.
com.sterlingcommerce.security.util. CertificateSigningRequest	Gera um par de chaves em um HSM e cria e gerencia um Certificate Signing Request PKCS10 associado. O PKCS10 pode ser fornecido para uma autoridade para obter um certificado assinado pela autoridade. Esse programa pode ser usado para carregar esse certificado no keystore e associá-lo ao par de chaves certo.
com.sterlingcommerce.db.ImportSystemCert	Importe uma chave privada e um certificado em um formato suportado (PKCS12 ou PEM) em um keystore em um HSM. Importe informações sobre uma chave privada e um certificado em um HSM no banco de dados do Sterling B2B Integrator.

Mudanças de JDK para Suporte ao nCipher HSM

Para o Sterling B2B Integrator utilizar nCipher HSMs, você deve instalar os provedores de serviços criptográficos Java nCipher. Para instalar, copie os arquivos jar a seguir no subdiretório jre/lib/ext do JDK. Modifique java.security para carregar os provedores de nCipher.

Os seguintes arquivos são colocados em /opt/nfast/java/classes pelo programa de instalação nCipher:

- rsaprivenc.jar
- nfjava.jar
- kmjava.jar

- jutils.jar
- kmcsp.jar

É necessário incluir provedores nCipher depois do provedor IBM JCE e antes do provedor Certicom. Exemplo:

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.3=com.ncipher.provider.km.nCipherKM
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.ibm.jsse2.IBMJSSEProvider2
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
```

Em sistemas Solaris com o SUN JDK, você deve colocar os provedores nCipher depois dos provedores Sun JCS e JCE e antes do provedor Certicom. Exemplo:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=com.ncipher.fixup.provider.nCipherRSAPrivateEncrypt
security.provider.4=com.ncipher.provider.km.nCipherKM
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=com.sun.net.ssl.internal.ssl.Provider
security.provider.7=com.sun.rsajca.Provider
security.provider.8=sun.security.jgss.SunProvider
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
```

Configure uma política TLSProvider usando a amostra em security.properties. Exemplo:

```
TLSProviderPolicy=TLS:MD:MD5:P:Certicom;TLS:MD:SHA1:P:Certicom;TLS:MAC:HmacMD5:P:Certicom;
TLS:MAC:HmacSHA1:P:Certicom;TLS:SIG:MD2withRSA:P:Certicom;TLS:Cipher:RawRSA:P:Certicom;
TLS:*:ECDH:P:Certicom;TLS:*:ECDSA:P:Certicom;TLS:*:*:P:nCipherKM
```

Mudanças de JDK para Suporte ao Eracom HSM

Para o Sterling B2B Integrator utilizar Eracom HSMs, você deve instalar o provedor de serviços criptográficos Java Eracom. Para instalar, coloque os arquivos appropriate.jar no subdiretório jre/lib/ext do JDK e depois modifique o java.security para carregar os provedores de nCipher.

Esses arquivos são colocados em /opt/nfast/java/classes pelo programa de instalação nCipher:

- jcprov.jar
- jprov.jar

Você deve incluir o provedor Eracom depois do provedor Certicom. Exemplo:

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.certicom.ecc.jcae.Certicom
security.provider.3=au.com.eracom.crypto.provider.ERACOMProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.8=com.sterlingcommerce.security.provider.SCI
```

Nota: Eracom tem um provedor que pode ser especificado para cada slot na placa. Para o provedor para o slot 8, use:

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

Mudanças de Ambiente do Linux para Suporte a nCipher HSM

nCipher recomenda que você crie uma conta do usuário especial para execução do hardserver nCipher. A conta a partir do qual você executa o Sterling B2B Integrator precisa ter permissões equivalentes ou você precisará executar o Sterling B2B Integrator a partir da conta especial nCipher ou como raiz. Se escolher uma dessas opções e estiver usando MySQL, você deverá alterar as permissões para MySQL ou iniciar MySQL a partir de sua conta normal antes de chamar run.sh.

Mudanças de Ambiente do Linux para Suporte a Eracom HSM

Para usar o dispositivo Eracom, você deve fornecer informações adicionais nas variáveis de ambiente para a sessão que irá acessar o dispositivo. As mudanças recomendadas para PATH, LD_LIBRARY_PATH e MANPATH são como a seguir:

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

Além disso, se estiver usando um dispositivo de rede em vez de uma placa PCI local, você deverá fornecer ET_HSM_NETCLIENT_SERVERLIST, como a seguir:

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

Você deve exportar essas variáveis em tmp.sh.

Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos. Este material pode estar disponível na IBM em outros idiomas. No entanto, pode ser necessário que você possua uma cópia do produto ou da versão do produto nesse idioma para que seja possível acessá-lo.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. 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, a avaliação e verificação da operação de qualquer produto, programa ou serviço não IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. 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

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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 A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS (OU CONDIÇÕES) DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Estas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras 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 esses Web sites. Referências nestas informações à documentação ou a Web sites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses documentos ou Web sites.

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 independentemente 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

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

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

Os dados de desempenho e os exemplos de cliente citados somente são apresentados com propósito ilustrativo. Os resultados de desempenho reais podem variar dependendo de configurações e condições operacionais específicas.

As informações relativas a produtos não IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou 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.

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.

Todos os preços IBM mostrados são preços de varejo sugeridos pela IBM, são atuais e estão sujeitos à alteração sem aviso prévio. Os preços do revendedor podem variar.

Estas informações foram projetadas apenas com o propósito de planejamento. As informações aqui contidas estão sujeitas a alterações antes que os produtos descritos estejam disponíveis.

Estas informações contêm exemplos de dados e relatórios utilizados nas operações diárias de negócios. Para ilustrá-los da forma mais completa possível, os exemplos podem incluir nomes de indivíduos, empresas, marcas e produtos. Todos estes nomes são fictícios e qualquer semelhança com nomes e endereços utilizados por uma empresa real é mera coincidência.

LICENÇA DE COPYRIGHT:

Estas informações contêm programas de aplicativos de amostra na linguagem fonte, ilustrando as técnicas de programação em diversas plataformas operacionais. O Cliente pode copiar, modificar e distribuir estes programas de amostra 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 amostra são criados. Esses exemplos não foram testados completamente em todas as condições. Portanto, a IBM não pode garantir ou implicar a confiabilidade, manutenção ou função destes programas. Os programas de amostra são fornecidos "NO ESTADO EM QUE SE ENCONTRAM", sem garantia de nenhum tipo. A IBM não poderá ser responsabilizada por nenhum dano derivado do uso de programas de amostra.

Cada cópia ou parte destes programas de amostra ou qualquer trabalho derivado deve incluir um aviso de copyright com os dizeres.

Marcas Registradas

IBM, o logotipo IBM e ibm.com são marcas ou marcas registradas da International Business Machines Corp., registradas em vários países no mundo todo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Uma lista atual das marcas comerciais da IBM está disponível na web em "Copyright and trademark information" em www.ibm.com/legal/copytrade.shtml.

Adobe, o logotipo Adobe, PostScript e o logotipo PostScript são marcas ou marcas registradas da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

IT Infrastructure Library é uma marca registrada da Agência Central de Computação e Telecomunicações que agora é parte do Departamento de Comércio do Governo.

Intel, o logotipo Intel, Intel Inside, o logotipo Intel Inside, Intel Centrino, o logotipo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium e Pentium são marcas ou marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos e em outros países.

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

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

ITIL é uma marca registrada e uma marca registrada da comunidade do Departamento de Comércio do Governo e está registrada no Departamento de Marcas e Patentes dos Estados Unidos.

UNIX é uma marca registrada do The Open Group nos Estados Unidos e em outros países.

Java™ e todas as marcas registradas e logotipos baseados em Java são marcas ou marcas registradas da Oracle e/ou de suas afiliadas.

Cell Broadband Engine é uma marca registrada da Sony Computer Entertainment, Inc. nos Estados Unidos e/ou em outros países e são usadas sob licença a partir deste ponto.

Linear Tape-Open, LTO, o logotipo LTO, Ultrium e o logotipo Ultrium são marcas registradas da HP, IBM Corp. e Quantum nos Estados Unidos e em outros países.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker® e Sterling Integrator® são marcas ou marcas registradas da Sterling Commerce, Inc., uma Empresa IBM.

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

Termos e condições da documentação do produto

As permissões de uso destas publicações são concedidas estando sujeitas aos seguintes termos e condições.

Aplicabilidade

Esses termos e condições somam-se a quaisquer termos de uso do website IBM.

Uso pessoal

É possível reproduzir estas publicações para uso pessoal, não comercial, desde que todos os avisos do proprietário sejam preservados. Não é possível distribuir, exibir ou fazer trabalho derivado destas publicações ou de qualquer parte delas, sem o consentimento expresso da IBM.

Uso comercial

Somente é possível reproduzir, distribuir e exibir estas publicações dentro da empresa do cliente, desde que todos os avisos do proprietário sejam preservados. Não é possível fazer trabalhos derivados destas publicações ou reproduzir, distribuir ou exibir estas publicações ou qualquer parte delas fora da empresa do cliente, sem o consentimento expresso da IBM.

Direitos

Com exceção daquilo que é concedido expressamente nesta permissão, nenhuma outra permissão, licença ou direito é concedido, de forma expressa ou implícita, para as publicações ou quaisquer informações, dados, softwares ou outra propriedade intelectual contida nelas.

A IBM reserva o direito de retirar as permissões concedidas neste documento sempre que, a seu critério, o uso das publicações for prejudicial aos seus interesses ou, conforme determinação da IBM, as instruções acima não forem seguidas da forma adequada.

Não é possível fazer download, exportar ou exportar novamente, exceto quando em total conformidade com todas as leis e regulamentações aplicáveis, incluindo todas as leis e regulamentações de exportação dos Estados Unidos.

A IBM NÃO GARANTE O CONTEÚDO DESTAS PUBLICAÇÕES. AS PUBLICAÇÕES SÃO FORNECIDAS "NO ESTADO EM QUE SE ENCONTRAM" E SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE, NÃO INFRAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO.

Número do Programa:

Impresso no Brasil