

Sterling B2B Integrator

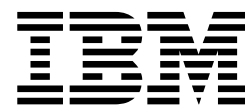


# Security (V5.2.3 or later)

*Version 5.2.3*



Sterling B2B Integrator



# Security (V5.2.3 or later)

*Version 5.2.3*

**Note**

Before using this information and the product it supports, read the information in "Notices" on page 131.

**Copyright**

This edition applies to Version 5 Release 2 Modification 3 of Sterling B2B Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2000, 2015.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

## Security (V5.2.3 or later). . . . . 1

Role Based Security . . . . .	1
Role-Based Security Overview . . . . .	1
Groups . . . . .	2
Permissions. . . . .	5
User Accounts . . . . .	20
Single Sign On . . . . .	27
Single Sign On . . . . .	27
Single Sign On Provider Default Class . . . . .	27
Single Sign On Plug-in Components . . . . .	29
Single Sign On with Netegrity SiteMinder Checklist . . . . .	31
Single Sign On with IBM Global High Availability Mailbox (V5.2.6 or later) . . . . .	31
Configure Properties Files for Single Sign On with Netegrity SiteMinder . . . . .	32
Configure Netegrity Secure Proxy Server . . . . .	34
Create Netegrity Policy Server Secure Realms . . . . .	35
Passwords. . . . .	36
Password Policies . . . . .	36
Custom Password Policy . . . . .	37
Example: Password Policy Example . . . . .	37
Installation Password or Passphrase . . . . .	38
Custom Policy Password Checklist . . . . .	38
Example - Custom Policy Password . . . . .	38
Search for Password Policies. . . . .	39
Create Password Policies . . . . .	40
Edit Password Policies. . . . .	41
Delete Password Policies . . . . .	41
Change the Number of Days for User Password Expiration . . . . .	42
Reset Your Own Password After Lockout . . . . .	42
Define Error Message for Custom Password Policy . . . . .	42
Specify the Custom Password Policy Extension in the customer_overrides.property file . . . . .	43
Add the Implementation class JAR to the Classpath for the Custom Password Policy . . . . .	43
LDAP Authentication . . . . .	44
Lightweight Directory Access Protocol (LDAP) as an Authentication Tool for Sterling B2B Integrator . . . . .	44
Example: LDAP Authentication Configuration Parameters . . . . .	45
LDAP Authentication Configuration Checklist. . . . .	46
Configure LDAP in Password Binding Mode . . . . .	46
Configure LDAP in Password Comparison Mode . . . . .	46
Configure LDAP with Sterling B2B Integrator . . . . .	47
Verify LDAP Configuration . . . . .	49
Encrypt LDAP Passwords . . . . .	50
User News . . . . .	51
User News . . . . .	51
Create User News Messages for All Users . . . . .	51
Create User News Messages for Specific Users . . . . .	52
Search for User News Messages . . . . .	52
Edit User News Messages . . . . .	53
Delete User News Messages . . . . .	53

Document Encryption . . . . .	54
Document Encryption Feature Overview . . . . .	54
Encryption Key for Document Encryption . . . . .	54
Assign a Different Certificate for Document Encryption . . . . .	55
Enable Document Encryption for File System and Database Documents . . . . .	55
Enable Document Encryption for Database Documents . . . . .	55
Enable Document Encryption for File System Documents . . . . .	56
Disable Document Encryption for Documents . . . . .	56
Certificates . . . . .	57
Digital Certificates . . . . .	57
CA Certificates . . . . .	57
Benefits of Self-signed and CA-signed Digital Certificates . . . . .	58
Expiration Dates for Certificates . . . . .	59
System Certificate Parameter Definitions. . . . .	59
IBM Key Management Utility (iKeyman) . . . . .	59
Certificate Tasks . . . . .	60
Online Certificate Status Protocol (OCSP) . . . . .	75
Federal Information Processing Standards (FIPS) . . . . .	84
Federal Information Processing Standards (FIPS) 140-2 . . . . .	84
FIPS 140-2 with Sterling B2B Integrator . . . . .	84
Enable FIPS During Installation. . . . .	84
Enable FIPS Mode Manually. . . . .	85
Disable FIPS Mode . . . . .	85
Proxy Servers. . . . .	85
Proxy Servers. . . . .	85
Configure HTTP Proxy Server . . . . .	85
Configure SSP Proxy Server . . . . .	86
Configure a Proxy Server for SSL . . . . .	87
Edit Proxy Servers . . . . .	87
Delete Proxy Servers . . . . .	87
SSL . . . . .	87
About Implementing SSL in Sterling B2B Integrator . . . . .	87
Client Adapters for SSL . . . . .	89
Server Adapters for SSL . . . . .	89
Check in a Certificate . . . . .	90
Create Self-Signed Certificates for Testing . . . . .	90
SSL/TLS renegotiation (V5.2.6 or later) . . . . .	90
Troubleshoot SSL . . . . .	92
HTTPS Configuration for the GPM . . . . .	94
New SSL Parameters . . . . .	94
HTTPS Support for the GPM . . . . .	98
Switch from HTTP to HTTPS Using the Base SSL Port . . . . .	98
Switch from HTTP to HTTPS Mode Using a Secure HTTP Server Adapter . . . . .	99
Switch from HTTPS to HTTP Mode . . . . .	101
Hardware Security Module (HSM) V5.2.3 - 5.2.5 . . . . .	102
Hardware Security Module (HSM) . . . . .	102

Sterling B2B Integrator Features for HSM	
Support . . . . .	102
HSM System Certificate Parameters . . . . .	102
SafeNet Eracom HSM . . . . .	104
Use a Hardware Security Module . . . . .	106
Manage System Certificate Utilities . . . . .	108
Use nCipher and SafeNetEracom . . . . .	112
Hardware Security Module (HSM) V5.2.6 or Later	115
Hardware Security Module (HSM) . . . . .	115
Sterling B2B Integrator Features for HSM	
Support . . . . .	116

HSM System Certificate Parameters . . . . .	116
Use a Hardware Security Module. . . . .	117
Manage System Certificate Utilities . . . . .	120
Configure nCipher and SafeNet Luna Devices	124
Configure HSM using IBM PKCS11IMPLKS	
(V5.2.6.2 or Later) . . . . .	127
<b>Notices . . . . .</b>	<b>131</b>
Trademarks . . . . .	133
Terms and conditions for product documentation	134

---

## Security (V5.2.3 or later)

Sterling B2B Integrator uses a variety of security mechanisms, including system passwords for administrative functions, password policies based on your company's security policies, and role-based security to provide different levels of access to different users within the organization.

The following security features are provided with Sterling B2B Integrator:

- Role-based security provides users access to files, business processes, Web templates, services, and product features, according to the permissions associated with the user account.
- Password policies are sets of security decisions that you make and apply to different user accounts according to security policies in your company. These choices include such items as the number of days a password is valid and the maximum and minimum length of a password.
- LDAP authentication can be used to delegate authentication of an external user account to an LDAP directory and to provide authentication using the same security information used for other applications in your company. If your company has already adopted LDAP, you can use your existing LDAP directories with the application.
- System Installation passphrase - During installation, you create a system passphrase for your Sterling B2B Integrator installation. The passphrase is a highly complex string longer than 16 characters. The system passphrase is required to start the system and to access protected system information.
- Support for x.509 certificates for encryption, signing, and transport layer security.
- Federal Information Processing Standards (FIPS) 140-2 certified software module and support for FIPS 140-2 certified hardware from nCipher and Safenet.
- Secure Socket Layering (SSL) and Transport Layer Security (TLS).

Additionally, the following security features can be configured:

- Security time out feature provides you with the ability to configure user sessions time outs.
- Custom Password Policy feature allows you to add additional password policy rules. These additional password rules can help you prevent the use of weak, easily hacked passwords and reject non-compliant passwords.
- Single Sign On (SSO) feature is an authentication process that enables users to access several applications and only have to enter one user name and password.
- Document Encryption feature allows for the configuration of an additional layer of security beyond traditional file and database permissions.

---

## Role Based Security

### Role-Based Security Overview

Role-based security provides users with access to certain files, business processes, Web templates, services, and product features, according to the permissions associated with the user account.

In order to understand how to administer role-based security, you need to understand how groups, permissions, and user accounts work together.

- Permissions provide access to user interface pages and the functionality provided by the page.
- Groups are collections of permissions.
- User accounts are assigned to permissions and password policies.

Managing role-based security includes the following tasks:

- Create permissions
- Create groups
- Create password policies
- Create user accounts

## Groups

Groups are collections of permissions. Groups make it possible to maintain access permissions for several users from a single place. Groups help to minimize the amount of work that is involved with maintaining accounts, especially when several users perform the same job function.

You can associate many permissions to different users by creating groups for each job function instead of each user. You can also assign a group as a subgroup to another group.

For example, a procurement department has five procurement specialists that all perform the same jobs. Instead of applying permissions to each individual procurement specialist user account, you can create a procurement group and maintain access permissions for all procurement specialists in one group. Within the procurement group, you can assign subgroups to further refine your access permissions according to the type of procurement the specialist conducts. You can assign subgroups named office supplies, machinery, general equipment, or vehicles to the procurement group to refine access permissions.

To avoid overwriting when applying upgrades or patches, do not modify the groups that come preconfigured with the system.

Group tasks include:

- Create a group
- Search for a group
- Edit a group
- Delete a group

### Preconfigured Groups

To assign permissions to users, you can assign the preconfigured groups. Users inherit all permissions associated with the groups. A predefined group might be assigned to a user when Accessibility and Theme are defined for the user account.

You must have permission to the Accounts module to create groups.

### Group Naming Conventions

Group naming has a series of conventions.

Use the following naming conventions for groups:

- Group IDs must be distinct.
- Names are case-sensitive.



- Two group names with different capitalization are considered as distinct names.
- If a group name has been used, it cannot be used as the name for a new group. An error message will display.

## Search for Groups

You can search for a group from the **Administration** menu.

### About this task

To search for a group:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Groups**.
2. Complete one of the following actions:
  - Under **Search**, enter a portion of the **Group Name** or the entire **Group Name** you are searching for and click **Go!** The **Groups** page lists all of the groups that match your search criteria.
  - Under **List**, select **ALL** or the letter that begins the name of the group you are searching for in the **Alphabetically** field and click **Go!** The **Groups** page lists all of the groups that match your search criteria.

## Create Groups

You can create a group from the **Administration** menu.

### About this task

Before you begin, you need to know:

- Group ID for the group you are creating.
- Group name of the group you are creating.
- Name of the Owner for the group.
- Identity of the trading partner to associate with the group. Only one trading partner can be associated with a group, but a user account can be associated with many groups. This enables a user account to be associated with more than one trading partner. The identity field is used for routing messages in Mailbox.

To create a group:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Groups**.
2. Next to **Create a new Group**, click **Go!**
3. In the **New Group** page, enter the **Group ID**.
4. Enter **Group Name**.
5. Enter **Owner**.
6. Select the **Identity**.
7. Click **Next**.
8. In the **Assign Subgroups** page, if you want to filter groups by name, under **Filter Data** in the **By Name** field, enter a portion of the name or the entire name of the group you want to filter for and click the filter button.
9. Select the groups you want to assign to this group. Move the groups from the **Available** pane to the **Assigned** pane.
10. Click **Next**.

11. In the Assign Permissions page, do you want to filter permissions?
  - To filter by name, under Filter Data in the **By Name** field, enter a portion of the name or the entire name of the permission you want to filter for and click the filter button to the right of the **By Type** field.
  - To filter by type, under Filter Data, select the type of permission you want to filter for from the By Type list and click the filter button to the right of the **By Type** field.
12. Select the permissions you want to assign to this group. Move the permissions from the Available pane to the Assigned pane. By default, the permissions associated with the subgroups assigned to this group are already selected. The associated permissions do not display in the available column; but they are displayed in the confirm page.
13. Click **Next**.
14. Review the group information.
15. Click **Finish**.

## Edit Groups

You can edit a group to update settings, subgroups, and permissions.

### About this task

When you edit a group, you can update:

- Settings
- Subgroups
- Permissions

You cannot change the Group ID. If you need to change the Group ID, you must create a new group.

To edit a group:

### Procedure

1. From the **Administration Menu**, select **Accounts > Groups**.
2. Search for the group you want to edit, using either the Group Name Search or Alphabetically List and click **Go!**
3. Select **edit** for the group you want to update.
4. Update any of the group settings and click **Next**.
5. Update any of the assigned subgroups and click **Next**.
6. Update any of the assigned permissions and click **Next**.
7. Click **Next**.
8. Review the group information.
9. Click **Finish**.

## Delete Groups

You can delete groups from the **Administration** menu.

### About this task

You cannot remove the Sterling B2B Integrator Admin group or the UI Accounts permission from an administrator user. These allow the system administrator to administer the system.

To delete a group:

### Procedure

1. From the **Administration Menu**, select **Accounts > Groups**.
2. In the Groups page, locate the group you want to delete by using either the Search or List option.
3. In the Groups page, next to the group you want to delete, click **delete**.  
The system deletes the group and displays the message:  
The system update has completed successfully.

### Review the Group Name and ID

You can review a group name and ID from the **Administration** menu.

### About this task

To review a group name and ID:

### Procedure

1. From the **Administration Menu**, select **Account > Group**.
2. In the Group page, locate the group you want to review by using either the Search or List options.
3. Select the group. The group name and ID are displayed.

## Permissions

Permissions provide access to the different modules within Sterling B2B Integrator and are the foundation of role-based security. A user's permissions consist of permissions from groups plus any permissions that are assigned individually.

Use permissions to:

- Manage access for several users from a single place.
- Manage user accounts with minimum effort, especially for multiple users who perform the same job function.

Permissions tasks include:

- Create a permission
- Search for a permission
- Edit a permission name
- Delete a permission

Before you create, edit, or delete a permission, decide which modules the users in that group need or do not need to access to perform their assigned functions. You must be assigned permission to the Accounts module to create permissions.

To avoid overwriting when applying upgrades or patches, do not modify the permissions that come preconfigured with the system. When customized groupings of permissions are required, create a new group.

### Permissions Naming Conventions

Permissions names are case-sensitive and cannot be duplicated.

Permission naming conventions include:

- Names are case-sensitive and two names with different capitalization are considered to be unique names. For example "Any document" and "Any Document" are two different permission names.
- If a name has been used for an existing permission, it cannot be used as the name for a new permission. An error message will display.

While two permissions may have the same name with different capitalization, it is not recommended.

## Permissions Inherited from Groups

These are preinstalled groups and the permissions inherited when a permissions group is assigned to a user account. The same permissions are inherited when a group is assigned as a subgroup.

Each group contains permissions for menu items plus the corresponding UI permission that is used to grant access to the page. For example, EBXML contains UI EBXML.

Group Name	Group ID	Permissions Inherited from the Group
ACCOUNTS	ACCOUNTS	PasswordPolicy, Permissions, UI Accounts, UserNews
ADAPTER_UTILITIES	ADAPTER_UTILITIES	BEATuxedo, CDNetmaps, CDNetmapXref, CDNnodes, SAPRoutes, SAPRouteXREF, SAPSuiteBuilder, UI Adapter Utilities
ADVANCED_SETUP	ADVANCED_SETUP	DeliveryChannels, DocumentExchange, Identities, Packaging, Profiles, Transports, UI Advanced Trading Profile Setup
AS2 Edition	as2admin	All permissions from the subgroup BPMONITOR, plus 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 Partners
Abnormal Event Notification	eventAbnormal	None
Accounts	acctadmin	All permissions from the subgroup ACCOUNTS, plus UI Groups, UI User Accounts.
Alert Notifications	notifications	None
BPMONITOR	BPMONITOR	BPSSCorrelation, BusinessProcesses, CentralSearch, CommunicationSessions, Correlation, CurrentActivities, CurrentDocuments, CurrentProcesses, DataFlows, Documents, EBXMLCorrelation, EDICorrelation, EDIINT, GentranServerforUnix, Message Entry Workstation Home, SWIFTNETCorrelation, UI BP Monitor, RosettaNet
Business Process	bpadmin	All permissions from the BPMONITOR and SERVICES subgroups, plus UI BP Manager, UI Business Process, UI Delete BP.
CD Server Proxy Administrator	cdsp_admin	All permissions from the subgroups ACCOUNTS, BPMONITOR, CD Server Proxy User, OPERATIONS, and SERVICES, plus UI Groups, UI Licenses, UI Password Policy, UI SQL Tool, UI User Accounts.

Group Name	Group ID	Permissions Inherited from the Group
CD Server Proxy User	cdsp_user	This group is assigned by default when a user account is created with CDSP Accessibility.  All permissions from the ACCOUNTS, BPMONITOR, OPERATIONS, and SERVICES subgroups, plus CDSP Services, UI CA Certs, UI Import/Export, UI Lock Manager, UI Logs, UI Perimeter Servers, UI Reports, UI Support Case Tool, UI System Certs, UI Trusted Certs.
Command-Line User	commandlineuser	eInvoicing, eInvoicing ALL BUYERS, eInvoicing ALL SUPPLIERS, eInvoicing Archive, eInvoicing Configuration, eInvoicing CREATE/EDIT AGREEMENT, eInvoicing DELETE AGREEMENT, VIEW AGREEMENT
DEPLOYMENT	DEPLOYMENT	UI Deployment, Resource Tags
Dashboard Users	dashboardUsers	This group is assigned by default when a user account is created with Dashboard UI accessibility and any of the following dashboard themes: <ul style="list-style-type: none"> <li>• AFT</li> <li>• Default</li> <li>• Community Management Operator, Participant, Participant Sponsor, or Sponsor</li> </ul> Administration Management Console, Business Process Search Portlet, Cache Statistics Portlet, Cache Usage Portlet, Community Management Portlet, Community Statistics Portlet, Database Pool Usage Portlet, Database Status Portlet, Database Usage Portlet, Document Search Portlet, Document Tracking Portlet, Documents Processed Bar Chart Portlet, Documents Processed Time Series Portlet, Event Viewer Portlet, IFrame Portlet, Log File Viewer Portlet, Log File Viewer Portlet 2, ParticipatingCommunities Portlet, Peers Portlet, Queue Priority Statistics Portlet, Quick Links Portlet, RSS Feed Portlet, Sponsored Communities Portlet, System Alerts Portlet, Web Search Portlet, Web View Plus Portlet
Deployment	deploymentadmin	All permissions from the ADAPTER_UTILITIES, DEPLOYMENT, EBXML, MAILBOX, MAPS, SERVICES, WEB_EXTENSIONS, and WEB_SERVICES subgroups, plus UI Connect:Direct, UI Delete CPA and CPSS Schema/Extension, UI Delete Map, UI Delete PGP Profile, UI Delete SAP Routes, UI Delete Schema, UI Delete Service Instance, UI Delete SWIFTNet Routing Rule, UI Delete Web Resource, UI Delete Web Templates, UI Delete WSDL, UI Delete XSLT Template, UI Generate/Download WAR Files, UI Import/Export, UI Scheduler, UI Schemas, UI SSH Local Identity Key, UI SWIFTNet Routing Rule, UI XSLT
EBICS Administrators	EBICS_ADM	UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS File Format Configuration, UI EBICS Offer Configuration, UI EBICS Order Type Configuration, UI EBICS Partner Profile Configuration, UI EBICS User Permission Configuration, UI EBICS User Profile Configuration, UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS Subscriber Key Validation,

Group Name	Group ID	Permissions Inherited from the Group
EBICS Operators	EBICS_OPERATOR	UI EBICS Bank Profile Configuration, UI EBICS Contract Configuration, UI EBICS File Format Configuration, UI EBICS Offer Configuration, UI EBICS Order Type Configuration, UI EBICS Partner Profile Configuration, UI EBICS Subscriber Key Validation, UI EBICS User Permission Configuration, UI EBICS User Profile Configuration
EBXML	EBXML	BPSS, BPSSExtension, CPA, UI EBXML
ENVELOPES	ENVELOPES	ControlNumberHistory, ControlNumbers, EDISquenceCheckQueue, Envelopes, TransactionRegister, UI Envelopes
Exceptional Event Notifications	eventExceptional	None
MAILBOX	MAILBOX	Configuration, Messages, Routing Rules, UI Mailbox, VirtualRoots
MAPS	MAPS	ExtendedRuleLibraries, Maps, Standards, UI Maps
Mailbox Administrators	mboxadmins	All permissions from the MAILBOX and Mailbox Browser Interface Users groups, plus DeadLetter Mailbox, Mailbox Global Delete, Mailbox Global Query, EBICS_DEADLETTER Mailbox
Mailbox Browser Interface Users	mbiusers	Mailbox Add Business Process, Mailbox Extract Business Process, Mailbox Path List Process, Mailbox Query Business Process, Mailbox Search Business Process, Mailbox Self Registration Business Process, Mailbox View Business Process, MBISearch JSP
OPERATIONS	OPERATIONS	JDBCMonitor, MessageMonitor, Perfdumps, SequenceManager, Statistics, ThreadMonitor, Troubleshooter, Tuning, UI Federated Systems, UI Operations
Provisional Trading Partners	provisionalpartners	None
SERVICES	SERVICES	Configuration, Installation/Setup, UI Services
SSH	SSH	AuthorizedUserKey, KnownHostKey, RemoteProfiles, UI SSH, UserIdentityKey
Session Demo Web Suite Buyer	sd_buyer	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite Query Business Process, WebSuite RA Send Business Process, WebSuite Self Registration Business Process, WebSuite Session Demo Confirm Send Template, WebSuite Session Demo PO Send Business Process, WebSuite Session Demo PO Template, WebSuite Session Demo PO View Template, WebSuite Session Demo Query List Template

Group Name	Group ID	Permissions Inherited from the Group
Session Demo Web Suite Suppliers	sd_supplier	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite PO to Advance Ship Notice Template, WebSuite PO to Invoice Template, WebSuite PO Turn Business Process, WebSuite Query Business Process, WebSuite RA Send Business Process, WebSuite Self Registration Business Process, WebSuite Session Demo Confirm Send Template, WebSuite Session Demo PO Send Business Process, WebSuite Session Demo PO View Template, WebSuite Session Demo Query List Template
Sterling B2B Integrator Admin	super	All permissions from the ACCOUNTS, ADAPTER_UTILITIES, ADVANCED_SETUP, BPMONITOR, DEPLOYMENT, EBXML, ENVELOPES, MAILBOX, MAPS, Mailbox Administrators, OPERATIONS, SERVICES, SSH, WEB_EXTENSIONS, and WEB_SERVICES subgroups, plus UI Archive, UI AS2 Trading Profile Setup, UI Basic Trading Profile Setup, UI BP Manager, UI Business Process, UI CA Certs, UI CodeLists, UI Connect:Direct, UI Contracts, UI Delete BP, UI Delete CPA and CPSS Schema/Extension, UI Delete Map, UI Delete PGP Profile, UI Delete SAP Routes, UI Delete Schema, UI Delete Service Instance, UI Delete SWIFTNet Routing Rule, UI Delete Trading Partner Data, UI Delete Web Resource, UI Delete Web Templates, UI Delete WSDL, UI Delete XSLT Template, UI Federated, UI Generate/Download WAR Files, UI Groups, UI Import/Export, UI Licenses, UI Lock Manager, UI Logs, UI Notify, UI Perimeter Servers, UI PGP Profile Manager, UI Reports, UI Scheduler, UI Schemas, UI SQL Tool, UI SSH Local Identity Key, UI Support Case Tool, UI SWIFTNet Routing Rule, UI System Certs, UI Trading Partners, UI Trusted Certs, UI User Accounts, UI XSLT
System Operations	operator	All permissions from the OPERATIONS subgroup, plus UI Archive, UI Licenses, UI Lock Manager, UI Logs, UI Notify, UI Perimeter Servers, UI Reports, UI Scheduler, UI SQL Tool, UI Support Case Tool
Trading Profiles	tpadmin	All permissions from the ADVANCED_SETUP, ENVELOPES, and SSH subgroups, plus 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

Group Name	Group ID	Permissions Inherited from the Group
Web Suite Buyers	wsbuyers	WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack View Template, WebSuite PO Send Business Process, WebSuite PO Template, WebSuite PO View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite RA Send Business Process, WebSuite Remittance Advice Template, WebSuite Remittance Advice View Template, WebSuite Self Registration Business Process
Web Suite Employees	wsemployees	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite ER Send Business Process, WebSuite Expense Report Template, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req Send Business Process, WebSuite Purchase Req Template, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet Template, WebSuite TimeSheet View Template, WebSuite TS Send Business Process
Web Suite Finance	wsfinance	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process
Web Suite Human Resources	wshr	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet View Template
Web Suite Managers	wsmanagers	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite ER Send Business Process, WebSuite Expense Report View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req Send Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process, WebSuite TimeSheet View Template, WebSuite TS Send Business Process



Group Name	Group ID	Permissions Inherited from the Group
Web Suite Purchasers	wspurchaser	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query List Template, WebSuite Self Registration Business Process
Web Suite Suppliers	wssupplier	WebSuite ASN Send Business Process, WebSuite ASN Template, WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password 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

### Permissions Needed to Access UI Resources

This is the minimum set of permissions required to access a menu item and its associated page and functionality. Assigning the set of minimum permissions may make some additional functionality available to the user as well. If you do not have permission to a menu item and its associated functionality, it will not display.

From the Administration Menu > Business Process, UI Resource	Permission Name / Permission ID
Business Process > Manager	UI BP Manager (BPMANAGE) plus UI Business Process (BUSINESS_PROCESS)
Business Process > Monitor > Advanced Search > Business Process	BusinessProcesses (PLTADM2) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > SWIFNET Correlation	SWIFNETCorrelation (GISADM9) plus UI BP Monitor (BPMONITOR) and UI SWIFNet Routing Rule (SWIFNET_ROUTING_RULE)
Business Process > Monitor > Advanced Search > Data Flows	DataFlows (GISADM1) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > Documents	Documents (GISADM2) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > Communication Sessions	Communication Sessions (GISADM3) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > Correlation	Correlation (GISADM4) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > BPSS Correlation	BPSSCorrelations (GISADM5) plus UI BP Monitor (BPMONITOR)

<b>From the Administration Menu &gt; Business Process, UI Resource</b>	<b>Permission Name / Permission ID</b>
Business Process > Monitor > Advanced Search > EBXML Correlation	EBXMLCorrelation (GISADM6) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > EDI Correlation	EDICorrelation (GISADM7) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Advanced Search > EDIINT	EDIINT (STDSADM6) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Central Search	CentralSearch (GISADM10) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Current Processes	CurrentProcesses (PLTADM3) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Current Documents	CurrentDocuments (GISADM11) plus UI BP Monitor (BPMONITOR)
Business Process > Monitor > Current Activities	CurrentActivities (PLTADM4) plus UI BP Monitor (BPMONITOR)
Business Process > Message Entry Workstation	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

<b>From the Administration Menu &gt; Trading Partner, UI Resource</b>	<b>Permission Name / Permission ID</b>
Trading Partner > Setup > Basic	UI Basic Trading Profile Setup (BASIC_SETUP)
Trading Partner > Setup > Advanced > Identities	Identities (GISADM12) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP)  Deleting also requires UI Delete Trading Partner permission (TP_DELETE)
Trading Partner > Setup > Advanced > Transports	Transports (GISADM13) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP)  Deleting also requires UI Delete Trading Partner permission (TP_DELETE)
Trading Partner > Setup > Advanced > Document Exchange	DocumentExchange (GISADM14) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP)  Deleting also requires UI Delete Trading Partner permission (TP_DELETE)
Trading Partner > Setup > Advanced > Delivery Channels	DeliveryChannels (GISADM15) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP)  Deleting also requires UI Delete Trading Partner permission (TP_DELETE)
Trading Partner > Setup > Advanced > Packaging	Packaging (GISADM16) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP)  Deleting also requires UI Delete Trading Partner permission (TP_DELETE)

<b>From the Administration Menu &gt; Trading Partner, UI Resource</b>	<b>Permission Name / Permission ID</b>
Trading Partner > Setup > Advanced > Profiles	Profiles (GISADM17) plus UI Advanced Trading Profile Setup (ADVANCED_SETUP)  Deleting also requires UI Delete Trading Partner permission (TP_DELETE)
Trading Partner > Digital Certificates > CA	UI CA Certs (CA_CERTS) plus UI System Certs (SYSTEM_CERTS) UI  System Certs adds the System option.
Trading Partner > Digital Certificates > Trusted	UI Trusted Certs (TRUSTED_CERTS)
Trading Partner > Digital Certificates > System	UI System Certs (SYSTEM_CERTS)
Trading Partner > Document Envelopes > Envelopes	Envelopes (STDSADM1) plus UI Envelope (ENVELOPE)
Trading Partner > Document Envelopes > Control Numbers	ControlNumbers (STDSADM2) plus UI Envelope (ENVELOPE)
Trading Partner > Document Envelopes > Transaction Register	TransactionRegister (STDSADM3) plus UI Envelope (ENVELOPE)
Trading Partner > Document Envelopes > Control Number History	ControlNumberHistory (STDSADM4) plus UI Envelope (ENVELOPE)
Trading Partner > Document Envelopes > EDI Sequence Check Queue	EDISequenceCheckQueue (STDSADM5) plus UI Envelope (ENVELOPE)
Trading Partner > Contracts	UI Contracts (CONTRACTS) plus UI Advanced Trading Partner Setup (ADVANCED_SETUP)
Trading Partner > Code Lists	UI CodeLists (CODELISTS)
Trading Partner > AS2	UI AS2 Trading Profile Setup (AS2_SETUP)
Trading Partner > SSH > Remote Profiles	RemoteProfiles (ASSETADM1) plus UI SSH
Trading Partner > SSH > Known Host Key	KnownHostKey (ASSETADM2) plus UI SSH
Trading Partner > SSH > User Identity Key	UserIdentityKey (ASSETADM3) plus UI SSH
Trading Partner > SSH > Authorized User Key	AuthorizedUserKey (ASSETADM4) plus UI SSH
Trading Partner > AS3	UI AS3 Trading Profile Setup (AS3_SETUP)
Trading Partner > Odette FTP Partner Profile > Physical Partner	OftpPhysicalPartner (ASSETOFTP1) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Trading Partner > Odette FTP Partner Profile > Physical Partner Contract	OftpPhysicalPartnerContract (ASSETOFTP3) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Trading Partner > Odette FTP Partner Profile > Logical Partner	OftpLogicalPartner (ASSETOFTP2) plus UI Adapter Utilities (ADAPTER_UTILITIES)

<b>From the Administration Menu &gt; Trading Partner, UI Resource</b>	<b>Permission Name / Permission ID</b>
Trading Partner > Odette FTP Partner Profile > Logical Partner Contract	OftpLogicalPartnerContract (ASSETOFTP4)
Trading Partner > PGP > Server Manager	PGP Server Manager (ASSETADM55) plus UI PGP Profile Manager (PGP)
Trading Partner > PGP > Sponsor Manager	PGP Sponsor Manager (ASSETADM56) plus UI PGP Profile Manager (PGP)
Trading Partner > PGP > Partner Manager	PGP Partner Manager (ASSETADM57) plus UI PGP Profile Manager (PGP)

<b>From the Administration Menu &gt; Deployment, UI Resource</b>	<b>Permission Name / Permission ID</b>
Deployment > Services > Installation/Setup	Installation/Setup (PLTADM9) plus UI Services (SERVICES)
Deployment > Services > Configuration	Configuration (PLTADM10) plus UI Services (SERVICES), UI BP Manager (BPMANAGE). As of V5.2.4.3 and higher, UI Adapters StartStop is also required.
Deployment > Schedules	UI Scheduler (SCHEDULER)
Deployment > Maps	Maps (ASSETADM5) plus UI_Maps
Deployment > Standards	Standards (STDSADM7) plus UI_Maps
Deployment > Extended Rule Libraries	ExtendedRuleLibraries (ASSETADM6) plus UI_Maps
Deployment > XSLT	UI XSLT (XSLT)
Deployment > Web Extensions > Web Resources	WebResources (GISADM19) plus UI Web Extensions and UI Web Services (WEB_SERVICES)  UI Web Services allows the user to check in a new Web Resource file
Deployment > Web Extensions > Utilities	Utilities (GISADM20) plus UI Web Extensions.  Visible only in the case of an upgrade from an earlier version.
Deployment > Schemas	UI Schemas (SCHEMAS)
Deployment > Mailboxes > Configuration	Configuration (MBXADM1) plus UI Mailbox (MAILBOX)
Deployment > Mailboxes > Virtual Roots	VirtualRoots (MBXADM2) plus UI Mailbox (MAILBOX)
Deployment > Mailboxes > Routing Rules	RoutingRules (MBXADM3) plus UI Mailbox (MAILBOX)
Deployment > Mailboxes > Messages	Messages (MBXADM4) plus UI Mailbox (MAILBOX)
Deployment > EBXML > BPSS	BPSS (ASSETADM7) plus UI EBXML (EBXML)
Deployment > EBXML > BPSS Extension	BPSSExtension (ASSETADM8) plus UI EBXML (EBXML)

<b>From the Administration Menu &gt; Deployment, UI Resource</b>	<b>Permission Name / Permission ID</b>
Deployment > EBXML > CPA	CPA (ASSETADM9) plus UI EBXM (EBXML)
Deployment > Resource Manager > Resource Tags	Resource Tags (PLTADM1) plus UI Deployment (DEPLOYMENT)
Deployment > Resource Manager > Import/Export	UI Import/Export (IMPORT_EXPORT)
Deployment > Adapter Utilities > SAP Suite Builder	SAPSuiteBuilder (ASSETADM10) plus UI Adapter Utilities
Deployment > Adapter Utilities > Sap Routes > Sap Routes	SAPRoutes (ASSETADM11) plus UI Adapter Utilities
Deployment > Adapter Utilities > Sap Routes > SapRouteXRef	SAPRouteXREF (ASSETADM12) plus UI Adapter Utilities
Deployment > Adapter Utilities > BEATuxedo	BEATuxedo (ASSETADM13) plus UI Adapter Utilities  Menu item does not display unless BEATuxedo jar is installed.
Deployment > Adapter Utilities > SWIFTNET Routing Rule	UI SWIFTNET Routing Rule (SWIFTNET_ROUTING_RULE)
Deployment > Adapter Utilities > SWIFTNET Service Profile	UI SWIFTNET Service Profile (SWIFTNET_SVC_PROFILE)
Deployment > Adapter Utilities > SWIFTNET Copy Service Profile	UI SWIFTNET Copy Profile (SWIFTNET_COPY_PROFILE)
Deployment > Adapter Utilities > Lockout Policy Manager	LockoutPolicyManager (ASSETADM50)
Deployment > Adapter Utilities > C:D Netmaps > C:D Node	CDNetmaps (ASSETADM51) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Deployment > Adapter Utilities > C:D Netmaps > C:D Netmaps	CDNodes (ASSETADM52) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Deployment > Adapter Utilities > C:D Netmaps > C:D Netmap X-REF	CDNetmapXref (ASSETADM53) plus UI Adapter Utilities (ADAPTER_UTILITIES)
Deployment > Adapter Utilities > Policy Configuration	Adapter Policies (ASSETADM54)
Deployment > Adapter Utilities > File System Virtual Root	File System Virtual Root (ASSETADM58)
Deployment > SSH Host Identity Key	UI SSH Local Identity Key (SSH_LCL_ID_KEY) and UI SSH (SSH)
Deployment > Web Services > Manager	WebServicesManager (ASSETADM16) and UI Web Services (WEB_SERVICES)
Deployment > Web Services > Schema Mappings	SchemaMappings (ASSETADM17), UI Web Services (WEB_SERVICES), and UI EBXML (EBXML)
Deployment > Web Services > WSDL Check In	WSDLCheckIn (ASSETADM18) plus UI Web Services (WEB_SERVICES)
Deployment > Web Services > Security Token	SecurityToken (ASSETADM18) plus UI Web Services (WEB_SERVICES)

<b>From the Administration Menu &gt; e-Invoicing, UI Resource</b>	<b>Permission Name / Permission ID</b>
e-Invoicing > Agreements	eInvoicing VIEW AGREEMENT (EINV_VIEW_AGREEMENT)  Deleting also requires eInvoicing DELETE AGREEMENT (EINV_DELETE_AGREEMENT) permission.
e-Invoicing > Integrated Archive	eInvoicing Archive (EINVOICING_ARCHIVE) plus eInvoicing VIEW INVOICE (EINV_VIEW_INVOICE)
e-Invoicing > Configuration	eInvoicing Configuration (EINVOICING_CONFIGURATION)

<b>From the Administration Menu &gt; Operations, UI Resource</b>	<b>Permission Name / Permission ID</b>
System > Troubleshooter	Troubleshooter (PLTADM17) plus UI Operations (OPERATIONS)
System > Performance > Tuning	Tuning (PLTADM18) plus UI Operations (OPERATIONS)
System > Performance > Statistics	Statistics (PLTADM19) plus UI Operations (OPERATIONS)
System > Performance > JVM monitor	Perfdumps (GISADMIN27) plus UI Operations (OPERATIONS)
System > Support Tools > SQL Manager	UI SQL Tool (SQLMANAGER)
System > Support Tools > Support Case	UI Support Case Tool (SUPPORT_CASE)
System > Logs	UI Logs (SYSTEM_LOGS)
System > Licenses	UI Licenses (LICENSES)
Reports	UI Reports (REPORTS)
Thread Monitor	ThreadMonitor (PLTADM24) plus UI Operations (OPERATIONS)
JDBC Monitor	JDBCMonitor (PLTADM25) plus UI Operations (OPERATIONS) and UI SQL Tool (SQLMANAGER)
Archive Manager	UI Archive (ARCHIVE-UI) plus UI Operations (OPERATIONS), UI BP Manage (BPMANAGE) and UI Business Process (BUSINESS_PROCESS)
Lock Manager	UI Lock Manager (LOCK_MANAGER)
Message Monitor	MessageMonitor (GISADM24) plus UI Operations (OPERATIONS)
Perimeter Services	UI Perimeter Servers (PSERVERS)
Proxy Servers	UI Proxy Servers (PROXYSERVERS) plus Sterling B2B Integrator Admin group

<b>From the Administration Menu &gt; Accounts, UI Resource</b>	<b>Permission Name / Permission ID</b>
Groups	UI Groups (GROUPS) plus UI Accounts (ACCOUNTS)

<b>From the Administration Menu &gt; Accounts, UI Resource</b>	<b>Permission Name / Permission ID</b>
Permissions	Permissions (PLTADM27) plus UI Accounts (ACCOUNTS)
User Accounts	UI User Accounts (USER_ACCOUNTS) plus UI Accounts (ACCOUNTS)
Password Policy	PasswordPolicy (PLTADM29) plus UI Accounts (ACCOUNTS)
User News	UserNews (GISADM25) plus UI Accounts (ACCOUNTS)
My Account	MyAccount (PLTADM30)

## Preconfigured Permissions

Preconfigured permissions are provided with the system. Like custom permissions, they provide access to the different modules within the system.

## Search for Permission Names

You can search for a permission from the **Administration** menu.

### About this task

To search for a permission:

### Procedure

1. From the **Administration Menu**, select **Accounts > Permissions**.
2. In the Permissions page, complete one of the following actions:
  - Under Search in the **Permission Name** field, enter a portion of the permission name or the entire permission name you are searching for and click **Go!** The Permissions page lists all of the permissions that match your search criteria.
  - Under List in the **Alphabetically** field, select **ALL** or the letter that begins the name of the permission you are searching for and click **Go!** The Permissions page lists all of the permissions that match your search criteria.

## Create Permissions

If you upgraded from a previous version of the system, the existing permissions are set to Other by default. You might need to edit each permission to apply a new permission type.

## About this task

Before you begin you need to know the following information:

Field	Description
Permission ID	<p>Permission ID for the permission you are creating. Permission ID is the name of the business process, XSLT document, Web template, or resource for which you are setting the permission. Include the extension for the resource after the ID. Required.</p> <p>Permission IDs:</p> <ul style="list-style-type: none"><li>• They must be unique.</li><li>• They are case-sensitive.</li><li>• The permission ID must match the name of the business process, XSLT document, Web template, or resource. If the permission ID and the name of the resource do not match exactly, you cannot lock down the resource.</li></ul>
Permission Name	<p>Name of the permission you are creating. Required.</p> <p>A permission name must be unique. Permission names are case-sensitive, for example "Any document" and "Any Document" are two different permission names.</p>
Permission Type	<p>Permission type of the permission you are creating. Required. Permission types include:</p> <ul style="list-style-type: none"><li>• UI – Allows access to specific menu items in the interface.</li><li>• Mailbox – Allows access to specific mailboxes in the system.</li><li>• Template – Allows access to specific Web templates.</li><li>• BP – Allows access to specific business processes.</li><li>• Tracking – Allows access to specific document tracking options.</li><li>• Community – Allows access to specific community management options.</li><li>• Web Service</li><li>• Service</li><li>• eInvoicing</li><li>• Other – Allows access to resources that are not identified by one of the preceding types.</li></ul>

To create a permission:

### Procedure

1. From the **Administration Menu**, select **Accounts > Permissions**.
2. **Next to Create a new Permission**, click **Go!**
3. In the Permissions page, enter the **Permission ID**.
4. Enter the **Permission Name**.
5. Select the **Permission Type**.
6. Click **Next**.
7. Review the permission settings.
8. Click **Finish**.

### Edit Permission Names

If you need to change the name of a permission to reflect the permission more closely, you edit a permission name. Permission names must be unique and are



case-sensitive. You cannot change the permission ID. If you need to edit the permission ID, you must create a new permission.

### About this task

To edit a permission name:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Permissions**.
2. Search for the permission you want to edit, using either the Permission Name Search or Alphabetically List and click **Go!**
3. Next to the Permission you want to edit, click **edit**.
4. Enter a new **Permission Name**.
5. Update the permission type, if required, and click **Next**.
6. Review the permissions settings information.
7. Click **Finish**.

### Delete Permissions

You can delete a permission that is associated with a user account. When you delete a permission, you remove it from use for all user accounts.

### About this task

If the permission you are deleting is the only permission that is associated with a user account, you must edit the user account to associate another permission. If you do not associate at least one new permission with the user account, the user can log in, but has no access to any menu items.

To delete a permission:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Permissions**.
2. Search for the permission you want to delete, using either the Permission Name Search or Alphabetically List and click **Go!**
3. In the Permissions page, click **Delete** for the permission you want to delete.
4. Verify that the permission information matches the permission you want to delete and click **Delete**.

The system deletes the permission and displays the message:

The system update completed successfully.

### Review the Permission Name and ID

You can review a permission name and ID from the **Administration** menu.

### About this task

To review a permission name and ID:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Permissions**.
2. Search for the permission you want to review, using either the Permission Name Search or Alphabetically List and click **Go!**
3. Select the permission. The permission name and ID are displayed.

## User Accounts

User accounts are defined by groups, permissions, and password policies to help to provide a secure environment. This type of user account definition is defined as a role-based security model.

Before you create any new user accounts, you need to determine what groups, permissions, and password policies your business environment requires. The assignment of groups, permissions, and password policies are optional.

Only account with create permissions can create new user accounts. User accounts tasks include:

- Create a user account
- Search a user account
- Edit a user account
- Delete a user account

### Default User Account Permissions

MyAccount and Admin Web App Permissions are automatically assigned to user accounts.

The following permissions are assigned automatically to user accounts:

- MyAccount (Permission ID PLTADM30) – Allows access to the My Account page (Accounts > My Account).
- Admin Web App Permissions (Permission ID WebAppAdminPermission) – Used to access other Web applications.

Do not remove these permissions from user accounts. If they are removed accidentally, edit the User Account and save. The missing permissions will be restored.

### User Account Authentication

User account authentication can be either local or external.

User account authentication can be either:

- Local – Authentication is completed against the database.
- External – Authentication is completed against an LDAP server. External authentication does not require the LDAP adapter, which is used with business processes and enables to communicate with local or remote LDAP servers by using a Java Naming Directory Interface (JNDI). If you do not have a license for single sign-on or LDAP, all the users you create are local users and authenticated against the application's database. To create an external user account, you must have an application license for single sign-on or LDAP.

### User Account Creation Checklist

You can create a user account.

Use this checklist to create a user account:

Task	Role-Based Security Checklist	Your Notes
1	Create new permissions or review the preconfigured permissions that come preinstalled.	

Task	Role-Based Security Checklist	Your Notes
2	Create new groups or review the groups that come preinstalled.	
3	Create a custom password policy to assign to user.	
4	If you are using external authentication, set up the environment for external authentication.	
5	Create the user account and assign the permissions, groups, and password policies.	

## Set Up the Environment for External User Account Authentication

If you are creating an external user, you can specify an alternative authentication method (generally LDAP).

### About this task

Before creating an external user account, you must:

#### Procedure

1. Stop Sterling B2B Integrator.
2. Specify the alternative authentication method by adding or modifying the authentication configuration in the authentication\_policy.properties.in file. The properties need to follow this format: authentication\_4.xxx=xxx\_value.
3. Enter setupfiles.sh.
4. Start Sterling B2B Integrator.

## Search for User Accounts

You can search for a user account from the **Administration** menu.

### About this task

To search for a user account:

#### Procedure

1. From the **Administration Menu**, select **Accounts > User Accounts**.
2. Complete one of the following actions:
  - Under Search in the **Account Name** field, type either a portion of the name or the entire name of the user account you are searching for, and click **Go!** The Accounts page lists all of the user accounts that match your search criteria.
  - Under List in the **Alphabetically** field, select **ALL** or the letter that begins the name of the user account you are searching for and click **Go!** The Accounts page lists all of the user accounts that match your search criteria.

## Create User Accounts

You create a new user account from the **Administration** menu.

## About this task

Before you begin, you need to know if you are using local or external authentication:

- Local – Authentication is completed against the application's database. Default.
- External – Authentication is completed against an LDAP server. External authentication does not require the LDAP adapter, which is used with business processes and enables the system to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).

If you are assigning one or more Authorized User Keys to this account, the keys must be obtained from your trading partner and checked in prior to creating the user account.

**Note:** While multiple foreign languages are supported, one user account should not be used with more than one specific language to avoid user interface display issues.

You also need to know the following information:

Field	Description
User ID	User ID for the user account you are creating. The user ID must be at least five alpha-numeric characters long. No special characters or punctuation are allowed. Required.  For the MySQL database only, the login is not case-sensitive. You should always use uniquely spelled IDs, so that one user does not accidentally use another user's ID.
Password (Local Authentication only)	Password for the user account you are creating. The password must be at least six alpha-numeric characters long. Special characters are allowed. Required for local users. This field does not display for external users.
Confirm Password (Local Authentication only)	Type the password a second time. Required for local users. This field does not display for external users.
Policy (Local Authentication only)	Password policy to associate with this user account. From the list, select from the policy you want to associate. Optional. This field does not display for external users.  The system calculates the expiration date from the first date that the user logs on with this password.
Authentication Host (External Authentication only)	The Lightweight Directory Access Protocol (LDAP) server on which the user is being authenticated. The server(s) listed in this field are specified in the authentication_policy.properties.in file.
Session Timeout	Amount of time in minutes that you can be inactive before you have to log in again. Time is in minutes. Required.
Accessibility	Portion of the dashboard user interface that the user account has access to. Optional.  The following are accessibility options: <ul style="list-style-type: none"><li>• Admin UI – Accesses the Admin Console pane in the dashboard only.</li><li>• AS2 UI – Accesses the AS2 Edition interface only.</li><li>• Dashboard UI – Accesses dashboard interface. Refine by choosing a Dashboard Theme.</li></ul>

Field	Description
Dashboard Theme	<p>Predefined dashboard that the user account has access to. Required if accessibility is set as Dashboard UI.</p> <p>The following are dashboard theme options:</p> <ul style="list-style-type: none"> <li>• Default</li> <li>• Operator</li> <li>• Participant</li> <li>• Participant Sponsor</li> <li>• Sponsor</li> <li>• AFT</li> </ul>
Given Name	User's first name. Required.
Surname	User's last name. Required.
E-mail	User's e-mail address.
Pager	User's pager number.
Preferred Language	<p>Set value to <b>Use Client Application Settings</b>.</p> <p><b>Note:</b> This value directs Sterling B2B Integrator to use the language specified in the user's browser and/or the locale of the client's operating system.</p> <p><b>Note:</b> This is the default value.</p>
Manager ID	User ID of the user's manager.
Identity	<p>Identity of the trading partner to associate with the user account. Only one trading partner can be associated with a user account. A user account can be associated with many groups, each with its own trading partner identity association. This enables a user account to be associated with more than one trading partner. The Identity field is used for routing messages in Mailbox. Select a trading partner identity from the list.</p> <p>The default value is Hub Organization.</p>

To create a user account:

### Procedure

1. From the **Administration Menu**, select **Accounts > User Accounts**.
2. Next to **Create a new Account**, click **Go!**
3. In the New Account page, select the **Authentication Type**.
4. Enter the **User ID**.
5. Enter the **Password**.
6. Confirm the Password.
7. Select the **Policy**.
8. Enter the **Session Timeout**.
9. Select the **Accessibility**.
10. Select the **Dashboard Theme**.
11. Click **Next**.

12. On the SSH Authorized User Key page, assign one or more public keys. Move the keys by from the **Available** pane to the **Assigned** pane and click **Next**.
13. On the Groups page, assign groups of permissions. Move the group names from the **Available** pane to the **Assigned** pane and click **Next**.
14. On the Permissions page, assign individual permissions. Move the permissions from the **Available** pane to the **Assigned** pane and click **Next**. By default, the permissions associated with the groups that this user is assigned to, are already selected. The required permissions are Admin Web App Permission and MyAccount.
15. On the User Information page, enter the **Given Name**.
16. Enter the **Surname**.
17. Enter the **E-mail address**.
18. Enter the **Pager number**.
19. Select the **Preferred Language**. Select the value **Use Client Application Settings**.

**Note:** This value directs Sterling B2B Integrator to use the language specified in the user's browser and/or the locale of the client's operating system.

20. Enter the **Manager ID**.
21. Select the **Identity**.
22. Click **Next**
23. Review the user account settings.
24. Click **Finish**. The user account is created and this message is displayed:  
The system update completed successfully.

If you created an external user, log out of the system, and then log back in with the external user ID or account. The system will authenticate the external user ID on the external LDAP server.

## Edit User Accounts

You can edit a user account from the **Administration** menu.

### About this task

**Note:** While multiple foreign languages are supported, one user account should not be used with more than one specific language to avoid user interface display issues.

To edit a user account:

### Procedure

1. From the **Administration Menu**, select **Accounts > User Accounts**.
2. Locate the user account you want to edit by using either the Search or List options.
3. Click **edit** for the user account you want to edit.
4. Make any changes to the authentication type for this user.  
If you change the authentication type from external to local, you need to create a password for the user. If you change the authentication type from local to external, you cannot change the user's password or password policy.
5. Make any changes to the **New Password** and confirm the new password.

6. Make any changes to the **Policy**.
7. Make any changes to the **Session Timeout** and click **Next**.
8. Make any changes to the **SSH Authorized User key** and click **Next**.
9. Make any groups changes and click **Next**.
10. Make any permissions changes and click **Next**.  
You cannot remove the Admin Web App Permission or MyAccount.
11. Make any changes to the user information and click **Next**.

**Note:** For user accounts displaying the user interface in a supported foreign language, verify the Preferred Language value is set to **Use Client Application Settings**. This value directs Sterling B2B Integrator to use the language specified in the user's browser and/or the locale of the client's operating system.

12. Review the user account settings.
13. Click **Finish**.

## Delete User Accounts

You can delete a user account from the **Administration** menu.

### About this task

To delete a user account:

#### Procedure

1. From the **Administration Menu**, select **Accounts > User Accounts**.
2. Locate the user account that you want to delete by using either the Search or List options.
3. Click **delete** for the user account you want to delete.
4. Click **OK**.
5. Review the user account settings.
6. Click **Delete**. The selected user account is deleted and this message is displayed:  
The system update completed successfully.

## Update My Account Information

My Account information is associated with your user name and password, so when you log in, your personal information displays in the My Account page. You can edit your own account information and change the initial page that you see when you log in to the system.

### About this task

There are many instances when personal account information changes requiring you to edit your account information. In addition, you may need to change your password for security purposes.

**Note:** While multiple foreign languages are supported, one user account should not be used with more than one specific language to avoid user interface display issues.

To update your account information:

## Procedure

1. From the **Administration Menu**, select **Accounts > My Account**.
2. If you want to update your account password, in the **Old Password** field, enter your current password and enter a new password in the **New Password** field. Enter the new password again in the **Confirm New Password** field.
3. Enter any changes in the **Given Name**, **Surname**, **E-mail**, or **Pager** fields.
4. To change the **SSH Authorized User Keys** assigned to this account, move keys from the Available to the Assigned panes.
5. To change the **Preferred Language**, select a language.

**Note:** For user accounts displaying the user interface in a supported foreign language, verify the value is set to **Use Client Application Settings**. This value directs Sterling B2B Integrator to use the language specified in the user's browser and/or the locale of the client's operating system.

6. To change the **Welcome Page** (Admin Console Home) that displays when you log in, select from the list.
7. To change the number of processes displayed at one time on the Current Processes page, select a new value for **Page Size for Current Processes**.
8. To change the number of documents displayed at one time on the Current Documents page, select a new value for **Page Size for Current Documents**.
9. If you want to reuse browser windows to launch shortcuts, select **Reuse windows for launching shortcuts**.
10. If you want the system to autocomplete searches based on strings that you have entered previously, then select **Autocomplete for searches**.
11. If you want the system to remember the search-by values, select **Remember search-by values**. This option saves the last value you typed in each of the Search fields.
12. Click **Save**. The new account information is saved and this message is displayed:  
Your update has completed successfully.

## User account user exits for login (V5.2.5 and higher)

Sterling B2B Integrator provides for Active Directory sync user exits, which you can use to manage your user accounts with Active Directory instead of the Sterling B2B Integrator user interface. These user exits can be configured by IBM Services during an IBM Services Customer Engagement. Contact your IBM Sales Representative for more information.

User Exit	Description
IUserLoginUserExit_preAuthenticate	Use to insert custom code before authentication.
IUserLoginUserExit_postAuthenticateFail	Use to insert custom code after a success authentication.
IUserLoginUserExit_postAuthenticateSuccess	Use to insert custom code after a failed authentication.

## User account user exits for logout (V5.2.6 and higher)

Sterling B2B Integrator provides for Active Directory sync user exits, which you can use to manage your user accounts with Active Directory instead of the Sterling



B2B Integrator user interface. These user exits can be configured by IBM Services during an IBM Services Customer Engagement. Contact your IBM Sales Representative for more information.

User Exit	Description
ILogoutUserExit_OnSessionInvalidate	Use to insert custom code before the session is invalidated.

---

## Single Sign On

### Single Sign On

Single Sign On (SSO) is an authentication process that enables users to access several applications and must enter only one user name and password. Previously, a user who is logged in to each application and had to manage several user names and passwords.

User authentication for SSO does not require the LDAP adapter, which is used with business processes to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).

Sterling B2B Integrator allows SSO through integration with Netegrity SiteMinder, or through custom implementation classes for SSO plug-ins on other single sign on applications and servers.

Single sign on is limited to the following components:

- Administration Interface
- Mailboxing Interface
- Dashboard Interface
- Advanced File Transfer (AFT) Interface
- MyAFT Interface

### Single Sign On Provider Default Class

The SSO login URL for all interfaces except dashboard is similar to the normal login interface. The dashboard interface URL is `http:Host:port/dashboard/sso.jsp`. The request header for the dashboard interface must have the value `SM_USER=SSO User Name` (or the value can be configured in `security.properties` file under `SSO_USER_HEADER`).

The `SSOProviderDefault` interface allows the Single Sign On (SSO) plug-in to handle the single sign on function for Netegrity SiteMinder.

You can configure the SSO to redirect to an external HTTP page (instead of the Sterling B2B Integrator logoff page) after the user logs off from an SSO session. The external page from the SSO server can be either a login or logoff page.

The following example shows the `SSOProviderDefault.java` class:

```
package com.sterlingcommerce.server_name.security.authentication;
import javax.servlet.*;
import javax.servlet.http.*;
import com.sterlingcommerce.server_name.security.SecurityManager;
import com.sterlingcommerce.server_name.util.frame.log.Logger;
import java.util.Properties;
import com.sterlingcommerce.server_name.util.frame.Manager;
```

```

import java.util.*;
/**
 * Default Single Sign On implementation for ISSOProvider that will use
 * Request Header to get SSO_USER
 *
 * @author developer name
 */
public final class SSOProviderDefault implements ISSOProvider {
    private static final String CLASS_NAME = "SSOProviderDefault";
    private static final Logger LOG = SecurityManager.getInstance().getLogger();
    private static final Logger AUTHLOG =
        SecurityManager.getInstance().getAuthenticationLogger();
/**
 * Authenticate SSO processing (login)
 *
 * @param Request : The http request.
 *
 * @return String : The SSO User ID if the authentication is passed
 *                  : null if authentication is denied
 * << No Exception thrown for the default SSO Provider - Either have value or null >>
 */
public String authenticate(HttpServletRequest request)
    throws SSOAuthenticationException, SSOException
{
    String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (AUTHLOG.isDebugEnabled) {
        AUTHLOG.logDebug(CLASS_NAME + " Authenticate user tag : " +
            SecurityManager.getInstance().getSSOAuthenticationHeader() +
            " value : " + sso_user);
    }
    return sso_user;
}
/**
 * AuthenticatePage SSO processing (Page)
 *
 * @param Request : The http request.
 *
 * @return boolean : True if the SSO authentication on the Page is passed or no Page
 *                  authentication is needed because not enable or not SSO User.
 *                  : False if authentication is denied
 *                  (Must throw SSOException if return false!!!!)
 */
public boolean authenticatePage(HttpServletRequest request)
    throws SSOAuthenticationException, SSOException
{
    return true; // Always pass Page Validation for SSOProviderDefault
    /****** Uncomment if want to do SSO_USER_HEADER (SM_USER) check on Page
String sso_user =
request.getHeader(SecurityManager.getInstance().getSSOAuthenticationHeader());
    if (sso_user != null) {
        passed = true;
    } else {
        passed = false;
        throw new
SSOAuthenticationException(ISSOProvider.REASON_SSO_AUTHENTICATION_FAILURE);
    }
    return passed; *****/
}
/**
 * When user logs out, calling this to do any extra actions
 *
 * @param Response : The http response
 * @param Request : The http request.
 * @param int reason : An id to to tell where we called from
 * @param String : The String identify the session type: WS, DASHBOARD, MAILBOX,
 *                AFT, MYAFT, or null if don't know

```

```

*
* @return boolean : True if executes sucessfully,
*                 False if not & should use default logout logic
*
*/
public boolean invalidate(HttpServletRequest request, HttpServletResponse response,
int reason, String sessionType)
{
    HttpSession session = request.getSession(false);
    String forward = "SSO_FORWARD_URL";
    if (sessionType != null) {
        forward = forward + ".";
        forward = forward + sessionType;
    }
    if (reason == REASON_GIS_SESSION_EXPIRED) {
        forward = forward + ".GIS_TIMEOUT";
    }
    else if (reason == REASON_LOGOUT) {
        forward = forward + ".LOGOUT";
    }
    else { // Others reason : send all to VALIDATION_FAILED
        forward = forward + ".VALIDATION_FAILED";
    }
    String forwardUrl = getForwardURLParameter(forward);
    if (AUTHLOG.debug) {
        AUTHLOG.logDebug(CLASS_NAME + " Forward properties: " + forward +
" is forwardUrl: " + forwardUrl);
    }
    if (forwardUrl != null) {
        try {
            // Dashboard Timeout - Use JSP to kick outof IFrame
            if ((reason == REASON_GIS_SESSION_EXPIRED)&&
(sessionType != null) &&
(sessionType.equalsIgnoreCase(DASHBOARD_SESSION))) {
                if (AUTHLOG.debug) {
                    AUTHLOG.logDebug(CLASS_NAME + " Set ExternalSsoUrl = "
+ forwardUrl); }
                request.setAttribute("ExternalSsoUrl", forwardUrl);
                return false; // Set to false, we need to handle redirect in JSP
            } else {
                response.sendRedirect(response.encodeRedirectURL(forwardUrl));
            }
        } catch (Exception e) {
            return false;
        }
    }
    return true;
}
return false; // Use default logic (ie: GIS Logout/Login Page)
}
}

```

## Single Sign On Plug-in Components

Sterling B2B Integrator allows a custom implementation class for Single Sign On (SSO) plug-ins on other single sign on applications and servers. You must add an implementation class `SSO_AUTHENTICATION_CLASS`.<n>=<New class entry> in `security.properties` file to implement an SSO plug-in.

You can write custom implementation classes for SSO plug-ins based on the following `ISSOProvider.java` interface class.

### SSOProvider.java interface class

```

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,
HttpServletRequest response, int reason, String sessionType)
throws SSOAuthenticationException;
public boolean authenticatePage(HttpServletRequest request)
throws SSOAuthenticationException, SSOException;
}

```

### SSOException class

```

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

```

### SSOAuthenticationException class

```

public class SSOAuthenticationException extends SSOException { }

```

### User Authentication Method

The authenticate method is initialized during login. The authenticate method returns the user ID after successful authentication. The SSOAuthenticationException is thrown for unsuccessful authentication. The exception should contain an appropriate reason code and a redirecting page to handle if SSO headers are present. If SSO headers are not present, the control is passed back to the system login screen.

### Page Authentication Method

The authenticatePage method will be initialized on each page. Any additional validation during page transition from the SSO server is handled in this method. For example, you can ping SSO server to check if the SSO session has timed out. For unsuccessful authentication, an exception should be thrown, which should contain an appropriate reason code and a redirecting page.

### SSO Requests That are Invalid

The invalidate method is initialized when the user logs off, fails to authenticate login or page, or when the session expires. The HTTP redirection method should be performed for invalidating SSO requests. The following methods are initialized for unsuccessful authentication:

- If the SSO server authentication is successful and the Sterling B2B Integrator authentication is unsuccessful, the REASON\_GIS\_AUTHENTICATION\_FAILURE method is initialized with the reason code.
- If the SSO server authentication is unsuccessful, the REASON\_SSO\_AUTHENTICATION\_FAILURE method is initialized with the reason code.
- If the user logs off, the REASON\_LOGOUT method is initialized with the reason code.
- If the HTTP session expires, the REASON\_HTTP\_SESSION\_EXPIRED method is initialized with the reason code.

- If the user's SSO session expires, the REASON\_SSO\_SESSION\_EXPIRED method is initialized with the reason code.

## Single Sign On with Netegrity SiteMinder Checklist

Before you can configure Single Sign On (SSO), you must know SSO and of Netegrity SiteMinder.

Use this checklist to configure SSO with Netegrity SiteMinder:

Task	Single Sign On with Netegrity SiteMinder Checklist	Notes
1	Install Netegrity SiteMinder and configure it with a reverse proxy server.	
2	Configure the Properties Files for use with Netegrity SiteMinder.	
3	Configure the Netegrity Secure Proxy Server.	
4	Create Netegrity Server Secure Realms.	

For custom implementation of SSO plug-ins for other single sign on applications and servers, see Single Sign On Plug-in Components.

## Single Sign On with IBM Global High Availability Mailbox (V5.2.6 or later)

Sterling B2B Integrator users with the appropriate permissions can directly access the IBM® Global High Availability Mailbox management tool by single sign-on from Sterling B2B Integrator to manage the Global Mailbox.

### Before you begin

Sterling B2B Integrator users must belong to one of the following groups to directly access the Global Mailbox management tool from Sterling B2B Integrator:

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

### About this task

When you choose to access the Global Mailbox management tool by single sign-on, your new session of Global Mailbox is opened in a new web browser tab, while your Sterling B2B Integrator session remains available.

You can access Global Mailbox by single sign-on only from Sterling B2B Integrator. If you sign out of the Global Mailbox management tool, you are not signed out of your Sterling B2B Integrator session.

If you want to change your Global Mailbox administrator password, you must directly sign in to the Global Mailbox management tool.

**Restriction:** If you sign in to the Global Mailbox management tool by single sign-on, you cannot change your Global Mailbox administrator password, and **Change password**, in the **Administrator** menu, is not available.

To access the Global Mailbox management tool by single sign-on:

### Procedure

1. From the Admin Console page, expand **Deployment** in the Administration Menu.
2. Expand **Global Mailbox**.
3. Select **Mailbox Administration**.
4. Click the **Launch Global Mailbox Management Tool** hyperlink to open a new session in the Global Mailbox management tool.

**Remember:** When you click the **Launch Global Mailbox Management Tool** hyperlink, a new session of Global Mailbox opens in a new web browser tab.

## Configure Properties Files for Single Sign On with Netegrity SiteMinder

You can configure properties file for single sign-on with Netegrity SiteMinder.

### About this task

To edit the neo-ui.properties and security.properties files:

### Procedure

1. Stop Sterling B2B Integrator.
2. Navigate to `/install_dir/install/properties`.
3. Open the neo-ui.properties file.
4. Add the associated SSO entry for each interface. The following code sample shows the associated entry to the same HTTP sites:

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

5. Save and close the neo-ui.properties file.
6. Open the `/install_dir/install/properties/security.properties` file in a text editor.

7. In security.properties, locate the ## SSO Authentication configuration parameters, as shown in the following code sample:

```
## SSO Authentication configuration
## enable sso authentication (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true
## enable sso authentication on each Page (true, false) default=false
#SSO_PAGE_AUTHENTICATION_ENABLED=false
## http header variable that contains externally authenticated userid
SSO_USER_HEADER=SM_USER
## List of SSOProvider Classes that are supplied to use - If SSO Authentication is
## enable, should have at least one class, the following is the default one that we
## supplied.
## SSO_AUTHENTICATION_CLASS.1= <SSOProvider Class 1> Will try to use this first
## SSO_AUTHENTICATION_CLASS.2= <SSOProvider Class 2> Will try to use this if first
## one failed
## SSO_AUTHENTICATION_CLASS.3= <SSOProvider Class 3> Will try to use this if second ## one failed too
## SSO_AUTHENTICATION_CLASS.<n>= <SSOProvider Class n> Will try to use this if all
## first -1 classes failed
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SSOProviderDefault
## External Page for SSO when Logout (Specify the SSO Server external page for each of
## the cases)
## Example: SSO_FORWARD_URL.MAILBOX.LOGOUT=http://sterlingcommerce.com
## After SSO User logout from Mailbox, instead of display the Mailbox Login Screen
## display IBM Web page.
SSO_FORWARD_URL.AFT.LOGOUT=
SSO_FORWARD_URL.MYAFT.LOGOUT=
SSO_FORWARD_URL.MAILBOX.LOGOUT=
SSO_FORWARD_URL.WS.LOGOUT=
SSO_FORWARD_URL.DASHBOARD.LOGOUT=
## Default handling for LOGOUT if don't know source
SSO_FORWARD_URL.LOGOUT=
## External Page for SSO when Timeout (Specify the SSO Server External page for each ## of the case)
SSO_FORWARD_URL.AFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MYAFT.GIS_TIMEOUT=
SSO_FORWARD_URL.MAILBOX.GIS_TIMEOUT=
SSO_FORWARD_URL.WS.GIS_TIMEOUT=
SSO_FORWARD_URL.DASHBOARD.GIS_TIMEOUT=
## Default handling for TIMEOUT if don't know source
SSO_FORWARD_URL.GIS_TIMEOUT=
## External Page for SSO on Validation/Authentication failure (SSO User Validation
## Failed - At login or Page Validation)
SSO_FORWARD_URL.AFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MYAFT.VALIDATION_FAILED=
SSO_FORWARD_URL.MAILBOX.VALIDATION_FAILED=
SSO_FORWARD_URL.WS.VALIDATION_FAILED=
SSO_FORWARD_URL.DASHBOARD.VALIDATION_FAILED=
##Default handling for VALIDATION FAILED if don't know source
SSO_FORWARD_URL.VALIDATION_FAILED=
```

8. Below the ##SSO Authentication configuration entry, make the following changes to the SSO parameters:

Parameter	Description	Shipped Value	New Value
SSO_AUTHENTICATION_ENABLED	Enables or disables the use of SSO.	False	True
SSO_USER_HEADER	User header name from Netegrity SiteMinder or your SSO application configuration.	SM_USER  This is the value in Netegrity SiteMinder.	Must match the entry in Netegrity SiteMinder or your SSO application.

Parameter	Description	Shipped Value	New Value
SSO_PAGE_AUTHENTICATION_ENABLED	Enables or disables SSO authentication on every page	False	True—To authenticate SSO on every page.  Change only if custom SSO Provider Class is provided.
SSO_AUTHENTICATION_CLASS.n	Implementation class to provide authentication support.	com.sterling commerce.woodstock. security.authentication .SSOProviderDefault	Select from the list of supplied SSOProvider classes.
SSO_FORWARD_URL URL	Displays the URL page provided after you log off from Mailbox. Otherwise displays the default.	Commented  Displays default page.	Provide the URL.

9. Save and close the security.properties file.
10. Start Sterling B2B Integrator.

## Configure Netegrity Secure Proxy Server

You can configure the Netegrity Secure Proxy Server by adding forwarding rules to the proxyrules.xml file.

### About this task

Before you configure the Netegrity Secure Proxy Server, you must:

- Install Sterling B2B Integrator on a server such as acme.si.com.
- Know the port number that the Mailbox Browser Interface (MBI) is installed on. You must use this information in the appropriate forwarding rules.
- Know the port number that the Sterling B2B Integrator Dashboard user interface is installed on. You must use this information in the appropriate forwarding rules.

To configure the Netegrity Secure Proxy Server:

### Procedure

1. Add the necessary forwarding rules for Sterling B2B Integrator to the /opt/netegrity/proxy-engine/conf/proxyrules.xml file.

The following example shows how the completed proxyrules.xml file should look after you add the forwarding rules to access Sterling B2B Integrator components:



```

<?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. Add the following to the lines to the proxyrules.xml file to turn off the Cross Server Scripting checking in the secure proxy server, since Sterling B2B Integrator does not support Netegrity Cross Server Scripting policy enforcement.

```

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

```

3. Save and close the proxyrules.xml file.

## Create Netegrity Policy Server Secure Realms

The Netegrity Policy Server Administrator must create Secure Realms around each of the URL patterns forwarded by the Secure Proxy Server. These Security Realms need the necessary rules assigned for authentication and authorization.

### About this task

In addition, the Web agent in the Secure Proxy Server must be configured to communicate with the Policy Server.

Create a secure realm for each URL pattern listed:

URL Pattern	Enables Access To:
/mbi/*	Application Mailbox interface

URL Pattern	Enables Access To:
/dashboard/*	Application dashboard interface, using the http://host:port/dashboard format
/datastore/*	Datastore components
/portlets/*	Application portlet components in the dashboard interface
/help/*	Context-sensitive help components
/webxtools/*	Web Extensions Utilities
/gbm/*	Graphical Process Modeler components

---

## Passwords

### Password Policies

Password policies are sets of security decisions that you make and apply to different user accounts according to security policies in your company. These choices include such items as the number of days a password is valid and the maximum and minimum length of a password.

You can use password policies to streamline your security operations when adding new users. Instead of adding having individual policies for each individual user, you can create one password policy and apply it to all users that require the same access.

After you create a password policy, you can apply it only to internal user accounts. This provides you the greatest flexibility in maintaining your security policies. If you are using LDAP, you cannot apply password policies to your external accounts.

The default values for the password policy are:

Parameter	Default Value
Policy ID	default_user
Policy Name	Default User Policy
Number of days valid	60
Minimum Length	6
Maximum Length	28
Number of passwords kept in history	5
Password required to contain special characters	Selected
Required password change in first login attempt	Selected

Password policies tasks include:

- Create a password policy
- Search for a password policy
- Edit a password policy
- Delete a password policy
- Edit the lock out parameter

- Edit the password expires message

## Custom Password Policy

The Sterling B2B Integrator Custom Password Policy is a security feature that adds more password policy rules. These additional password rules can help you prevent the use of weak, easily-hacked passwords and reject non-compliant passwords.

To enable this functionality, you need to:

- Implement some custom Java code via a plug-point. Once enabled, the plug-point is used for all users in the system associated with a password policy (this is a global setting).
- Add the `passwordPolicyExtensionImpl` property to the `customer_overrides.properties` file.
- Apply the custom password policy to User Accounts.

The custom password policy extension is applied prior to the default password policy. If a password violates more than one policy requirement (one enforced by the extension class and another enforced by the default implementation) only the error message returned from the extension class is displayed to the user.

## Example: Password Policy Example

This example shows a possible setting for a password policy.

For example, a password policy named Test may have the following settings for a password:

- Valid for 10 days
- Minimum of 10 characters in length
- Maximum of 20 characters in length
- Must have at least two special characters
- User must change default password during initial login
- Number of passwords to keep in history

Using the preceding example, the user is given a user name and a password by the system administrator. The user logs in using the user name and password provided and is prompted to change the password. If the user fails to provide a password with at least 10 characters, more than 20 characters, or without at least two special characters, the system prompts the user for corrections. Once all conditions set in the password policy are met by the user changing the password, the system saves the new password and allows the user access. Each user account can have only one password policy associated with it, but you can apply one password policy to multiple user accounts.

In addition to the password policy changes in the interface, you can change the number of times that a user can fail to log in correctly before locking the user account of the user that is attempting to log in.

For example, if the number of consecutive login attempts before failing is set to three, and you type the wrong password three times, you cannot log in using that specific computer. You can log in using any other computer that has access to the system.

## Installation Password or Passphrase

During installation, you create a system passphrase for your Sterling B2B Integrator installation. The passphrase is a highly complex string longer than 16 characters. The system passphrase is required to start the system and to access protected system information.

The only person who can update or change the passphrase is the person who created/installed the software. If you lose or forget your passphrase, you will not be able to start the system. The only user that can update the system passphrase is the user that performed the installation.

The system passphrase is not stored by the system, except on Windows installations, where it is stored in an obfuscated form in `security.properties` to facilitate the system running as a non-interactive service. It can be stored in the clear on other platforms in `security.properties` so you do not have to enter it on the command line when you start the system. However, the system passphrase is only protected by operating system file access control.

## Custom Policy Password Checklist

You can implement a custom policy password.

Use the following checklist to implement a custom password policy:

Task	Custom Policy Password Checklist
1	Create a directory structure within <code>&lt;SI_Install_Dir&gt;</code> for test, policy, and extension.
2	Create the java class within the extension directory.
3	Specify the Java class implementing the password policy ( <code>passwordPolicyExtensionImpl</code> property) in the <code>customer_overrides.properties</code> file.
4	Add the implementation class jar to the classpath.
5	Define error message.

## Example - Custom Policy Password

This example shows a custom policy password extension.

This is an example of a custom policy password extension.

The interface `com.sterlingcommerce.woodstock.security.PasswordPolicyExtension` was added to the system as follows:

```

public interface IPasswordPolicyExtension {
    /**
     * Implements extended validation on passwords and
     returns null if password
     * validation is successful. If validation fails,
     an error message key
     * that may be looked up in Login_*.properties* should
     be returned.
     * @param password - The password string to validate
     * @param policyId - The PWD_POLICY.POLICY_NAME of
     the policy associated with the user in case the extension needs
     it.
     * @return String Return null if password validation
     was successful, the error message key if password validation fails
     */
    public String validateNewPassword (String password,
String policyName);
}

```

Returning null from the method indicates that the password was accepted.  
Returning anything else means the password was not valid.

### Example Implementation

```

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

```

## Search for Password Policies

You can search for a password policy from the **Administration** menu.

### About this task

To search for a password policy:

### Procedure

1. From the **Administration Menu**, select **Accounts > Password Policy**.
2. In the Password Policy page, complete one of the following actions:
  - Under Search in the **Password Policy Name** field, enter a portion of the name or the entire name of the password policy you are searching for and click **Go!** The Password Policy page lists all of the permissions that match your search criteria.

- Under List in the **Alphabetically** field, select **ALL** or the letter that begins the name of the password policy for which you are searching and click **Go!** The Password Policy page lists all of the permissions that match your search criteria.

## Create Password Policies

You can create a password policy to assign the policy to user accounts. You do not need to associate a password policy with a user account, but it does help in managing your security.

### About this task

Before you begin, you need the following information:

Field	Description
Policy ID	ID that identifies the password policy in the database.
Policy Name	Policy name that displays in the user interface when any reference is made to the password policy.
Number of days valid	Number of days that a user password is valid. The default is 0, which means the password never expires.  If you supply a value between 1 and 999, the user is prompted to change the password when this time period expires. The expiration count down starts the first time a user logs in after a password is assigned to the user account.
Minimum Length	Minimum length that the password must be. Required. Valid values are any numerals. This number must be set to at least the number 6. The default value is 6. If no policy is applied, the system enforces a minimum length of 6.
Maximum Length	Maximum length that the password can be. Required. Valid values are any numerals. This number must be set to at least the same number as the minimum length. The default value is 28.
Number of passwords kept in history	Number of passwords to keep in the PWD_HISTORY table in the database for a user. After this number of passwords is exceeded, the oldest password is removed from the table and can be re-used by the user. The default value is 0.
Password required to contain special characters	Specifies that the password must contain at least one special character. Valid values include numerals, capital letters, !, @, #, \$, %, ^, &, or *.
Required password change on first login attempt	Specifies that the user must change the default password after the initial log in. This prompts the user to change the password after logging in for the first time.

To create a password policy:

### Procedure

1. From the **Administration Menu**, select **Accounts > Password Policy**.
2. Next to **Create a new Password Policy**, click **Go!**
3. In the Password Policy page, enter the **Policy ID**.
4. Enter the **Policy Name**.
5. Enter the **Number of days valid**.

6. Enter the **Minimum Length**.
7. Enter the **Maximum Length**.
8. Enter the **Number of passwords kept in history**.
9. If the password is required to contain special characters, select the checkbox.
10. If the user is required to change the password change on first login attempt, select the checkbox.
11. Click **Next**.
12. Review the password policy settings.
13. Click **Finish**.

## Edit Password Policies

You can edit the password policy from the **Administration** menu.

### About this task

To edit the password policy:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Password Policy**.
2. Locate the password policy you want to edit by using either the Search or List options.
3. Click **edit** for the password policy you want to edit.
4. In the Password Policy Settings page, make the appropriate changes and click **Next**.
5. Review the password policy settings.
6. Click **Finish**.

The following message is displayed:

The system update completed successfully.

## Delete Password Policies

If you delete a password policy, user accounts that are associated with that specific password policy can still log in, but the user is not forced to change the password. If the user does change the password, no validation is completed against the new password.

### About this task

To delete a password policy:

#### Procedure

1. From the **Administration Menu**, select **Accounts > Password Policy**.
2. Locate the password policy you want to delete by using either the Search or List options.
3. Click **delete** for the password policy you want to delete.
4. In the Confirm page, click **Delete**.

The following message is displayed:

The system update completed successfully.

## Change the Number of Days for User Password Expiration

The system notifies you of impending password expirations by placing a message in the System Alerts section of the Admin Console home page. System administrators can change the number of days before expiration for users to be notified.

### About this task

The message states that your password will expire in a specific number of days. Each day, the number is reduced by one, until the day that the password expires, when you are prompted to change your password.

System administrators can change the number of days prior to expiration in the `ui.properties.in` file. You should make all changes to the `ui.properties.in` file and not the `ui.properties` file. If you make the changes to the `ui.properties` file and restart the system, the changes you made to the `ui.properties` file are overwritten by the `ui.properties.in` file.

To change the number of days for the password expiration:

### Procedure

1. Stop Sterling B2B Integrator.
2. Navigate to `/install_dir/install/properties`.
3. Open the `ui.properties.in` file.
4. Locate the `MsgPwdExpires= 15` entry.
5. Change the 15 to the new number of days for the user password expiration.
6. Save the file.
7. Navigate to `/install_dir/install/bin`.
8. Enter `setupfiles.sh`.
9. Restart Sterling B2B Integrator. The changes you made in the `ui.properties.in` file are applied to the `ui.properties` file and are in effect for all user accounts.

## Reset Your Own Password After Lockout

If you are locked out, you can log in using any other computer, wait 30 minutes for the lock to expire, or contact the system administrator to remove the lock.

### About this task

If you are locked out:

- Log in using any other computer that has access to the system.
- Wait 30 minutes and the lock expires allowing you to try to log in using the locked computer again.
- Contact the system administrator to have the lock removed through the Lock Manager page. This allows you to try to log in using the locked computer again.

## Define Error Message for Custom Password Policy

You can define error message for a custom password policy extension.



## About this task

Error messages inform the user of password rules and lists the reasons for rejected password changes. The custom password error messages are defined in the `Login_language_dir.properties_uniqueID_ext` files. If custom-specific text is not provided, the default error message is returned to the user. The `Login_language_dir.properties_uniqueID_ext` file is not part of the default system code. It must be created after the initial system installation and populated to match your environment.

To define error message for a custom password policy extension:

### Procedure

1. Navigate to the `/install_dir/install/properties/lang/language_dir` directory. Where `language_dir` is the language set for the customer's locale (for example, `en`, `ja`, `fr`).
2. Edit the `Login_language_dir.properties_uniqueID_ext` file. Where `language_dir` is the language set for the customer's locale and `<filename>` is the unique identifier for the new custom password extension. For example: `Login_en.properties_custompasswd_ext`.
3. Add an entry to the file for the error condition set in the custom extension file and define the descriptive string to return to the user. For example, `nogood = The password must contain a minimum of one lower case character, one upper case character, and one digit or special character.`
4. Save and close the file.

## Specify the Custom Password Policy Extension in the `customer_overrides.property` file

You can specify the Java class that implements the password policy extension.

### About this task

To plug in the custom implementation, the Java class name needs to be specified in the `passwordPolicyExtensionImpl` property in the `customer_overrides.properties` file.

To specify the Java class implementing the password policy extension:

### Procedure

1. Navigate to the installation directory.
2. Navigate to the properties directory.
3. Edit the `customer_overrides.properties` file.
4. Add the `passwordPolicyExtensionImpl` property at the end of the file and enter the name of the Java class implementing the extended validation of passwords. For example, `security.passwordPolicyExtensionImpl=test.policy.extension.PwdPolExtnImpl.`
5. Save and close the file.

## Add the Implementation class JAR to the Classpath for the Custom Password Policy

For a custom password policy, you must add the implementation class JAR to the classpath.

## About this task

The extension implementation class must be compiled and jarred as follows:

### Procedure

1. Navigate to *SI\_Install\_Dir*.
2. Enter the following command to compile the custom class file:  

```
javac -cp /SI_Install_Dir/jar/platform_ifcbase/1_3/platform_ifcbase.jar  
test/policy/extension/*.java
```
3. Create the jar file by running the following command from within *SI\_Install\_Dir* :  

```
jar cf any_filename.jar absolute_path_to_custom_class_file.class
```

 where *any\_filename.jar* is the name of the new jar file to be created and where *absolute\_path\_to\_custom\_class\_file.class* is the name of the custom implementation Java class file. For example: 

```
jar cf userExit.jar  
test/policy/extension/PwdPolExtnImpl.class
```
4. Navigate to *SI\_Install\_Dir/bin* directory.
5. Enter the following command to add the newly created jar to the classpat:  

```
./install3rdParty.sh userExit 1_0 -j  
path_to_jar_that_was_created_in_step3
```

 for example, 

```
./install3rdParty.sh userExit 1_0 -j SI_Install_Dir/  
userExit.jar
```

---

## LDAP Authentication

### Lightweight Directory Access Protocol (LDAP) as an Authentication Tool for Sterling B2B Integrator

Lightweight Directory Access Protocol (LDAP) is a set of protocols that are used to access information that is stored in an information directory, which is an LDAP directory.

An LDAP directory is a database, but not a relational database, used to manage information that is spread across multiple servers on a network and is optimized for read performance.

You can use LDAP to delegate authentication of an external user account to an LDAP directory and to provide authentication using the same security information used for other applications in your company. If your company has already adopted LDAP, you can use your existing LDAP directories.

User account authentication does not require the LDAP adapter, which is used with business processes to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).

If your LDAP server is not working, users who have internal accounts retain access; however, those users who have external accounts do not have access until the LDAP server is working.

Before you can configure LDAP with Sterling B2B Integrator, you must have:

- Knowledge of LDAP
- Access to an installed and configured LDAP server containing user information

- The location of the LDAP server
- (For SSL) Installed security certificates in the Keystore and Truststore
- Created the external user accounts for each user that will authenticate through your LDAP server
- (For SSL) The location of your Keystore and Truststore

## Example: LDAP Authentication Configuration Parameters

This example shows the LDAP Authentication configuration parameters.

The following example shows the LDAP Authentication configuration parameters:

```
## GIS/LDAP Authentication configuration
## optional ssl (jsse) java system properties for locating and using
## the trustStore and the keyStore
## one set of keystore and truststore properties for all LDAP configuration.
# LDAP_SECURITY_TRUSTSTORE=/home/applications/properties/cacerts
# LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit
# LDAP_SECURITY_KEYSTORE=/home/applications/properties/keystore
# LDAP_SECURITY_KEYSTORE_PASSWORD=password
#####
#
# GIS Authentication Configuration
#
#####
authentication_0.className=com.sterlingcommerce.woodstock.security
.GISAuthentication
authentication_0.display_name=GIS Authentication
#####
#
# For additional LDAP Server Authentication Configuration,
# copy-paste the following set of properties and uncomment all properties
# that start with "authentication_<number>". Replace the <number>
# tag with the additional number for the authenticationmethod. For example,
# if the last authentication method is "authentication_0", then you should
# replace the <number> tag with "1" for your next new LDAP authentication
# method.
# Then you have to change each property with the properLDAP server information.
#
# You can comment out or leave blank the "authentication_<number>
# .security_protocol"
# property if you are not going to use SSL for the security protocol.
#
# The authentication_1 LDAP authentication propertieswould be replaced if
# the customer already used LDAP authentication as configuredin security
# .properties.
#
#####
#####
#
# LDAP Server <number> Authentication Configuration
#
#####
# authentication_<number>.className=com.sterlingcommerce.woodstock.security
# .LDAPAuthentication
# authentication_<number>.display_name=LDAP Serveragrona <number>
## enable ldap authentication (true, false) default=false
# authentication_<number>.enabled=true
## jndi parameters for ldap connections
# authentication_<number>.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory
# authentication_<number>.server=acme.inc.com
# authentication_<number>.port=636
# authentication_<number>.security_type=simple
# authentication_<number>.principle=cn=Manager,dc=acme,dc=inc,dc=com
# authentication_<number>.credentials=SecretPassword
```

```

## comment out or leave as blank on this property if the server is not
## going to use SSL for the security protocol.
# authentication_<number>.security_protocol=ssl
## search parameters for user password
# authentication_<number>.password_attribute=userPassword
# authentication_<number>.search_root=dc=acme,dc=inc,dc=com
# authentication_<number>.search_filter=(uid=<userid>)
# authentication_<number>.with_user_bind=false
Below the ##LDAP Authentication

```

## LDAP Authentication Configuration Checklist

You can configure LDAP with Sterling B2B Integrator.

Use this checklist to configure LDAP with Sterling B2B Integrator:

Tasks	LDAP Configuration Checklist
1	Configure LDAP in one of the following modes: <ul style="list-style-type: none"> <li>• Password Comparison Mode</li> <li>• Password Binary Mode</li> </ul>
2	Configure LDAP with Sterling B2B Integrator
3	Verify LDAP configuration
4	Optional. Encrypt LDAP passwords.

## Configure LDAP in Password Binding Mode

You can configure LDAP in a password binding mode by entering your **user ID** and **password** from your external account.

### About this task

To configure LDAP in a password binding mode:

### Procedure

Enter your **user ID** and **password** from your external user account. The system:

- Attempts to bind to the LDAP repository with credentials enabling execution of necessary queries.
- Searches for the user in the LDAP directory with the proper userid.
- Retrieves the user's distinguished name (DN) from the LDAP directory.
- Attempts to bind to the LDAP repository using the user's DN and password.
- Success – The system binds to the LDAP repository as a user.
- Failure – The system cannot bind to the LDAP repository as a user.

## Configure LDAP in Password Comparison Mode

You can configure LDAP in a password comparison mode.

### About this task

To configure LDAP in a password comparison mode:

### Procedure

1. Enter your **user ID** and **password** from your external user account.

2. The system attempts to bind to the LDAP repository with credentials enabling execution of necessary queries.
3. The system searches for the user in the LDAP directory with the proper userid.
4. The system retrieves the user password from the LDAP directory.
5. The system compares the password supplied by the user with the password retrieved from the LDAP directory. If the passwords match, you are authenticated and permitted access to the system. If the passwords do not match, you are not authenticated and not permitted access.

## Configure LDAP with Sterling B2B Integrator

To configure Sterling B2B Integrator to use LDAP, you must edit the `authentication_policy.properties.in` file. You can also use the `customer_overrides.properties` file to set property values that cannot be overwritten by a patch installation.

### About this task

To configure LDAP authentication:

### Procedure

1. Stop Sterling B2B Integrator.
2. Navigate to the installation directory.
3. Navigate to the properties directory.
4. Open the `authentication_policy.properties.in` file.
5. In `authentication_policy.properties.in`, locate the `## GIS/LDAP Authentication` configuration entry.
6. Below the `##GIS/LDAP Authentication` configuration entry, make the following changes to the LDAP parameters:

Parameter	Description	Shipped Value	Change to
<code>#LDAP_SECURITY_TRUSTSTORE</code>	Path to the local truststore. You must have LDAP required certificates stored in the truststore. You cannot use certificates from trading partners. Optional. Use only if you are using SSL.	Inactive path	Full path to the local truststore.
<code>#LDAP_SECURITY_TRUSTSTORE_PASSWORD</code>	Password that allows access to the truststore. Optional. Use only if you are using SSL.	<code>changeit</code>	Password allowing access to the local truststore.
<code>#LDAP_SECURITY_KEYSTORE</code>	Path to the local keystore. You must have LDAP required certificates stored in the keystore. You cannot use certificates from trading partners. Optional. Use only if you are using SSL.	Inactive path	Full path to the local keystore.
<code>#LDAP_SECURITY_KEYSTORE_PASSWORD</code>	Password that allows access to the keystore. Optional. Use only if you are using SSL.	<code>password</code>	Password allowing access to the local keystore.

Parameter	Description	Shipped Value	Change to
#authentication_<number>.enabled	Enables or disables the use of LDAP.  False – All users who are created from this authentication host will be disabled (fail to log in).  True – Each user can be accessed either internally or externally, but not both, since each user ID is unique. This value is not checked when it is for internal authentication.	False	True
#authentication_<number>.jndi_factory	Class name of the factory class that creates the initial context for the LDAP service provider. This is the standard context factory shipped with the JDK.	com.sun.jndi.ldap.LdapCtxFactory	No change
#authentication_<number>.server	URL specifying the host name of the LDAP server.	Inactive path	Local LDAP host URL.
#authentication_<number>.port	The port number of the LDAP server.		
#authentication_<number>.security_type	Authentication method for the provider to use. The system supports only simple authentication.	simple	No change
#authentication_<number>.principle	Identity of the principle to authenticate, which enables the system to perform queries. This parameter is the name component in an LDAP ASN.1 bind request.	cn=Manager, dc=amr, dc=stercomm, dc=com	Local naming information.
#authentication_<number>.credentials	Password set up in the LDAP repository for the LDAP principle, which enables the system to perform queries.	SecretPassword	Local password that goes with your local principle.
#authentication_<number>.security_protocol	Object specifying which security protocol for the provider to use.	SSL	No change. This parameter is not visible if you have chosen not to use SSL.
#authentication_<number>.password_attribute	Name of the LDAP attribute that contains the user password.  This parameter is only used if the  #LDAP_AUTHENTICATE_WITH_USER_BIND is set to false.	userPassword	Local attribute that contains the password.

Parameter	Description	Shipped Value	Change to
#authentication_<number>.search_root	Object specifying the root from which the user query is based.	dc=amr, dc=stercomm, dc=com	Local search path.
#authentication_<number>.search_filter	Object specifying the template to use in the search. The <userid> value is dynamically replaced at request time with the userid of the user requesting authentication.	(uid=<userid>)	A Windows Active Directory server may use an entry such as (sAMAccountName=<userid>)
#authentication_<number>.with_user_bind	Specifies whether to authenticate a user according to a successful bind.  False – The system extracts the value of the user password from the LDAP server and performs a comparison to the user credentials provided.  True – The system binds to the LDAP server using the user's distinguished name and provided credentials. A successful bind means a successful authentication.	false	Change to true if you want to authenticate with the user bind.

7. Save the authentication\_policy.properties.in file.
8. Enter `/install_dir/install/bin/setupfiles.sh` (UNIX) or `\install_dir\install\bin\setupfiles.cmd` (Windows) to update LDAP entries into the authentication\_policy.properties file from the authentication\_policy.properties.in file.
9. Start Sterling B2B Integrator.  
The changes to the authentication\_policy.properties file are applied and you can now begin using your LDAP server to authenticate users.  
After startup, the system identifies LDAP servers from the authentication\_policy.properties file. The system authenticates external users when the users log in.

## Verify LDAP Configuration

To verify that you configured the LDAP correctly with Sterling B2B Integrator, review the Authentication.log file under User Authentication to ensure that the system accepted the LDAP configuration.

### About this task

If there are problems connecting to the LDAP directory or LDAP authentication fails, check the DEBUG log statements in the Authentication.log file to troubleshoot the issue. The Authentication.log file records all login attempts, whether successful or unsuccessful.

## Encrypt LDAP Passwords

You can hide LDAP-related passwords in property files by encrypting them in the `customer_overrides.properties` file.

### About this task

The following parameters (properties) can be used to be encrypted the LDAP passwords in the `customer_overrides.properties` file:

Parameter/property	Description
<code>authentication_policy.authentication_1.credentials</code>	This parameter or property governs the principal password necessary to access an LDAP instance. This should be secured since no password that governs security and access should be exposed in plain text.
<code>authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD</code>	This parameter or property governs the password for the trust store (JKS format) used for securing LDAP connections. The passphrase for this JKS must be supplied so that the trust store can be accessed since it is an encrypted file.
<code>authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD</code>	This parameter or property governs the password if client-based SSL authentication is used to secure connections to a given LDAP instance.

To encrypt LDAP passwords:

### Procedure

1. Navigate to the bin directory.
2. Use the `encrypt_string.[sh/cmd]` to determine the real value of the property/parameters you want to encrypt.
3. Update the parameters/properties in `customer_overrides.properties` file to have following entries. Replace all `<ENCVAL>` with the encrypted value of the non-encrypted string commented out for that property using the `bin/encrypt_string.sh` (or `.cmd`). For example:

```
authentication_policy.LDAP_SECURITY_TRUSTSTORE=&INSTALL_DIR;/../  
woodstock2/com/sterlingcommerce/woodstock/security/units/cacerts  
# non-encrypted  
#authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=changeit  
# encrypted  
authentication_policy.LDAP_SECURITY_TRUSTSTORE_PASSWORD=<ENCVAL>  
authentication_policy.LDAP_SECURITY_KEYSTORE=&INSTALL_DIR;/../woodstock2/  
com/sterlingcommerce/woodstock/security/units/keystore  
# non-encrypted  
#authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=password  
# encrypted  
authentication_policy.LDAP_SECURITY_KEYSTORE_PASSWORD=<ENCVAL>  
authentication_policy.authentication_2.display_name=LDAP Server agrona 2  
authentication_policy.authentication_2.enabled=true  
authentication_policy.authentication_2.jndi_factory=com.sun.jndi.ldap.LdapCtxFactory  
authentication_policy.authentication_2.server=agrona.sci.local  
authentication_policy.authentication_2.port=18100  
authentication_policy.authentication_2.security_type=simple  
authentication_policy.authentication_2.principle=cn=Manager,dc=amr,dc=stercomm,dc=com  
# non-encrypted  
#authentication_policy.authentication_2.credentials= Sterling  
# encrypted  
authentication_policy.authentication_2.credentials=<ENCVAL>  
authentication_policy.authentication_2.security_protocol=ssl
```



```

authentication_policy.authentication_2.password_attribute=userPassword
authentication_policy.authentication_2.search_root=dc=amr,dc=stercomm,dc=com
authentication_policy.authentication_2.search_filter=(uid=<userid>)
authentication_policy.authentication_2.with_user_bind=false
authentication_policy.authentication_2.className=com.sterlingcommerce.woodstock.security
.LDAPAuthentication

```

---

## User News



### User News

The User News feature enables you to post messages to the Admin Console home pages. User news makes it possible to inform users about changes to or to remind them of important events and tasks.

Messages can be posted:

- For all users
- For a specific user
- Multiple users

The news item is displayed based on an effective date and expiration date. You can also set the message up as:

Message Type	Symbol	Description
Notice		Provides announcement information of general or low priority.
Alert		Provided announcement information of high priority.

You must have write permissions for Accounts to create user news messages. Deleting old messages reduces storage requirements and the amount of effort required to retrieve specific messages.

User News tasks include:

- Create a User News Message for Specific Users
- Create a User News Message for All Users
- Search for a User News Message
- Edit a User News Message
- Delete a User News Message

### Create User News Messages for All Users

You can create user news messages for all users from the **Administration** menu.

#### About this task

Before you begin, you need to know the following information:

Field	Description
Type	Type of message you are creating. Valid values are Notice and Alert.
Subject	Subject of the message you are creating.
Message	Body of the message you are creating.

## Procedure

1. From the **Administration Menu**, select **Accounts > User News**.
2. Next to **New Message**, click **Go!**
3. Enter the **Type**.
4. Enter **Subject**.
5. Enter **Message**.
6. Click **Next**.
7. Select **ALL Users** and click **Next**.
8. Enter the **Effective Date** of the message (yyyy-mm-dd).
9. Enter the **Expiration Date** of the message (yyyy-mm-dd).
10. Click **Next**.
11. Review the News Message Settings.
12. Click **Finish**.

## Create User News Messages for Specific Users

You can create user news messages for specific users from the **Administration** menu.

### About this task

Before you begin, you need to know the following information:

Field	Description
Type	Type of message you are creating. Valid values are Notice and Alert.
Subject	Subject of the message you are creating.
Message	Body of the message you are creating.

## Procedure

1. From the **Administration Menu**, select **Accounts > User News**.
2. Next to **New Message**, click **Go!**
3. Enter the **Type**.
4. Enter the **Subject**.
5. Enter the **Message**.
6. Click **Next**.
7. Select **Selected Users**.
8. Select each user's name that you want to receive this message.
9. Click **Next**.
10. Enter the **Effective Date** of the message (yyyy-mm-dd).
11. Enter the **Expiration Date** of the message (yyyy-mm-dd).
12. Click **Next**.
13. Review the News Message Settings.
14. Click **Finish**.

## Search for User News Messages

You can search for a user news message from the **Administration** menu.

## About this task

To search for a user news message:

### Procedure

1. From the **Administration Menu**, select **Accounts > User News**.
2. Use one of the following Search Options:

User News Search Options	Action
by User ID	Select either ALL or the specific user from the list.
by Subject	Enter a portion of the message text.
by Effective Date Range	Enter the date range (mm/dd/yyyy).

3. Click **Go!** The User News page list all of the messages that match your search criteria.

## Edit User News Messages

You can edit a user news message from the **Administration** menu.

### About this task

To edit a user news message:

### Procedure

1. From the **Administration Menu**, select **Accounts > User News**.
2. Search for the user news message you want to edit.
3. Click edit for the user news message you want to edit.
4. Update the type of message, subject or message, if required.
5. Click **Next**.
6. Update the users who will receive this message, if required and click **Next**.
7. Update the **Effective Date** of the message (yyyy-mm-dd), if required.
8. Update the **Expiration Date** of the message (yyyy-mm-dd), if required.
9. Click **Next**.
10. Review the News Message Settings.
11. Click **Finish**.

## Delete User News Messages

You can delete a user news message from the **Administration** menu.

### About this task

To delete a user news message:

### Procedure

1. From the **Administration Menu**, select **Accounts > User News**.
2. Search for the user news message you want to delete.
3. Click **delete** for the news message you want to remove.
4. Review the News Message Settings.
5. Click **Delete**. The following message is displayed:

## Document Encryption

### Document Encryption Feature Overview

Document encryption is a feature that is provided with Sterling B2B Integrator that configures an extra layer of security beyond the traditional file and database permissions. If you integrate Sterling File Gateway with Sterling B2B Integrator, it uses the same document encryption feature for protecting data at rest.

Sterling File Gateway is an application for securely transferring files between partners using different protocols, file naming conventions, and file formats.

The document encryption feature is intended to protect data at rest from snooping. The feature allows you to encrypt the payload data stored in the database and/or the file system. It is also designed to prevent someone outside the system from viewing the payload data by directly accessing the database or file system.

Important aspects of document encryption:

- The default configuration at installation is no encryption. If you want to have your documents encrypted, you will need to turn on this feature.
- You can turn this feature on at any time, but only documents received after encryption is turned on are encrypted.
- Once you turn on this feature, encryption is for all payloads across the entire system.
- Only the document payload data is encrypted, **not** the meta data.
- The same encryption key is used to encrypt and decrypt.
- The system uses a predefined certificate (doccrypto) to encrypt documents. You can create a different system certificate. If you do you must update the value of CERT\_NAME in the customer\_overrides.properties file.

While performance is impacted when encryption is enabled, each customer will see different performance impacts depending on hardware, the number and size of documents being processed, and the relative amount of processing time spent by a given server doing document persistence and retrieval against other activities.

### Encryption Key for Document Encryption

The same encryption key is used to encrypt and decrypt database or file system documents. The digital certificate is used to generate and encrypt the keys, and the system passphrase is used to encrypt the digital certificates.

Document encryption creates one key per document and this key is stored along with the document as part of the metadata. Digital certificates are stored like any other system certificate.

The system uses a predefined certificate (doccrypto) to generate and encrypt the keys that are used to encrypt the documents. You can create a different system certificate. If you do you must update the value of CERT\_NAME in the customer\_overrides.properties file.

## Assign a Different Certificate for Document Encryption

The system uses a predefined certificate (doccrypto) to encrypt documents. You can create a different system certificate to use for encrypting documents, for example, if the previous certificate is expiring. If you do, you must update the value of CERT\_NAME in the customer\_overrides.properties file.

### About this task

**CAUTION:** Do not delete or rename the previous system certificate. You need the previous certificate for decrypting documents that were previously encrypted by it. Your new system certificate cannot decrypt these documents, as it was never used to encrypt them.

Before you perform this procedure, you need to:

- Generate the new certificate
- Know the name of the certificate

To update the value of CERT\_NAME:

### Procedure

1. Navigate to the install directory.
2. Navigate to the properties directory.
3. Open the customer\_overrides.properties file.
4. Add the following line to the file:  
`security.CERT_NAME=name_of_new_system_certificate`
5. Save and close the customer\_overrides.properties file.
6. Stop and restart Sterling B2B Integrator.

## Enable Document Encryption for File System and Database Documents

You can encrypt file system and database documents from the properties directory.

### About this task

To encrypt file system and database documents:

### Procedure

1. Navigate to the install directory.
2. Navigate to the properties directory.
3. Open the customer\_overrides.properties file.
4. Add the following line to the file.  
`security.ENC_DECR_DOCS=ENC_ALL`
5. Save and close the customer\_overrides.properties file.
6. Stop and restart Sterling B2B Integrator.

## Enable Document Encryption for Database Documents

You can encrypt database documents from the install directory.

## About this task

To encrypt database documents:

### Procedure

1. Navigate to the install directory.
2. Navigate to the properties directory.
3. Open the customer\_overrides.properties file.
4. Add the following line to the file.  
`security.ENC_DECR_DOCS=ENC_DB`
5. Save and close the customer\_overrides.properties file.
6. Stop and restart Sterling B2B Integrator.

## Enable Document Encryption for File System Documents

You can encrypt file system documents from the install directory.

### About this task

To encrypt file system documents:

### Procedure

1. Navigate to the install directory.
2. Navigate to the properties directory.
3. Open the customer\_overrides.properties file.
4. Add the following line to the file.  
`security.ENC_DECR_DOCS=ENC_FS`
5. Save and close the customer\_overrides.properties file.
6. Stop and restart Sterling B2B Integrator.

## Disable Document Encryption for Documents

You can disable document encryption from the properties directory.

### About this task

The default configuration at installation is no encryption.

To disable document encryption:

### Procedure

1. Navigate to the install directory.
2. Navigate to the properties directory.
3. Open the customer\_overrides.properties file.
4. Update the value of ENC\_DECR\_DOCS to NONE. For example:  
`security.ENC_DECR_DOCS=NONE`
5. Save and close the customer\_overrides.properties file.
6. Stop and restart Sterling B2B Integrator.

---

## Certificates

### Digital Certificates

Use the IBM Key Management Utility (iKeyman) to help you manage your digital certificates.

The system uses the following types of digital certificates:

- CA and trusted certificates – Digital certificates for which the system does not have the private keys. These certificates are stored in standard DER format.
- System certificates – A digital certificate for which the private key is maintained in the system. These certificates are stored with the private key in a secure format.

The following is some basic information about how digital certificates are used:

- Every organization exchanging secure documents must have a certificate. Use iKeyman to generate the certificate or it can be generated externally. For information about iKeyman, see “IBM Key Management Utility (iKeyman)” on page 59.
- Every trading profile for a trading partner with whom you exchange signed and encrypted documents must have a certificate.
- An organization or trading profile can have only one active certificate at a time. In the case of dual certificates, an organization can have one active pair of certificates; one for signature, one for encryption.
- An organization or trading profile must have an active certificate to successfully exchange signed and encrypted documents.
- An organization or trading profile can have multiple valid certificates.
- Certificates can be used to sign documents you transmit by all transport methods.
- The key length for a certificate does not have to be the same as that of a trading partner certificate.
- Before you set the validity period for the certificate, it is recommended you read and apply the best practice recommendations from the Microsoft PKI Quick Guide. For information about the best practice recommendations for using certificates, see <http://www.windowsecurity.com/articles/Microsoft-PKI-Quick-Guide-Part3.html>.

### Supported Digital Certificates

Sterling B2B Integrator supports version 3 X.509 of digital certificates. Digital certificates can be either self-signed or CA-signed.

- A self-signed certificate is a digital certificate that is signed with the private key that corresponds to the public key in the certificate, demonstrating that the issuer has the private key that corresponds to the public key in the certificate.
- A CA-signed certificate is a digital certificate that is signed by using keys maintained by certificate authorities. Before issuing a certificate, the CA typically evaluates a certificate requestor to determine that the requestor is in fact the certificate holder referenced in the certificate.

### CA Certificates

A CA certificate is a digital certificate issued by a certificate authority (CA). The CA verifies trusted certificates for trusted roots. Trusted roots are the foundation upon which chains of trust are built in certificates.

Trusting a CA root means that you trust all certificates issued by that CA. If you elect not to trust a CA root, Sterling B2B Integrator does not trust any certificates issued by that CA.

CA certificates contain a public key corresponding to a private key. The CA owns the private key and uses it to sign the certificates it issues. To validate a trusted certificate, you must first check in a CA certificate.

Root certificates from common CAs are contained in a Java keystore (JKS) in the JVM that ships with Sterling B2B Integrator. This allows users to establish some authority-based trust relationships more easily than if they had to search for and obtain the certificates from a CA Web site.

CA certificates are stored separately from trusted certificates in the product.

From the user interface, you can check in CA root certificates that originate from any of the following sources:

- Common CA root certificates shipped with Sterling B2B Integrator in the JKS keystore.
- Only certificates and trusted certificates are recognized. Certificates and private keys are not visible to the UI.
- SSL certificates imported from trading partners.
- Other certificates obtained externally.

Based on security policies at your site, CA certificates in the JKS keystore can also be checked in through the console. Although CA certificates are public documents, you must be careful about who has rights to add them. Someone could maliciously add a false CA certificate in order to verify false end-user certificates.

### **CA Certificate Names**

The CA certificate name is not part of the content of the certificate. They are built from the issuer Relative Distinguished Name (RDN) and serial number of the certificate. However, certificates from the JKS keystore are named with an arbitrary string.

Because the certificate name is stored in the system database and is used as the alias to refer to the certificate in the GUI, you may want to rename CA certificates with shorter or more meaningful names based on your file naming conventions. Certificates can be renamed when checked in or when edited.

## **Benefits of Self-signed and CA-signed Digital Certificates**

Depending on your needs, there are pros and cons to self-signed versus CA-signed digital certificates.

When you and your trading partners are deciding whether to generate a self-signed certificate or purchase a signed certificate from a CA, consider the following:

- You can easily create self-signed certificates using Sterling B2B Integrator. However, these self-signed certificates are not verified by a trusted third party.
- The primary advantage of using certificates from a CA is that the identity of the certificate holder is verified by a trusted third party. The disadvantages include extra cost and administrative effort. If you decide to use a third-party certificate, obtain it from a CA.



- A CA provides a centralized source for posting and obtaining information about certificates, including information about revoked certificates.

By default, the system trusts all CA certificates and self-signed certificates generated by the application. You can, however, specify whether all or some certificates issued by a specific CA should be trusted. You also explicitly cannot trust a self-signed certificate of a trading partner.

## Expiration Dates for Certificates

If an adapter and servlet are used for inbound communications, you must monitor the expiration dates of the system certificates to ensure that the certificates are valid. Before the certificates expire, they must be replaced with valid certificates.

## System Certificate Parameter Definitions

If an adapter and servlet are used for inbound communications, you must monitor the expiration dates of the system certificates to ensure that the certificates are valid. Before the certificates expire, they must be replaced with valid certificates.

Parameter	Description
alias	The key name stored in the HSM. Use only alias names containing characters a-z, A-Z, 0-9 or hyphen (-), and whose total length is no longer than the system GUID length.
certname	Name to assign to the system certificate in the database.
Certype	The certificate type to import. Four types of certificate files are supported: pkcs12, pkcs8, pem, and keystore. Sterling B2B Integrator only supports pem keys encrypted with DES or 3DES.  Use keystore to list or import the keystore.
file	Name of the File to import.
keypass	PIN for the slot on the Eracom device.
keystoretype	Keystore type to import. Valid value is CRYPTOKI.
keystoreprovider	Provider type. Eracom is the only HSM supported provider type.  Valid values are: <ul style="list-style-type: none"> <li>• ERACOM</li> <li>• ERACOM.n (if you are importing certificates to a slot other than the first position)</li> </ul>
password	Store passphrase for the certificate file.
pkcs12file	Name of the PKCS12 file to import.
pkcs12storepass	Store passphrase used for the generation of the PKCS12 file.
pkcs12keypass	Valid passphrase for the PKCS12 file.
storepass	PIN for the slot on the Eracom device where the keystore resides.
systempass	System passphrase.

## IBM Key Management Utility (iKeyman)

IBM Key Management Utility (iKeyman) is a component of the IBM SDK that generates keys, certification requests, and self-signed certificates.

You can use iKeyman to create certificates to secure communications, and to encrypt and decrypt data. In a secure transfer using SSL, certificates provide an added level of security.

In Sterling B2B Integrator, you can use iKeyman to create:

- **Certificate Signing Requests (CSRs)** – A file to be sent by e-mail to a certificate authority to request an X.509 certificate.
- **Key certificates** – A combination of an ASCII-encoded certificate and an ASCII-encoded PKCS12 encrypted private key. If you generate key certificates using the standard format (default) with certain ciphers, the output certificate will error when imported into the Sterling B2B Integrator. PKCS12 is the recommended format for the key certificates.

For more information about configuring and using iKeyman, see iKeyman Overview for IBM SDK, Java Technology Edition 7.0.0

## Certificate Tasks

### Create a Self-Signed Certificate

You can create a self-signed certificate from the **Administration** menu.

#### About this task

To create a self-signed certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Create Self-signed Certificate**, click **Go!**
3. Enter the **Name** of the self-signed certificate.
4. Enter the name of the originating **Organization**.
5. Select the **Country** or origin of the self-signed certificate.
6. Enter a contact **e-mail** address for the person responsible for certificates in the organization and then click **Next**.
7. Enter the **Serial Number** for the certificate. The serial number is the number you want to assign to the self-signed certificate.
8. Enter the number of days (**Duration**) that the self-signed certificate is valid.  
  
**Note:** In V5.2.6.2 or later, the maximum expiration date is *Jan 1, 2080*. Any duration entered that would result in an expiration date beyond Jan 1, 2080 is defaulted to *Jan 1, 2080*. In earlier releases, there is no upper limit.
9. Enter the **IP addresses** of the network interfaces you want to associate with the certificate as the SubjectAltName field.
10. Enter the **DNS Names** of the network interfaces you want to associate with the certificate as the SubjectAltName field.
11. Select the **Key Length**. Select one of the following key lengths:
  - 512
  - 1024

- 2048

**Note:** The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 2048 is the most secure, but also the slowest, and may not work with some applications.

**Note:** If you select the key length 512, you must also use JDK 7 SR5. JDK 7 SR7 FP1 does not support key lengths below 1024.

12. Select the **Signing Algorithm**.
13. Select the **Validate When Used** option. Validation options are:
  - Validity – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - Auth Chain – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
14. Set the **Certificate Signing Bit** by selecting the checkbox.
15. Click **Next**.
16. Review the information about the self-signed certificate.
17. Click **Finish**.

### **Obtain Trusted Certificate Automatically from Trading Partners**

The Certificate Capture Utility automates the process of obtaining an SSL certificate from a trading partner. This method of obtaining certificate information allows a partner to easily connect and save a certificate.

#### **About this task**

If desired, an out-of-band security check can then be made before the certificate is checked into the system as a CA or Trusted certificate.

Before you begin:

- Verify that your partner's host system is SSL-enabled.
- Obtain host and port information for your trading partner's server.
- If FTPS mode will be used, determine whether mode will be explicit or implicit.
- Configure the default SSLCertGrabberAdapter service instance to use the appropriate perimeter server and (HTTPS only) proxy server. See the adapter documentation for details.

To obtain the SSL certificate automatically from a trading partner:

#### **Procedure**

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > Certificate Capture Utility**.
2. Next to **Capture Partner Certificate**, click **Go!**
3. Select the connection type for the server and click **Next**.
  - FTPS
  - HTTPS
4. Enter the **Host name** or **IP address**.
5. Enter the **Port** number.
6. Select the connection mode for FTPS (if you are using HTTPS, skip this step):

- Explicit – SSL negotiation occurs after the FTP connection is established. Default.
  - Implicit – SSL negotiation occurs before the FTP connection is established.
7. Click **Next**. The system attempts to connect and retrieve certificates.
  8. After the capture is complete, review the summary information and decide which certificates you want to save.
  9. Select an encoding method for each certificate and click **Save**. Encoding formats are:
    - BASE64 – Uses BASE64 encoding on the standard DER certificate. Default.
    - DER – Standard format for digital certificates, accepted by most applications.
  10. Click **Save** and browse to the location where you want to save the file.
  11. Accept the default file name or edit it according to your file naming conventions and click **Save**.
  12. After saving, the certificates may be checked in into the system. If you decide to check a certificate into the system:
    - a. Verify that each certificate is valid and trusted.
    - b. Check in the certificate as a CA or a Trusted certificate, depending on function. For Certificate Authority-based trust, you may need to check in the certificate chain, excluding the end user certificate. For direct trust, check in the end user certificate.

## Configure Status Information on Certificate Summaries

By default, certificate status information is provided at the end of the summary pop-up window when a hyperlinked certificate name is selected. You can include or exclude the status information. Because the status information is compiled in real time, you might not want to include it.

### About this task

The `VerificationOnPopupInfo` property controls whether the status information is displayed in the certificate summary. This property is in the `ui.properties` file. Values for the `VerificationOnPopupInfo` property are:

- `true` - include validation information (default)
- `false` - do not compile or display validation information in the pop-up window
- (any other value) - include validation information

To prevent the compilation and display of the status information:

### Procedure

1. Open the `ui.properties` file.
2. Update the value of `VerificationOnPopupInfo` to be `false`. For example:  
`VerificationOnPopupInfo=false`
3. Save and close the file.
4. Restart Sterling B2B Integrator.

## Configure Thumbprint Displays

In addition to the precomputed SHA1 hash, extra certificate thumbprints can be included in certificate display, confirmation, and summary screens. Hash computations are done on demand when a display is generated.

## About this task

Additional thumbprints display on GUI screens, but have no effect upon message handling or system communication.

To configure the system to compute and display additional certificate thumbprints:

### Procedure

1. In the ui.properties file, modify this line:

```
AddtlCertThumbprintAlgs=hash_algorithm
```

To display more than one additional hash, separate the values with commas.

For example:

```
AddtlCertThumbprintAlgs=SHA384,SHA512
```

Parameter	Description
hash_algorithm	Name of a hash algorithm to be applied to the certificate thumbprint. Valid values are: <ul style="list-style-type: none"><li>• SHA-256</li><li>• SHA-384</li><li>• SHA-512</li></ul>

2. Save and close ui.properties file.
3. Restart Sterling B2B Integrator.

## Search for CA Certificates

You can search for a CA certificate from the **Administration** menu.

### About this task

To search for a CA certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Complete one of the following and then click **Go!**
  - Under Search in the **by Certificate Name** field, enter a portion of the name or the entire CA certificate name you are searching for. The CA Digital Certificates page lists all CA certificates that match your search criteria.
  - Under List in the **Alphabetically** field, select **ALL** or the letter that begins the name of the CA certificate you are searching for. Selecting ALL lists all CA certificates. The CA Digital Certificates page lists all CA certificates that match your search criteria.

## View CA Certificate Summary Information

When a list of certificates is displayed, you can click the certificate name to view summary information about that certificate. You can configure the system name, the thumbprint, and the status.

## About this task

The following fields are configurable in the system.

Certificate Summary Field	Description
System Name	<p>The Certificate Name is the database label. It is used to refer to this certificate in the GUI and stores this name in its database.</p> <p>The default name for a certificate from the JKS keystore is an arbitrary string. Names for other certificates are built from the issuer relative distinguished name (RDN) and serial number of the certificate.</p> <p>You can change a certificate name to a shorter or more recognizable name when checking in or editing the certificate.</p>
Thumbprint	<p>Information for the SHA1 hash is included by default. To configure computation and display of thumbprint information for other hashes, edit the ui.properties file.</p>
Status	<p>A real-time check of current status, stating whether certificate dates are valid and the certificate has been verified. To configure whether or not this information is computed at the time of display, edit the ui.properties file.</p>

Although this information applies to summary information for a CA certificate, similar fields appear in summary and confirmation screens for other types of certificates.

## Check In CA Certificates from the User Interface

You can check in a CA certificate from the User Interface under the **Administration** menu.

### About this task

Based on security policies at your site, CA certificates in the JKS keystore can also be checked in through the console.

Before you begin, save any CA certificates that you have obtained externally to a local file.

To check in a CA certificate:

### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Check in New Certificate**, click **Go!**
3. Select a method to import certificates:

Import method	Next Steps
Import from JVM – Imports from the JKS keystore	<ol style="list-style-type: none"> <li>1. Click <b>Import</b> from <b>JVM</b>.</li> <li>2. Accept the default password that appears in the password field and click <b>Next</b>.</li> </ol> <p>The default keystore password is supplied by Sun Microsystems. If the password field is empty, the system still uses the default password.</p>
Import from File – Imports certificates saved as a file on a local drive	<ol style="list-style-type: none"> <li>1. Click <b>Import</b> from <b>File</b>.</li> <li>2. Enter the Filename or click <b>Browse</b> to select a CA certificate file. Click <b>Next</b>.</li> </ol> <p>You may ignore the password that appears in the password field. There is no need to erase the entry.</p>

Available certificates are listed with a summary of identifying information. All certificates are selected by default.

4. Click the check boxes to the left of each entry to select or de-select certificates to import.
5. For each certificate selected, accept the suggested Certificate Name or edit it based on your file naming conventions.
6. Select the **Validate When Used** option and click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Attempts to construct a chain of trust up to the root for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. If you receive a message stating that the certificate duplicates a certificate already in the database, enter Y or N to indicate whether to import the duplicate.

This check is done on single certificates only. It does not take place when checking in one or more certificates from a file.

Certificates are identified by SHA1 hash for purposes of determining duplicates. More than one copy of a certificate can be present in the database, since each will populate a different row and have a distinct object ID. The existing certificate is not overwritten.

8. Review the CA certificate information.
9. Click **Finish**.

### Check In CA Certificates from the Console

After you save any CA certificates to a local file, you can check in the CA certificate at the console from the installation directory.

### About this task

Common CA certificates are contained in a JKS keystore that is part of the JVM that is shipped with Sterling B2B Integrator. The JKS keystore is located at `/install_dir/jdk/jre/lib/security/cacerts`. You may also obtain certificates externally.

To import certificates into the Sterling B2B Integrator trusted repository, modify the command at `/install_dir/install/bin/ImportCACerts.sh` (UNIX) or `\install_dir\install\bin\ImportCACerts.cmd` (Windows).

Before you begin, save any CA certificates obtained externally to a local file.

To check in a CA certificate at the console:

### Procedure

1. Navigate to the installation directory.
2. Navigate to the bin directory.
3. Enter this command:  
(UNIX) `./ImportCACerts.sh`  
(Windows) `ImportCACerts.cmd`
4. All certificates in the file are listed, one at a time, with these exceptions:
  - Entries containing symmetric or private keys are not processed or listed.
  - Only the first certificate in a DER-format file is processed and listed.
5. Following the prompts, enter Y (not case-sensitive) for any certificate you want to import.
6. For each certificate accepted, accept the suggested Certificate Name or edit it based on your file naming conventions.
7. If the certificate label duplicates a label already in the database, enter Y or N (not case-sensitive) to indicate if you want to change the label. Although certificates are not generally identified by label and the database allows label duplicates, some services look up certificates by label. Avoid duplicate labels to avoid the possibility of unexpected behavior.
8. If the certificate duplicates a certificate already in the database (as indicated by the SHA1 hash of the certificate, specify with Y or N whether you want to import the duplicate.

Certificates are identified by SHA1 hash for purposes of determining duplicates. More than one copy of a certificate can be present in the database, since each will populate a different row and have a distinct object ID. The existing certificate is not overwritten.

### Edit CA Certificates

You can edit a CA certificate from the **Administration** menu.

#### About this task

To edit a CA certificate:

### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Using either Search or List, locate the CA certificate you want to edit and click **Go!**
3. Next to the **CA certificate** you want to edit, click **edit**.
4. Enter the Certificate Name.



5. Select the **Validate When Used** option and click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. Review the CA certificate information.
7. Click **Finish**.

## Delete CA Certificates

You can delete a CA certificate from the **Administration** menu.

### About this task

To delete a CA certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Alphabetically**, click **Go!**
3. Next to the CA certificate you want to delete, click **delete**.

## Search for System Certificates

You can search for a system certificate from the **Administration** menu.

### About this task

To search for a system certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. In the system certificates, complete one of the following actions and then click **Go!**
  - Under **Search**, in the **by Certificate Name** field, enter a portion of the name or the entire system certificate name you are searching for. The System Certificates page lists all of the system certificates containing the full or partial name you typed.
  - Under **List**, in the **Alphabetically** field, select **ALL** or the letter that begins the name of the CA certificate you are searching for. Selecting **ALL** lists all system certificates. The System Certificates page lists all of the system certificates that match your search criteria.

## Edit System Certificates

You can edit a system certificate from the **Administration** menu.

## About this task

To edit a system certificate:

### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Using either Search or List, locate the **system certificate** you want to edit and click **Go!**
3. Next to the system certificate you want to edit, click **edit**.
4. Enter the **Certificate Name**.
5. Select the **Validate When Used** option and click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
6. Review the system certificate information.
7. Click **Finish**.

## Identify System Certificates in Sterling B2B Integrator

You can identify a system certificate from the **Administration** menu.

## About this task

To identify a system certificate:

### Procedure

1. From the **Administration Menu**, select **Deployment > Services > Configuration**.
2. In the List section, select the applicable service or adapter type from the **by Service Type** list and click **Go!**
3. From the list of configurations, choose the configuration.
4. Click the **service name** to view configuration information.
5. Review the certificate summary information.

## Check the Expiration Date of a System Certificate

If an adapter and servlet are used for inbound communications, you must monitor the expiration dates of the system certificates to ensure that the certificates are valid.

## About this task

To check the expiration date of a system certificate:

### Procedure

1. Choose one:

- If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. To view all system certificates, select **All** from the Alphabetical drop-down list and click **Go!**
  3. Select the system certificate name you want to view. The Certificate Summary is displayed.
  4. In the **Description** section of the Certificate Summary, review information provided in the **Valid Dates** field.
  5. Review the information provided in the **Status** section to see if the dates are valid and the certificate has been verified.

### Export System Certificates in Sterling B2B Integrator

This export command is only applicable to Sterling B2B Integrator system certificates. You cannot use this command to export system certificates on HSM.

#### About this task

To export a system certificate, enter the following command, with the appropriate parameters:

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

Parameter	Description
keyname	Keyname of the system key to export.
pkcs12filename	Name of the file that contains exported information.
pkcs12storepass	Store password that protects the store.
pkcs12keypass	Key password that protects the key.

### Delete System Certificates in Sterling B2B Integrator

You can export a copy of the system certificate to your local disk before you delete it. The OpsDrv, OpsKey, and UIKeys are system certificates that cannot be deleted.

#### About this task

To delete a system certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Alphabetically**, click **Go!**
3. Next to the system certificate you want to delete, click **delete**.
4. Click **Delete** on the Confirm page.

## Check Out System Certificates

To export a system certificate, you must check out the certificate. This procedure exports only the public certificate, not the private key, and provides you with a public certificate to send to a trading partner.

### About this task

To check out a system certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Using either Search or List, locate the system certificate you want to check out.
3. Next to the system certificate you want to check out, click **check out**.
4. In the **Check Out System Certificate** dialog box, select the certificate format and then click **Go!**:
  - PKCS12 – This option formats the digital certificate as a PKCS12 file. You also have the option of entering a Private Key Password and a Key Store Password.
  - BASE64 – This option uses BASE64 encoding on the standard DER certificate.
  - DER – This standard format for digital certificates is accepted by most applications.
5. In the **File Download** dialog box, click **Save**.
6. In the **Save As** dialog box, select the location where you want to save the certificate, and then click **Save**. The option to open the certificate is not supported. You must open the certificate within the operating system. If you receive the error message, This is an invalid Security Certificate file, open the file in a text editor and delete any blank lines before -----BEGIN CERTIFICATE-----. Save the edited file and then try to open the file.
7. Click **Close** In the Check Out System Certificate dialog box. The System Certificate page is displayed.

## Search for Trusted Certificates

You can search for a trusted certificate from the **Administration** menu.

### About this task

To search for a trusted certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. In the Trusted Digital Certificates page, complete one of the following actions, and then click **Go!**:

- Under Search in the **by Certificate Name** field, enter a portion of the name or the entire trusted certificate name you are searching for. The Trusted Digital Certificates page lists all of the trusted certificates that match your search criteria.
- Under **List in the Alphabetically** field, select **ALL** or the letter that begins the name of the trusted certificate you are searching for. The Trusted Digital Certificates page lists all of the trusted certificates that match your search criteria.

## Check In Trusted System Certificates

You can check in trusted certificates such as SSL certificates imported from trading partners or other external certificates.

### About this task

Trusted certificates might originate from the following sources:

- SSL certificates imported from trading partners
- Other certificates obtained externally

Before you begin, save the trusted system certificate to a file on your local computer.

To check in a trusted system certificate:

### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Check in New Certificate**, click **Go!**
3. Enter the **Filename** or click **Browse** to select the file name of the trusted certificate and then click **Next**.
4. Enter the **Certificate Name**.
5. Verify the name of the trusted certificate you are checking in. For each certificate you selected, the Certificate Name field shows a suggested name, followed by a summary of the identifying information in the certificate. You can change the name based on your file naming conventions.
6. If you have more than one trusted certificate contained in the file you selected, select the check box to the left of each certificate to check in each certificate.
7. Select the **Validate When Used** option and click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Attempts to construct a chain of trust up to the root for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
  - **CRL cache** – Controls whether the CRL Cache is consulted each time the system certificate is used.
8. Review the trusted certificate information.
9. Click **Finish**.

## Edit Trusted Certificates

You can edit a trusted certificate from the **Administration** menu.

### About this task

To edit a trusted certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Using either Search or List, locate the trusted certificate you want to edit and click **Go!**
3. Click **edit** next to the trusted certificate you want to edit.
4. Enter the **Certificate Name**.
5. Select the **Validate When Used** option and click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Attempts to construct a chain of trust up to the root for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
  - **CRL cache** – Controls whether the CRL Cache is consulted each time the system certificate is used.
6. Review the certificate information.
7. Click **Finish**.

## Delete Trusted System Certificates

You can delete a trusted system certificate from under the **Administration** menu.

### About this task

To delete a trusted system certificate:

#### Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Alphabetically**, click **Go!**
3. Next to the trusted certificate you want to delete, click **delete**.

## Import PKCS12 System Certificates

You can import a PKCS12 system certificate.

### About this task

To import a PKCS12 system certificate:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter:

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

## Check In PKCS12 System Certificates

After you save the PKCS12 system certificate to a file on your local computer, you can check in the PKCS12 system certificate from under the **Administration** menu.

### About this task

Before you begin, you need to save the PKCS12 system certificate to a file on your local computer.

To check in a PKCS12 system certificate:

## Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. In the System Certificates page, under Check in, next to **PKCS12 Certificate**, click **Go!**
3. Enter the **PKCS12 Certificate Name**.
4. Enter the **Private Key Password**. This is the password used to encrypt the PKCS12 certificate.
5. Enter the **Key Store Password**. This is the password for the PKCS12 object. It may be the same as the private key password.
6. Enter the **Filename** or click **Browse** to select the file name of the PKCS12 certificate, and then click **Next**.
7. Select the **Validate When Used** option and then click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
8. Review the PKCS12 system certificate information.
9. Click **Finish**.

## Import Pem System Certificates

You can import a pem system certificate encrypted with DES or 3DES.

### About this task

Only pem keys encrypted with DES or 3DES are supported.

To import a pem system certificate:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter:  

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

## Import Key System Certificates

You can import a key system certificate.

### About this task

To import a key system certificate:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter:  

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

## Import Keystore System Certificates

You can generate a keystore system certificate on an HSM.

### About this task

To generate a keystore system certificate on an HSM:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter:  

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

## Check In Key System Certificates

After you save the key system certificate to a file on your local computer, you can check in the key system certificate from under the **Administration** menu.

### About this task

Before you begin, save the key system certificate to a file on your local computer.

To check in a key system certificate:

## Procedure

1. Choose one:
  - If you use Sterling B2B Integrator, from the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
  - If you use the AS2 Edition, from the **AS2 Administration** menu, select **Certificates**.
2. Next to **Key Certificate**, click **Go!**
3. Enter the **Certificate Name**.
4. Enter the **Private Key Password**. This is the password used to encrypt the private key.



5. Enter the **Filename** or click **Browse** to select the file name of the key certificate and click **Next**.
6. Select the **Validate When Used** option and click **Next**. Validation options are:
  - **Validity** – Verifies dates in the validity period of the certificate are still in effect. If the dates are not in effect, the certificate is not used.
  - **Auth Chain** – Constructs a chain of trust for certificates that are not self-signed. If a chain of trust cannot be constructed using valid certificates, the certificate is not used. If the certificate is self-signed, this option verifies only the certificate signature.
7. Review the key certificate information.
8. Click **Finish**.

## Online Certificate Status Protocol (OCSP)

### Online Certificate Status Protocol (OCSP) Support in Sterling B2B Integrator

The Online Certificate Status Protocol (OCSP) is a set of ASN.1 defined data structures for requesting and receiving information about certificate revocation status. These data structures can be sent and received by many transport protocols in principle. In practice, HTTP is used.

An OCSP client sends questions and processes responses. An OCSP responder answers questions and generates responses.

### OCSP Client Functionality

An OCSP client implementation consists of data structures for managing information about OCSP responders, functionality for generating OCSP requests, functionality for processing OCSP responses, and functionality for transmitting OCSP requests and receiving OCSP responses.

An OCSP client implementation consists of:

- Data structures for managing information about OCSP responders
- Functionality for generating OCSP requests
- Functionality for processing OCSP responses
- Functionality for transmitting OCSP requests and receiving OCSP responses

### How Sterling B2B Integrator Performs an OCSP Check

An OCSP check for a certificate in Sterling B2B Integrator is determined when the OCSP check within Sterling B2B Integrator is implemented as a part of internal system APIs used by services for getting certificates and keys from the database.

### About this task

OCSP checks are performed by Sterling B2B Integrator when methods are called to get certificates and keys from the objects that encapsulate them in the database.

The following steps describe how the OCSP check is implemented in Sterling B2B Integrator:

### Procedure

1. The system examines the object that encapsulates the certificate to determine if OCSP checking is enabled. This allows the system to decide with no additional database calls whether to attempt an OCSP check.

2. If OCSP checking is enabled, the system gets the encoded issuer name from a certificate.
3. The system hashes the encoded issuer name with SHA1.
4. The system attempts to find an authority configured in the system that has a name whose hash matches that of the certificate.
5. If no authority is found, no check is performed.
6. If an authority is found, the system checks the OCSP policy for the authority. If the policy permits or requires OCSP checks, see the CERT\_AUTHORITY table for more information. The system attempts to find an OCSP responder for the authority.
7. If no OCSP responder is found for the authority, one of the following happens:
  - If the authority policy is set to always check, an exception is thrown and the check fails.
  - If the authority policy is to only check when a responder is configured, no check is performed.
  - If an OCSP responder is found for the authority, an OCSP check is attempted.

### Database Tables

CERT\_AUTHORITY and OCSP\_RESPONDER are added to manage OCSP-related information.

Two new database tables have been added to manage OCSP-related information:

- CERT\_AUTHORITY
- OCSP\_RESPONDER

### CERT\_AUTHORITY

The CERT\_AUTHORITY table maintains information about certificate authorities.

Column	Type	Description
OBJECT_ID	VARCHAR (255)	This is a GUID that constitutes a unique ID for a record. This is the primary key. Cannot be null.
NAME	VARCHAR (255)	A name for a record. Null allowed.
CREATE_DATE	DATETIME	A create date for a record.
MODIFIED_DATE	DATETIME	The date a record was last modified.
MODIFIED_BY	VARCHAR(255)	Information about who modified a record.
ISSUER_NAME	BLOB	The RDN of the authority taken from its certificate.
HASH_ALG	VARCHAR(128)	The hash algorithm used to compute name and key hashes. Only SHA1 is supported.
RDN_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the DER encoded issuer RDN taken from the authority's certificate. This column is indexed.
KEY_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the encoded public key in the issuer's certificate

Column	Type	Description
CERT_OID	VARCHAR(255)	The OBJECT_ID of the authority's certificate in the CA_CERT_INFO table. Each authority must have a CA certificate in the database. Nulls not allowed.
OCSP_POLICY	VARCHAR(128)	<p>The OCSP policy for the authority. This consists of two comma separated values. The values describe when to use OCSP and what to check.</p> <p>Possible values are:</p> <p><b>OCSP_When</b></p> <ul style="list-style-type: none"> <li>• never – never use OCSP</li> <li>• resp – use OCSP only if a responder is configured when a request is made</li> <li>• always – always use OCSP when a request is made. This requires a responder to be configured and will cause certificate checking to fail if no responder is configured</li> </ul> <p><b>OCSP_What</b></p> <ul style="list-style-type: none"> <li>• none – never check any certificates</li> <li>• end-user- Check only end user certificates</li> <li>• both – check both end-user and intermediate certificates. Currently not supported</li> <li>• Null is not allowed in this column</li> </ul>
CRL_POLICY	VARCHAR(128)	Currently not used.

## OCSP\_RESPONDER

The OCSP\_RESPONDER table maintains information about OCSP responders.

Column	Type	Description
OBJECT_ID	VARCHAR (255)	This is a GUID that constitutes a unique ID for a record. This is the primary key. Cannot be null.
NAME	VARCHAR (255)	A name for a record. Null allowed.
CREATE_DATE	DATETIME	A create date for a record.
MODIFIED_DATE	DATETIME	The date a record was last modified.
MODIFIED_BY	VARCHAR(255)	Information about who modified a record.
ISSUER_NAME	BLOB	The RDN of the authority taken from its certificate.
HASH_ALG	VARCHAR(128)	The hash algorithm used to compute name and key hashes. Only SHA1 is supported.
RDN_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the DER encoded issuer RDN taken from the authority's certificate. This column is indexed.

Column	Type	Description
KEY_HASH	VARCHAR(255)	BASE64 encoded SHA1 hash of the encoded public key in the issuer's certificate
CERT_OID	VARCHAR(255)	The OBJECT_ID of the authority's certificate in the CA_CERT_INFO table. Each authority must have a CA certificate in the database. Nulls not allowed.
CACHE_TTL	VARCHAR(64)	The time in seconds to allow OCSP responses to live in the internal response cache  If the column is NULL, OCSP responses will only be cached for 1 second, which in practice means not at all.
TRANS_PROF_OID	VARCHAR(255)	OBJECT_ID of a profile in the GIS database. You have to create a profile for the OCSP responder that includes the correct URL for the responder.
COMM_BP	VARCHAR(255)	Name of a business process to use to communicate with the OCSP responder. This has to be a business process that does HTTP communication. Services in the business process have to be configured to not require or present HTTP headers when sending and receiving, respectively. The process HTTPClientSend that comes with the system can be used and is recommended
COMM_WAIT	VARCHAR(24)	The number of seconds to wait for communication with the OCSP responder to take place before inferring that something is wrong.

## OCSP Configuration

You can create unlimited authorities and responders when you configure the system to use OCSP.

### About this task

When configuring the system, you can create as many authorities and responders as you like.

To configure the system to use OCSP:

### Procedure

1. Check the certificate for the certificate authority who issues the certificates you want to check in with OCSP into Sterling B2B Integrator to verify it is a CA certificate.
2. List the CA certificates in the system and get the object ID for the certificate you just installed.
3. If the authority's OCSP response signing certificate is different than the authority's certificate issuing certificate, check the authority's OCSP response signing certificate into Sterling B2B Integrator as a Trusted certificate.

**Note:** With 5.2.4.2 and higher, you can check in the root certificate which issued the responder certificate as the CA, instead of the responder certificate as a Trusted Certificate. Since the responder certificate changes frequently, depending on the CA, it can cause OCSP to fail until the certificate is replaced with a valid one. You should always check in a root certificate from now on as a best practice, since they rarely change. However, both types will continue to be allowed.

4. If you checked in an additional OCSP signing certificate, list the CA certificates in the system and get the object ID for the certificate you just installed.
5. Go to the bin directory of the Sterling B2B Integrator installation.
6. Start the database if necessary.
7. Start the bash or sh shell.
8. Source the file tmp.sh
9. Create an authority using the utility in the class `com.sterlingcommerce.security.ocsp.SCICertAuthority`.
10. Create an OCSP responder using the utility in the class `com.sterlingcommerce.security.ocsp.SCIOCSPResponder`
11. Update the certificates for the authority or individual certificates to enable OCSP. The utility `com.sterlingcommerce.security.ocsp.SetAuthorityCertificatesOCSPInfo` will configure all trusted and system certificates for an authority. The utility `com.sterlingcommerce.security.ocsp.SetSystemCertificateOCSPInfo` will configure 1 system certificate. The utility `com.sterlingcommerce.security.ocsp.SetTrustedCertificateOCSPInfo` will configure 1 trusted certificate.

### OCSP Configuration Scripts

The following scripts have been included with the OCSP hotfix to run the OCSP configuration utilities. There is a UNIX/Linux and Windows version of each script. The scripts take the same command-line arguments as the utility programs they invoke. The scripts are located in the bin directory of the product install. The information about the command-line arguments is essentially just repeated in this section describing the scripts.

#### ManageCertAuthority.sh and ManageCertAuthority.cmd

Argument	Description
-a, -r, -d	Operation to perform: -a add -l list -d delete  The -l option takes no additional arguments. The -d option takes a single argument: the object ID of the record to delete
Name	Name of the authority. Required with -a.
Modified_by	User who modified or created the identity. Required with -a.

Hash_alg	Hash algorithm for the authority. Only the value "SHA1" is supported. Required with -a.
Certificate_id	Object ID of the CA certificate associated with the authority. Required with -a.
OCSP_policy	<p>The OCSP policy string for the authority. This is a comma-delimited string as described in the section on the CERT_AUTHORITY table. Required with -a.</p> <p>For the first element of the string, the following are permitted:</p> <ul style="list-style-type: none"> <li>• never – never use OCSP</li> <li>• resp – use OCSP only if a responder is configured when a request is made</li> <li>• always – always use OCSP when a request is made. This requires a responder to be configured and will cause certificate checking to fail if no responder is configured</li> </ul> <p>For the second element of the string, the following are permitted:</p> <p><b>OCSP What</b></p> <ul style="list-style-type: none"> <li>• none – never check any certificates</li> <li>• end-user- Check only end user certificates</li> <li>• both – check both end-user and intermediate certificates. Currently not supported.</li> </ul> <p>Examples:</p> <ul style="list-style-type: none"> <li>• never,none</li> <li>• always,end-user</li> </ul>
Crl_policy	CRL policy string for the authority. Required with -a. A value is required for this argument, but it is not currently used. "None" is acceptable.
Object_ID	An object ID to use when creating this record. Optional with -a.

### ManageOCSPResponder.sh and ManageOCSPResponder.cmd

Argument	Description
-l	<p>Gets a list of the currently configured OCSP Responders.</p> <p>This option takes no additional arguments.</p>
-d	<p>Deletes the configured OCSP Responder with the provided object ID for responders configuration data.</p> <p>This option takes object_id as an additional argument.</p>

-u2	<p>Updates existing records in the database with the correct information about the public key of the authority certificate and the subject DN of the authority certificate.</p> <p>This needs to be run against all existing records for both Cert Authority and OCSF Responders, or you need to delete and recreate the records to get the proper information into the database.</p> <p>This option takes object_id as an additional argument.</p>
-a	<p>Adds configuration data for a new OCSF Responder to be used for checking the status of certificates issued by the provided authority.</p> <p>Additional arguments are 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, and object_id.</p>
name	(Required with -a) Name of the authority.
modified_by	(Required with -a) User who modified or created the identity.
hash_alg	(Required with -a) Hash algorithm for the authority. Only the value "SHA1" is supported.
authority_cert_oid	(Required with -a) Object ID of the CA certificate associated with the authority.
response_signing_cert_oid	(Required with -a) Object ID of the certificate that the provider of the OCSF services used to sign the response providing the status for the certificates. This certificate must be added to the CA Digital Certificate store or the Trusted Digital Certificate store. This is the System Certificate ID for the certificate as it appears in the store.
resp_signing_cert_in_ca_store	(Required with -a) Flag indicating if the previous value for the response_signing_cert_oid argument is found in the CA Digital Certificate Store in Sterling B2B Integrator.
cache_ttl	(Required with -a) The time-to-live in seconds for OCSF responses in the internal cache.
trans_prof_oid	(Required with -a) The object ID of a transport configured for communicating with the OCSF responder.

comm_bp	(Required with -a) Name of a business process to use to communicate with the OCSP responder. This has to be a business process that does HTTP communication. Services in the business process have to be configured to not require or present HTTP headers when sending and receiving, respectively. The process HTTPClientSend that comes with the system can be used and is recommended.
comm_wait	(Required with -a) The number of seconds to wait for communication with the responder until inferring that an error has occurred.
send_nonce	(Required with -a) Indicates if a NONCE value will be sent to the OCSP service. The NONCE value is used to prevent replay attacks by some OCSP providers.
require_nonce	(Required with -a) Indicates if the server should require that the OCSP service provide a NONCE value in the response.
object_id	(Optional with -a) An object ID to use when creating this record.

### **SetSystemCertOCSPInfo.sh SetSystemCerOCSPInfo.cmd**

This utility will set the OCSP information in the database for a single system certificate

Argument	Description
-o, -n	How to interpret the second argument:  -o object_ID  -n name
Object_ID/Name	Object ID or name of the authority as determined by argument 1.

### **SetSystemCertOCSPInfo.sh and SetTrustedCertOCSPInfo.cmd**

This utility will set the OCSP information in the database for a single system certificate

Argument	Description
-o, -n	How to interpret the second argument:  -o object_ID  -n name
Object_ID/Name	Object ID or name of the authority as determined by argument 1.

### **Run an OCSP Script**

The following example shows how to run the OCSP configuration scripts. The scripts assume that you already checked in the CA certificates for the authority, started the database, are in the bin directory of your Sterling B2B Integrator installation, and sourced the file tmp.sh in the bin directory.



## About this task

After getting the object ID of the CA certificate from the authority, in Sterling B2B Integrator from the **Administration Menu**, select **Trading Partners > Digital Certificates-CA**. Select a certificate. The Certificate Summary dialog box appears with the certificate information, including its object ID.

Complete the following steps to run an OCSP Script. For a full list of OCSP script commands, see "OCSP Configuration Scripts" on page 79.

## Procedure

1. Run a command similar to the following to create an authority in the system:

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

2. After creating an authority, and creating a profile for communicating with an OCSP responder, run a command similar to the following to create an OCSP responder in the system:

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

3. Run a command similar to the following to list all of the authorities in the system:

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

Return output for each authority displays:

```
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 a command similar to the following to enable OCSP for all trusted and system certificates issued by the authority:

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

## OCSP Check Logic

The following steps describe the logic of OCSP checking in Sterling B2B Integrator. If the certificate status is OK, the OCSP check succeeds. Otherwise, it fails.

## Procedure

1. If an existing response whose time-to-live has not expired is found, then that response is used as the OCSP response.

2. If no existing response is found in the cache or the time-to-live has expired for a response in the cache, an OCSP request is created.
3. If the system creates an OCSP request, it launches the business process configured for the OCSP responder to send the request and get the response. Requests will include a nonce value if the responder was configured to have one sent.
4. If the business process completes successfully, the system attempts to parse its primary document as an OCSP response. The business process used to send OCSP requests and receive OCSP responses strips the HTTP headers from the response.
5. If the primary document can be parsed as an OCSP response, the system checks the status of the response.
6. If the response status indicates that the request generated a valid response, the system attempts to verify the signature on the OCSP response using the certificate configured for the OCSP responder.
7. If the signature is verified and the responder was configured to require nonce, the system attempts to get and check the nonce from the response.
8. If all other verifications passed, then the system looks for certificate status information for the certificate for which the request was constructed and sent.
9. If the status information is found, then the system updated the internal cache for an existing OCSP response for the certificate.

---

## Federal Information Processing Standards (FIPS)

### Federal Information Processing Standards (FIPS) 140-2

To conform to the security requirements of FIPS 200, applications must use cryptographic modules certified by the Cryptographic Module Validation Program and compliant with FIPS 140-1 or 140-2.

The minimum requirements for the use of validated cryptography by applications are:

- All cryptographic operations, including key generation, must be performed by validated cryptographic modules.
- Only approved security functions are permitted.
- Only approved key establishment techniques are permitted.

### FIPS 140-2 with Sterling B2B Integrator

The Certicom Government Service Edition (GSE) is a FIPS 140-2 Level 1 certified cryptographic module distributed with Sterling B2B Integrator. GSE is a low-level cryptographic toolkit in Java that implements various security functions, including unapproved security functions.

When in FIPS mode, performs the following tasks:

- Enables the GSE FIPS state machine and invokes power-on self-tests.
- Funnel cryptographic function calls from the core system to the GSE.

### Enable FIPS During Installation

During a new installation, when asked if you want to run in FIPS mode, select TRUE.

## Enable FIPS Mode Manually

You can enable FIPS mode manually after you install Sterling B2B Integrator. Before you begin, verify that you have a license for operating in FIPS mode before it is enabled. Your license is checked at startup and does not start if FIPS mode is enabled but not licensed.

### About this task

To manually enable FIPS mode:

#### Procedure

1. Navigate to `/install_dir/properties/`.
2. Locate the `security.properties` file.
3. Open the `security.properties` file in a text editor. If you make changes to the `security.properties` file, be sure to make the same changes to the `security.properties.in` file. This will prevent your customized settings from being overwritten. You should use the security property file to customize FIPS rather than editing property files directly.
4. Specify the following configurations: `FIPSMode=true`
5. Save and close the `security.properties` file.
6. Restart Sterling B2B Integrator. This is necessary for the changes to be recognized in the system.

## Disable FIPS Mode

You can manually disable FIPS mode.

### About this task

To manually disable FIPS mode:

#### Procedure

1. Navigate to `/install_dir/properties/`.
2. Locate the `security.properties` file.
3. Open the `security.properties` file in a text editor.
4. Specify the following configurations: `FIPSMode=false`
5. Save and close the `security.properties` file.
6. Restart Sterling B2B Integrator. This is necessary for the changes to be recognized in the system.

---

## Proxy Servers

### Proxy Servers

Proxy Servers enhance the security of your system.

### Configure HTTP Proxy Server

You can configure an HTTP proxy server from the **Administration** menu.

#### About this task

To configure an HTTP proxy server:

## Procedure

1. From the **Administration Menu**, select **Operations > Proxy Servers**.
2. Click **add**.
3. Enter the **Name** of the proxy server.
4. Select **HTTP** as the **Type**.
5. Enter the **Host** name. IPV6 addresses should be enclosed in square brackets.
6. Enter the **Port** number.
7. Enter the **Retry Count**.
8. Click **Next**.
9. If you want to require basic authentication for the user:
  - Select **Yes** and click **Next**.
  - If No (default), click **Next** and skip to Step 13.
10. Enter the **Auth UserID**.
11. Enter the **Auth Password**.
12. Click **Next**.
13. Review the Proxy Server Settings.
14. Click **Finish**.

## Configure SSP Proxy Server

You can configure an SSP proxy server from the **Administration** menu.

### About this task

To configure an SSP proxy server:

## Procedure

1. From the **Administration Menu**, select **Operations > Proxy Servers**.
2. Click **add**.
3. Enter the **Name** of the proxy server.
4. Select **SSP** as the **Type**.
5. Enter the **Host** name. IPV6 addresses should be enclosed in square brackets.
6. Enter the **Port** number.
7. Enter the **Retry Count**.
8. Click **Next**.
9. Is basic authentication required for the user, select Yes or No.
10. Is SSL Required, select Yes or No.
11. Click **Next**.
12. If you selected basic authorization for this user, you must enter the **Auth UserID** and the **Auth Password** and click **Next**. If you did not require this authorization, this page is not displayed.
13. If you select Yes for SSL required, you must select the **Cipher Strength**, **CA Certificates**, and **Key Certificates** and click **Next**. If you did not require SSL, this page is not displayed.
14. Click **Next**.
15. Review the Proxy Server Settings.
16. Click **Finish**.

## Configure a Proxy Server for SSL

You can use SSL with your SSP proxy server configuration by creating or importing an SSL certificate and setting the **Use SSL** field in the appropriate adapter configuration to **Must**.

### About this task

If you decide to use SSL with your SSP proxy server configuration, you must:

### Procedure

1. Create an SSL certificate or import the certificate from your certificate authority in Sterling B2B Integrator.
2. Set the **Use SSL** field in the appropriate adapter configuration to **Must**.

## Edit Proxy Servers

You can edit a proxy server configuration from the **Administration** menu.

### About this task

To edit a proxy server configuration:

### Procedure

1. From the **Administration Menu**, select **Operations > Proxy Servers**.
2. Click **edit** for the proxy server you want to edit.
3. Update the fields, as required.
4. Click **Next**.
5. Review the Proxy Server Settings.
6. Click **Finish**.

## Delete Proxy Servers

### About this task

Deleting a proxy server configuration may cause errors in some features of Sterling B2B Integrator. You may need to reconfigure specific adapters and services to work properly without a specific proxy server configuration.

To edit a proxy server configuration:

### Procedure

1. From the **Administration Menu**, select **Operations > Proxy Servers**.
2. Click **delete** for the proxy server you want to edit.
3. Review the Proxy Server Settings.
4. Click **Delete**.

---

## SSL

### About Implementing SSL in Sterling B2B Integrator

Secure Sockets Layer (SSL) provides secure communication over the Internet. It uses both symmetric and asymmetric cryptography.

The SSL security protocol provides server authentication and client authentication in Sterling B2B Integrator:

- Server authentication is performed when a client connects to the server. After the initial handshake, the server sends its digital certificate to the client. The client validates the server certificate or certificate chain.
- Client authentication is performed when a server sends a certificate request to a client during the handshake. If the client certificate or chain is verified and the certificate verify message is verified, the handshake proceeds further.
- An optional additional authentication is performed by checking the common name in the certificate against the server's fully qualified domain name from a reverse Domain Name Server (DNS) lookup where the server's fully qualified domain name can be obtained.

## Types of Trust

Two types of trust for SSL certificates are supported in Sterling B2B Integrator:

- CA Trust – Hierarchical trust based on a root certificate used to issue other certificates. This is the standard SSL certificate trust model.
- Direct Trust – Direct trust of self-signed certificates assumed to be distributed through secure out-of-band mechanisms. Direct trust and self-signed certificates are not part of the SSL standards, but are frequently used in certain trading communities.

## SSL Certificates

To communicate using SSL, configure the systems involved to support either server authentication or client/server authentication. To perform authentication against a server, you need a root Certificate Authority (CA) certificate and the set of intermediate certificates in the chain or, if the server uses a self-signed certificate, a copy of the self-signed certificate.

To support client/server authentication you need a CA or self-signed certificate and a system certificate.

You can obtain an SSL certificate from a trusted CA by providing a Certificate Signing Request (CSR) to the CA. The SSL certificate binds the public key and the SSL server or client.

If you plan to use client/server authentication, configure a system certificate. You can create system certificates in the following ways:

- Check in an existing key certificate file or PKCS12 file
- Generate a self-signed system certificate
- Use the Key Management Utility (iKeyman) to generate a CSR and get a certificate from a CA. For information about iKeyman, see “IBM Key Management Utility (iKeyman)” on page 59.

## Cipher Suites

Before you use Sterling B2B Integrator, you should review the available, predefined cipher lists and customize them according to your company's security requirements.

The IBM SDK, Java Technology Edition, Version 7 cipher suites can be found here: [http://www-01.ibm.com/support/knowledgecenter/SSYKE2\\_7.0.0/](http://www-01.ibm.com/support/knowledgecenter/SSYKE2_7.0.0/)

com.ibm.java.security.component.70.doc/security-component/jsse2Docs/ciphersuites.html. For other supported JDKs in Sterling B2B Integrator, see the JDK supplier documentation for a list of supported cipher suites.

Cipher strengths are configured in `security.properties` or in `customer_overrides.properties`. The levels of cipher suites available are:

- AllCipherSuite (UI selection is **ALL**) - includes everything listed in WEAK and STRONG.
- WeakCipherSuite (UI selection is **WEAK**) - Add supported weak cipher suites you want to use with Sterling B2B Integrator
- StrongCipherSuite (UI selection is **STRONG**) - Add supported strong cipher suites you want to use with Sterling B2B Integrator
- CipherSuiteDefault (available in V5.2.6 and higher) - by default, includes a subset of supported ciphers for IBM JDK7. Used if WeakCipherSuite and StrongCipherSuite are empty.

## Client Adapters for SSL

FTP Client adapter, HTTP Client adapter, and Sterling Connect:Direct® FTP+ Requester adapter (with Secure+ Option) support SSL.

The following client adapters support SSL:

- FTP Client adapter
- HTTP Client adapter
- Sterling Connect:Direct FTP+ Requester adapter (with Secure+ Option)

Parameters for SSL can be set in the trading partner profile or for the adapter. For the FTP Client adapter, these parameters are set in the FTP Client Begin Session service. For the HTTP Client adapter, these parameters are set in the HTTP Client Begin Session service. Parameters set in the Begin Session service override settings in a trading partner profile.

The parameters in the following table control SSL from a client perspective. See the documentation for the specific adapter or service you are configuring.

Parameter	Description
SSL	Determines SSL socket negotiation.
CACertificateId (trusted_root)	List of trusted CA public certificates. In process data, this parameter is displayed as an object ID.
CipherStrength	The level of encryption to apply to the data that flows through the socket connection.
SystemCertificateId	Select from the list of available system certificates. This certificate confirms the identity of the client to the server.

## Server Adapters for SSL

FTP Server adapter, HTTP Server adapter, Sterling Connect:Direct Server adapter (with Secure+ Option), and SMTP Send adapter support SSL.

The following server adapters support SSL:

- FTP Server adapter
- HTTP Server adapter

- Sterling Connect:Direct Server adapter (with Secure+ Option)
- SMTP Send adapter

The parameters in the following table control SSL from a server perspective. See the documentation for the specific adapter or service you are configuring.

Parameter	Description
SSL	Whether SSL is active.
Key Certificate Passphrase	Password that protects the server key certificate. This passphrase is used internally by the system to initialize the SSL libraries.
CipherStrength	Strength of the algorithms used to encrypt data.
Key Certificate (System Store)	Private key and certificate for server authentication.
CA Certificate	Certificate used, if any, to validate the certificate of a client.

## Check in a Certificate

To support client/server authentication, you need a CA or self-signed certificate and a system certificate.

### About this task

You can check in a CA certificate or a self-signed certificate in a CA certificate store by selecting **Trading Partner > Digital Certificates > CA > Check in New Certificate** from the **Administration Menu**.

## Create Self-Signed Certificates for Testing

For testing, you can use self-signed certificates. They can be generated and managed in Sterling B2B Integrator.

### About this task

To create a self-signed certificate:

### Procedure

1. Select **Trading Partners > Digital Certificates > System Certificates > Create Self-Signed Certificate**.
2. After it is created, find it, and check it out to a file.
3. Check the certificate back in to Sterling B2B Integrator as a CA certificate by selecting **Trading Partners > Digital Certificates > CA > Check In New Certificate**.

## SSL/TLS renegotiation (V5.2.6 or later)

Sterling B2B Integrator uses IBM JSSE parameters to control how restrictive SSL/TLS renegotiation is. The following parameters are available to be updated in the security.properties file.



Parameter Name	Definition	Valid Values
<b>com.ibm.jsse2. extended. renegotiation.indicator</b>	Use this property to force all negotiations to require RFC 5746, not just renegotiations. This negotiation would be practical only after all the required communication partners have implemented RFC 5746. The default setting is OPTIONAL.	Valid values are: <ul style="list-style-type: none"> <li>• BOTH - Causes the IBM JSSE2 Server or IBM JSSE2 client to connect only if the peer indicated support for RFC 5746 renegotiation. Note: Setting the property to BOTH causes interoperability problems with clients or servers that have not been updated to support RFC 5746.</li> <li>• CLIENT - Causes the IBM JSSE2 Client to connect only if the server indicated support for RFC 5746 Renegotiation. Note: Setting the property to CLIENT causes interoperability problems with servers that have not been updated to support RFC 5746.</li> <li>• OPTIONAL - This setting is the default. Using this option means that the IBM JSSE2 Server or IBM JSSE2 Client do not require the renegotiation indicator during the initial handshake.</li> <li>• SERVER - Causes the IBM JSSE2 Server to connect only if the client indicated support for RFC 5746 Renegotiation. Note: Setting the property to SERVER causes interoperability problems with clients that have not been updated to support RFC 5746.</li> </ul>

Parameter Name	Definition	Valid Values
<b>com.ibm.jsse2.renegotiate</b>	Use this property to change the renegotiation ability of IBM JSSE2. The default value is NONE.	Valid values are: <ul style="list-style-type: none"> <li>• ABBREVIATED - This setting overrides and allows unsecured abbreviated handshake during renegotiation when session continuity is proven. RFC 5746 renegotiations are allowed.</li> <li>• ALL - This setting overrides and allows unsecured full handshake, and unsecured abbreviated handshake, during renegotiation. RFC 5746 renegotiations are allowed.</li> <li>• DISABLED - This setting overrides and disables all unsecure and RFC 5746 renegotiations.</li> <li>• NONE - This setting is the default. No unsecured handshake renegotiation is allowed. Only RFC 5746 renegotiations are allowed.</li> </ul>
<b>com.ibm.jsse2.renegotiation.peer.cert.check</b>	Use this property to change the renegotiation ability of IBM JSSE2 to require the peer support that is specified in RFC 5746. This requirement is only practical after all the required communication partners have implemented RFC 5746. The default value is OFF.	Valid values are: <ul style="list-style-type: none"> <li>• OFF - This setting is the default. It stops the IBM JSSE2 Client or IBM JSSE2 Server performing an identify check against the certificate from the peer. The result is to allow the peer certificate to change during renegotiation.</li> <li>• ON - This setting causes the IBM JSSE2 Client or IBM JSSE2 Server to perform a comparison against the certificate from the peer. The reason is to ensure that the certificate does not change during renegotiation. The comparison is applicable to both secure and non-secure renegotiations.</li> </ul>

## Troubleshoot SSL

If you receive an error message, you can troubleshoot SSL.

### Corrupt or Unusable Certificate Error Messages

If you receive the following error message:

FATAL Alert:BAD\_CERTIFICATE - A corrupt or unusable certificate was received.

The information from the Perimeter log is as follows:

```
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)
```

When checking in the certificate, Sterling B2B Integrator shows a Status value of "Invalid Signature" on the naming screen. If a business process that performs an outbound HTTP POST with SSL fails on HTTP Method service with error, the following message is displayed::

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

Obtain the appropriate CA certificate for the trading partner. If the trading partner is using a self-signed certificate, the certificate itself can be used as the CA certificate.

## CA and Direct Trust

When Sterling B2B Integrator is the client, if the server has a certificate issued by a CA and that certificate has the DNS name of the server in the subject Relative Distinguished Names (RDN), you can put the root CA certificate in the CA store and trust that. If SSL still does not work, try direct trust. Put the server certificate in the CA store and trust that.

If the server is using a self-signed certificate, put that in the CA store and trust it. You are doing direct trust in this case as well.

## Use of SSL without a Certificate

You cannot use SSL-enabled adapters without having the required certificate or system certificate.

## SSL not working with a CBC-based cipher suite

If you selected the CBC-mode cipher suite, and SSL does not work, you must turn off CBC protection.

For V5.2.5 and lower perform the following steps:

1. Open the tmp.sh file for editing.
2. Find the server flag for the operating system you are configuring and add the following value:  
-DDisableSSLEmptyRecords=true
3. Save and close the file.

For V5.2.6 and higher perform the following steps:

1. In the <B2Bi Install>/bin directory, locate  
InstallNoappsWindowsService.cmd.in and

- Install `ContainerWindowsService.cmd.in` for Windows; locate `tmp.sh_platform_ifcresources_ext.in` for all other operating systems.
- Edit the file to change all instances of the following property to false:  
`jsse.enableCBCProtection=true`
- Run the `setupfiles` script.

## HTTPS Configuration for the GPM

Secure HTTP access via SSL is already supported for most web applications in Sterling B2B Integrator on the base HTTP port + 1.

This SSL enhancement:

- Enables HTTPS (HTTP w/ SSL encryption) for the Graphical Process Modeler (GPM)
- Enables disabling and redirection of web applications on the base HTTP port to another port (using HTTPS)
- Supports secure access to web applications by deploying the web applications on a secure HTTP Server Adapter instance
- Reduces security risks

If you use this feature, you will need to configure the Graphical Process Modeler (GPM) to communicate with the dashboard web application using HTTPS instead of HTTP. Access to web applications deployed via a secure HTTP Server Adapter may be slower than when accessed on the base port.

**Note:** In V5.2.6 and higher, the default security protocol is TLS 1.2 (for base HTTP port + 1.). If needed, you can change this to TLS 1.1 or TLS 1.0 by updating the `jsseProtocol` parameter in `properties_platform_ifcresources_ext`. Valid values include the following parameters:

- **TLS1-TLS1.1** - for TLS1.0 and TLS1.1
- **TLS1.1-TLS1.2** - for TLS1.1 and TLS1.2
- **TLS1** - for TLS1.0 only
- **TLS1.1** for TLS1.1 only
- **TLS1.2** - for TLS1.2 only

## New SSL Parameters

Several new parameters have been added for the enhanced SSL feature. You need to configure these parameters to facilitate SSL communication between the Graphical Process Modeler (GPM) and the server. These new parameters must be defined in their respective property files.

All custom properties for your environment should be set in the `customer_overrides.properties` file so that they are not overwritten during an upgrade or patch installation. Properties defined in the `sandbox.cfg` file must not be defined in `customer_overrides.properties`, as they will be ignored in `customer_overrides.properties`. These properties are the only ones which are not defined in `customer_overrides.properties`.

The following table describes the new SSL parameters and provides the name of the property file where the parameter can be found.

Parameter Name	Definition	Property file
WEBAPP_LIST_PORT	<p>Identifies the port the GPM client should use for communication with the server. It defaults to the base port during the installation.</p> <p>If the Dashboard and GPM web applications have been deployed to a secure HTTP Server adapter instance, this parameter should be modified to match the port of the secure HTTP Server adapter instance.</p> <p>If the base SSL port (base HTTP port +1) is being used for secure deployment of GPM and Dashboard, this parameter should be modified to match the base SSL port (SSL_PORT in sandbox.cfg).</p>	sandbox.cfg file
WEBAPP_PROTOCOL	Identifies the protocol to use for communication with the Dashboard web application (http/https).	sandbox.cfg file
SKIP_BASEPORT_DEPLOYMENT_WARS	<p>Indicates which web applications should be skipped during war deployment on the base port. The list of wars is comma-delimited, case-sensitive and without the .war suffix.</p> <p>The default is to not skip any wars. After the Dashboard and GPM web applications are successfully deployed on a secure HTTP Server Adapter, this parameter may be set to =admin,dashboard,gbm to remove access to those web applications on the base port. The complete list of web applications includes:</p> <ul style="list-style-type: none"> <li>• myaft</li> <li>• portlets</li> </ul> <p>The value ALL may be used as a wildcard to indicate that all wars deployed on the base HTTP port should be skipped. This may not be necessary if the base port is blocked to external access. The value ALL must not be used with any other value.</p>	customer_overrides.properties

Parameter Name	Definition	Property file
HTTPS_REDIRECT_WARS	<p>Indicates the wars that will be automatically redirected from the base HTTP port to either the secure HTTP Server Adapter or base SSL port.</p> <p>The value ALL may be used to redirect all skipped wars on the base HTTP port to the HTTPS_LIST_PORT (the secure HTTP Server Adapter or base SSL port).</p> <p>The value ALL must not be used with any other value.</p>	customer_overrides.properties
HTTPS_LIST_PORT	<p>Indicates the redirected destination port for requests made against the base HTTP port. Should be set to the value of the secure HTTP Server Adapter or base SSL port.</p>	customer_overrides.properties
HTTPS_CLIENT_CERTS	<p>A comma-separated list of system certificates whose public keys need to be added to the default trust store. These certificates are used for client-side verification during the SSL handshake when HTTPS calls are initiated from the application server-independent (ASI) server back to itself.</p> <p>This parameter requires server certificate keys that have a <b>SubjectAltName</b>. If you use existing keys without this parameter, this functionality will fail with very obscure messages.</p> <p><b>Note:</b> The certificate configured for HTTPS on baseport+1 (sslCert) is automatically added to the trust store and does not need to be added to this list.</p>	customer_overrides.properties

When configuring this feature, if you only define SKIP\_BASEPORT\_DEPLOYMENT\_WARS, but not HTTPS\_REDIRECT\_WARS and HTTPS\_LIST\_PORT, the web applications are inaccessible on the base port and the user is not automatically redirected to the HTTPS port. This is a valid scenario, if the user prefers not to redirect automatically for security reasons. The Web applications will still be available when accessed on the secure HTTP Server adapter or base SSL port.

### Enable Auto-Redirect to HTTPS

You can enable the automatic redirect to HTTPS.

## About this task

Support was added to allow for an automatic redirect to HTTPS to be configured for the web applications that are deployed on a secure port (Http Server Adapter or base SSL port) and skipped on the base port. This is an optional, but strongly recommended, configuration.

**Note:** All custom properties for your environment should be set in the `customer_overrides.properties` file so that they are not overwritten during an upgrade or patch installation.

To enable the automatic redirect to HTTPS:

### Procedure

1. Navigate to `/<install_dir>/install/properties`.
2. Open the `customer_overrides.properties` file and set the following parameter values as shown:

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

These parameters are configured to automatically redirect a user to the HTTPS instance of the web application.

**Note:** The `customer_overrides.properties` file is not part of the default system code. It must be created after the initial system installation and populated to match your environment.

3. Save and close the file.

### Example Implementation

Example implementation in `customer_overrides.properties` file:

```
## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
HTTPS_LIST_PORT=<http_server_adapter_port or base_ssl_port>
```

**Note:** If using a secure HTTP Server adapter instance, the configuration mandates that all wars specified as `HTTPS_REDIRECT_WARS` must be deployed on the same HTTP Server adapter instance.

### HTTPS\_CLIENT\_CERTS

If a Secure HTTP Server adapter instance is used, the SSL certificate that is used for configuring the Secure HTTP Server adapter instance must be added to the trusted certificate list.

This is needed because some of the Dashboard screens make https calls back to the ASI server. For these calls to complete the SSL handshake successfully, the certificates must be configured in the trust store on the ASI server. This is done by specifying the certificate name in the `HTTPS_CLIENT_CERTS` list.

These system certificates must have the DNS names and the IP address(es) specified as alternate names when the system cert is created. The default SSL host name verification supplied by the JDK requires that the name of the certificate presented by the SSL server match the host name used in the http url, or one of

the strings in the "SubjectAltName" attribute in the certificate. Some screens on the dashboard will not work without the "SubjectAltName" configuration.

Alternate names are configured through the "List of IP addresses Separated by Comma" and "List of DNS Names Separated by Comma" fields in the System Certificate creation wizard (**Trading Partner > Digital Certificates > System**).

## HTTPS Support for the GPM

Java Web Start (JavaWS) is used to launch the Graphical Process Modeler (GPM) by using HTTP. It supports HTTPS and the dynamic import of certificates similar to browsers.

During the SSL handshake, the server provides its certificate and JavaWS handles the trust verification. If the certificate could not be verified by JavaWS, the user is prompted to accept or reject it. SSL certificates cannot be automatically verified by JavaWS and must be verified by users.

### Import Certificates for Java Web Start

If you want to avoid an untrusted certificate prompt during Java Web Start (JavaWS) operation, you can import the certificates into the local machine store before you launch Graphical Process Modeler (GPM).

#### About this task

This can reduce user confusion in the event that the SSL certificate associated with the secure HTTP Server Adapter or base SSL port is not trusted by the user's local machine.

To import trusted root certificates into JavaWS:

#### Procedure

1. Save the trusted root certificate to a file on your local computer.
2. Open the **Java Control Panel** on your local computer (javaws.exe under jre\bin).
3. Open the **Security** tab and click **Certificates**.
4. Click **Import** to browse to a trusted root certificate and select it.
5. Click **Open** to import the new trusted root certificate. After the trusted root certificate is checked in, JavaWS uses it for trust verification during SSL handshake.

## Switch from HTTP to HTTPS Using the Base SSL Port

You can switch from HTTP to HTTPS by using the base SSL port.

#### About this task

To switch from HTTP to HTTPS using the base SSL port:

#### Procedure

1. Navigate to /install\_dir/install/properties.
2. Open the sandbox.cfg file.
3. Modify the following parameters:  
WEBAPP\_PROTOCOL=https  
WEBAPP\_LIST\_PORT=<base\_port + 1>



These parameters are used by the Graphical Process Modeler (GPM) for communication with the server.

4. (Optional, Recommended) If you want to turn off access to the dashboard and GPM Web applications on the base port, and configure auto-redirect to the HTTPS port, specify the following parameters in a `customer_overrides.properties` file:

```
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>
```

For example:

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port. Use comma-separated
## list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars. If specified, this
## should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<base_port + 1>
```

5. Save and close the file.
6. Navigate to `/install_dir/install/bin`.
7. Stop Sterling B2B Integrator.
8. Apply the configuration changes. Enter `./setupfiles.sh`.
9. Deploy the new configuration. Enter `./deployer.sh`.
10. Start Sterling B2B Integrator.
11. (Optional) If you turned off access to the Dashboard and GPM Web applications on the base port (Step 4), verify the changes you made. For example, you can verify:
  - Dashboard Web application access on `http://host:baseport/dashboard` is inaccessible or redirected to `https://host:<base_port + 1>/dashboard` automatically.
  - GPM Web application access on `http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp` is inaccessible or redirected to `https://host:<base_port + 1>/gbm/pmodeler/ProcessModeler.jnlp` automatically.

## Switch from HTTP to HTTPS Mode Using a Secure HTTP Server Adapter

You can switch from HTTP to HTTPS mode by using a Secure HTTP Server adapter.

### About this task

To switch from HTTP to HTTPS mode:

### Procedure

1. Create a new HTTP Server adapter instance with SSL enabled. You must configure the following parameters as specified:
  - **User Authentication Required** is set to **No**
  - **Use SSL** is set to **Must**

2. Deploy required WAR files to the HTTP Server adapter instance with SSL enabled.

**Note:** All WAR files must be picked up from the `/install_dir/install/noapp/deploy` directory when configuring the HTTP Server Adapter instance. Additionally, the context name of the admin web application must match the `ADMIN_CONTEXT_PATH` parameter in `/install_dir/install/properties/sandbox.cfg` file. For all the other web applications, the context name should be the name of the war file without the ".war" extension.

This is necessary so that any changes made via a patch or hotfix are automatically reflected in the HTTP Server adapter deployment.

The required WAR files include:

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

Additional WAR files may be required to support new functionality added by you to your Dashboard.

3. Open the `sandbox.cfg` file and modify the following parameters:

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

These parameters are used by the GPM for communication with the server.

4. (Optional, Recommended) If you want to turn off the deployment of the Dashboard and GPM Web applications on the base port, specify the following parameters in a `customer_overrides.properties` file:

```
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>
```

For example:

```
## Identifies the war files to be skipped during deployment on the base port.
## Use comma-separated list to specify multiple wars
noapp.SKIP_BASEPORT_DEPLOYMENT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies wars for auto-redirect to the https port.
## Use comma-separated list to specify multiple wars
noapp.HTTPS_REDIRECT_WARS=admin,dashboard,gbm,communitymanagement,myaft,portlets
## Identifies the https port for the redirected wars.
## If specified, this should match the WEBAPP_LIST_PORT in sandbox.cfg
noapp.HTTPS_LIST_PORT=<secure_http_server_adapter_port>
```

5. If you want to use a different certificate for this functionality, modify `/install_dir/install/properties/customer_overrides.properties` to add following line: `noapp.sslCert={mention_name_of_your_own_cert}`. If you do not specify a different certificate, the functionality uses `ASISslCert`.
6. (Optional) If you want to send cookies from the browser using a secure protocol like HTTPS, navigate to `/install_dir/install/properties` and specify the following parameter in a `customer_overrides.properties` file:  

```
## sending cookies as secure over https
http.useSecureCookie=true
```
7. Navigate to `/install_dir/install/bin`.
8. Stop Sterling B2B Integrator.

9. Apply the configuration changes. Enter `./setupfiles.sh`.
10. Deploy the new configuration. Enter `./deployer.sh`.
11. Start Sterling B2B Integrator.
12. 11. Verify the Dashboard Web application is accessible via the HTTP Server adapter by accessing `https://host: <secure_http_server_adapter_port>/dashboard`.
13. Verify the GPM Web application is accessible via the secure HTTP Server adapter by accessing `https://host:<secure_http_server_adapter_port>/gbm/pmodeler/ProcessModeler.jnlp`.
14. Save and close the file.
15. If you turned off the deployment of the Dashboard and GPM Web applications on the base port (Step 4), verify the following:
  - Dashboard Web application access on `http://host:baseport/dashboard` is redirected to `https://host:<secure_http_server_adapter_port>/dashboard` automatically.
  - GPM Web application access on `http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp` is redirected to `https://host:<secure_http_server_adapter_port>/gbm/pmodeler/ProcessModeler.jnlp` automatically.

## Switch from HTTPS to HTTP Mode

You can switch from HTTPS to HTTP mode.

### About this task

To switch from HTTPS to HTTP mode:

### Procedure

1. Navigate to `/install_dir/install/properties`.
2. Open the `sandbox.cfg` file.
3. Modify the following parameters:
 

```
WEBAPP_PROTOCOL=http
WEBAPP_LIST_PORT=<base_port>
```
4. Save and close the file.
5. (Optional) If the deployment of the Dashboard and GPM web applications on the base port was turned off when switching to the HTTPS mode, you must open the `customer_overrides.properties` file and comment out the following parameters so that they are not applied:

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

6. (Optional) Save and close the file.
7. Navigate to `/install_dir/install/bin`.
8. Stop Sterling B2B Integrator.
9. Apply the configuration changes. Enter `./setupfiles.sh`.
10. Deploy the new configuration. Enter `./deployer.sh`.
11. Start Sterling B2B Integrator.
12. Verify the following:
  - Dashboard Web application is accessible on `http://host:baseport/dashboard`

- GPM Web application is accessible on <http://host:baseport/gbm/pmodeler/ProcessModeler.jnlp>
13. (Optional) Undeploy the web applications from the SSL enabled HTTP server adapter instance.

---

## Hardware Security Module (HSM) V5.2.3 - 5.2.5

### Hardware Security Module (HSM)

HSM is a hardware-based security device that generates, stores, and protects cryptographic keys. You can store system certificates in a database by using Sterling B2B Integrator or on an HSM.

Sterling B2B Integrator supports the following HSM devices:

- SafeNet Eracom ProtectServer Orange External
- ProtectServer Gold PCI devices

You can use the HSM to:

- Create system certificates on the HSM
- Import system certificates from Sterling B2B Integrator
- Export system certificates from Sterling B2B Integrator
- Remove system certificates from HSM
- View system certificate details for certificates on the HSM

### Sterling B2B Integrator Features for HSM Support

An entry is stored in the CERTS\_AND\_PRI\_KEY table by Sterling B2B Integrator for each key pair and certificate.

This entry contains information about:

- Keys and certificates, including the validity period, serial number, usage restrictions, issuer and subject used by the UI to display to the user without having to actually access the key or certificate.
- Normalizations of the distinguished name used by the system in searches
- Modifications to the record.
- Certificate revocation status information.
- Keystore type.
- References to a binary keystore object stored in the DATA\_TABLE. When a software keystore is used, the referenced object may contain key material. In the case of an HSM, it contains either reference information (nCipher) or a placeholder (Eracom).

### HSM System Certificate Parameters

The following table provides the parameters for the CreateSystemCert, ImportSystemCert, and ExportSystemCert commands.

Parameter	Description
autogen	Whether to use system generated information to control access to the key and keystore. Must be set to false for keys on HSMs.
alias	The key name stored in the HSM. Only alias names containing characters a-z, A-Z, 0-9 or hyphen (-), and whose total length is no longer than the system GUID length.

Parameter	Description
Certype	The certificate type to import. Four types of certificate files are supported: pkcs12, pkcs8, pem, and keystore. Sterling B2B Integrator only supports pem keys encrypted with DES or 3DES. Use keystore to list or import the keystore.
certname	The name to assign the certificate in the Sterling B2B Integrator database.
file	Keycert or PEM file to import.
keyname	The name of the Sterling B2B Integrator system key to create.
keypass	The PIN for the token protecting the SafeNet Eracom HSM where the keystore resides.
key passphrase	The passphrase for the private key. This value is optional on the command line. If you do not provide it, you are prompted for it. The PIN for the token on the SafeNet Eracom HSM where the keystore resides.
keysize	The length, in bits, of the RSA modulus. Valid values are 768, 1024, 2048, 3072, or 4096
keystoretype	The keystore type to import. Valid value is CRYPTOKI.
keystoreprovider	The provider type. SafeNet Eracom is the only HSM supported. ERACOM or ERACOM.n if you are importing certificates to a slot other than the default slot 0.
keytype	The public key algorithm. RSA is the only supported algorithm.
ObjectID	The ID of the system certificate.
pkcs12file	The pkcs12 file to import.
password	Store passphrase for the keycert or PEM file.
pkcs12storepass	The store passphrase for the PKCS12 file.
pkcs12keypass	The key passphrase used to encrypt the private key in the PKCS12 file.
provider	The provider of the keystore type. ERACOM or ERACOM.n if you are importing certificates to a slot other than the default slot 0.
rfc1779rdnsequence	The distinguished name string field contains any of the fields identified in the Valid Values column. Only the CN field is required. Separate each field with a comma. Valid information: <ul style="list-style-type: none"> <li>• CN = CommonName</li> <li>• O = Organization</li> <li>• OU = Organization Unit</li> <li>• L = Location</li> <li>• ST = State</li> <li>• C = Country (provide a two-letter ISO3166-1 alpha-2 code)</li> </ul>
storetype	The keystore type. CRYPTOKI is the only keystore type supported.
signingbit	Sets the sign key usage bit for the self-signed certificate. Value values are true or false.
serial	The certificate serial number.
system passphrase	The Sterling B2B Integrator system passphrase. This value is optional on the command line.

Parameter	Description
store passphrase	The passphrase for accessing the keystore. The PIN for the token on the SafeNet Eracom HSM where the keystore resides. This value is optional on the command line.
systempass	The Sterling B2B Integrator system passphrase.
storepass	The PIN for the token protecting the SafeNet Eracom HSM where the keystore resides.
totrusttable	Determines if the certificate is added to the trusted certificate table. Value values are true or false.
validityindays	Length of time in days that the certificate is valid.

## SafeNet Eracom HSM

Before you can use an HSM with Sterling B2B Integrator, you must configure Sterling B2B Integrator to use and recognize the SafeNet Eracom HSM.

To install and set up the SafeNet Eracom HSM, follow the instructions provided by the vendor; ensure that you install Java Runtime. Use the provider for the slot where Sterling B2B Integrator keys will be stored when you set up and use the utilities. After you create a PIN for the SafeNet Eracom slot, do not change the PIN. Sterling B2B Integrator cannot access a key on the HSM if you change the PIN.

The SafeNet Eracom architecture divides the HSM into multiple slots. Install and configure cards or HSMs according to the vendor's instructions. Each slot has an associated security provider and can be protected by a separate Personal Identification Number (PIN). You can create a separate slot on the HSM for Sterling B2B Integrator and protect the slot with a unique PIN. The provider for the default slot 0 is ERACOM. Providers for additional slots are named ERACOM.*n*, where *n* is the number of the slot. Ensure that java runtime components are available to interact with the device.

### Configure Sterling B2B Integrator to use SafeNet Eracom HSM

You can configure Sterling B2B Integrator to use the SafeNet Eracom HSM.

#### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Add the following lines to the `tmp.sh` and `tmp.sh.in` files:

```
LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/opt/Eracom/lib
export LD_LIBRARY_PATH
```
3. If you are configuring a network-based server, add the following lines to the `tmp.sh` and `tmp.sh.in` files, where `network_device_IP_OR_hostname` is the IP address or fully qualified domain name of the SafeNet Eracom network-based server:

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
export ET_HSM_NETCLIENT_SERVERLIST
```
4. Copy the `jprov.jar` from the `/opt/Eracom/lib` directory to the `/install_dir/install/jdk/jre/lib/ext` directory.
5. Add a definition for each security provider to the `/install_dir/install/bin/jdk/jre/lib/security/java.security` file. To add a definition, identify the number assigned to the Certicom provider and assign `n+1` to the SafeNet Eracom

provider. For all other providers identified after the SafeNet Eracom provider, increase the security.provider number by 1.

```
security.provider.n=com.certicom.ecc.jcae.Certicom
```

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

If you are using a slot other than zero on the SafeNet Eracom HSM, specify the slot as follows, where *x* is the number of the slot:

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

6. Define the TLSProviderPolicy in the `/install_dir/install/properties/security.properties` file.

- If the provider is defined in slot 0, ensure that the only uncommented line for the TLSProviderPolicy parameter is the following:

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

- If the provider is defined in a slot other than 0, modify the TLSProviderPolicy parameter as follows, where *x* is the slot you are configuring:

```
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. Define the KeyStoreProviderKey command in the `/install_dir/install/properties/security.properties` file:

- If the provider is defined in slot 0, ensure that KeyStoreProviderMap is defined as:

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

- If the provider is defined in any slot other than 0, modify the KeyStoreProviderMap parameter as follows, where *x* is the slot number:

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

## Supported nCipher and SafeNet/Eracom Network and PCI Devices

Sterling B2B Integrator currently supports Safenet/Eracom ProtectServer Orange PCI card and Orange External network device, in addition to support for nCipher.

The following are supported:

Manufacturer	Supported Device Types
nCipher	<ul style="list-style-type: none"> <li>• nShield series of PCI cards</li> <li>• NetHSM network devices</li> </ul>
Safenet/Eracom	<ul style="list-style-type: none"> <li>• ProtectServer Gold PCI card</li> <li>• ProtectServer Orange PCI card</li> <li>• ProtectServer Orange External network device</li> </ul>

## Use a Hardware Security Module

### Create System Certificates to Store on the HSM

You can create a self-signed system certificate to store on the HSM.

#### Before you begin

Before you begin:

- Stop Sterling B2B Integrator.
- Ensure that the Sterling B2B Integrator database is running.

#### About this task

To create a self-signed system certificate to store on the HSM:

#### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./CreateSystemCert.sh storetype provider autogen totrusttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. If you did not provide the system passphrase, store passphrase, and key passphrase on the command line, you are prompted to enter them.

### List System Certificates Stored in the HSM

You can list information about system certificates stored in the HSM.

#### About this task

To list information about system certificates stored in the HSM:

#### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

#### Example

The following is an example of the command output:

```
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
```

### Import a HSM System Certificate to the Sterling B2B Integrator Database

Use this procedure when a key and certificate exist on the HSM and were added to the HSM independent of Sterling B2B Integrator. You must import the information for a system certificate that is stored on an HSM to the database before it can be used by Sterling B2B Integrator.



## About this task

Depending upon the method used to add the private key and certificate to the HSM, the list function may display duplicate entries for a single key and certificate pair.

You must obtain the system certificate alias before you can import information about a system certificate to the database.

To import the system certificate:

### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

## Remove System Certificates Stored in the HSM

You can permanently delete the system certificate from the HSM. The private key data that it contains cannot be recovered.

## About this task

To remove a system certificate stored in the HSM:

### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./RemoveSystemCert.sh -r xxxx`  
Where `xxxx` is the object ID of the certificate you want to remove.

## Export System Certificates

You can export system certificates from the Sterling B2B Integrator so that they can be imported into the HSM.

## About this task

System certificates on an HSM cannot be exported using `ExportSystemCert.sh`.

### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Enter your passphrase.

## Example: HSM System Certificate

You can import a system certificate to the HSM in `keycert`, `pkcs12`, or `pem` format. Importing a system certificate adds the key and certificate to the HSM and creates a corresponding entry in the Sterling B2B Integrator database.

If you import a `pem` type certificate and key, make sure that the private key is created in `DES`- or `triple-DES` encrypted format.

The following is a sample `pem` private key created in `triple-DES` format:

```

-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, CE0243B4833BD321
RtN+AFGTmx6ER0cbo8fMXnMaRM/JcK1c3jbKYB5t6H6H5uvUrAmv+Si62QEtqg9V
x5r+GhiLcA9sd11KpnIXYg63Y+egn8DsdGUCqnC+HDU1RVHX0NWKJ3FwXukr9iN
WP4MBR+NXMSETaBA000B4oSRCWvxe1c2U2GItvUqJs0jLSILbahAgZk/j6LUDMy4
2FWoRtWZyGVz/gc+pN+b0wFHpbRZxd1YqZGRNKeZKTPXws1qxp5NDraB11cmJ3vL
0RTnkWZnnyJ1Brc/Wyn1VfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAY5Y/w
7Yowicmwbo4q7RLVLm1ZmvPF40XL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQKQ9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvattg/H72Ut39Yz185Ec+E8sV0BtilppVsYSt1g6
10805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfHwbuhnyuQmco3SsCtYXnZ81cDHX+408sGqHA1zMwuqErrorUvwxD6ZNN1c
DTmKI826oows4Gtw48aEwjV41k8FXQsWQjDWHJfNnVgyszPjvPvM8zL1Ewx0
mJFeNx8b0U3zgLS5aK/HHRn1/gz0BHwtr8bdFFBkpLoVgnbw+mRVxmJ0vPe7Z0+
sJXLEWC8Bm4k1V8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHAbk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAEI11IQ==
-----END RSA PRIVATE KEY-----

```

## Manage System Certificate Utilities

### HSM Key Pairs and Certificate Signing Requests

The GenCSR utility generates a key pair on an HSM and creates a PKCS10 certificate signing request (CSR) with the public key from that key pair. You can then submit the CSR to a Certificate Authority (CA).

When you receive a CA-issued certificate, use GenCSR to update the certificate. The system certificate is not available in Sterling B2B Integrator until it is updated with a CA-issued certificate.

You can also use this utility to view a list of CSRs, write information about a CSR to a file, delete a CSR, or write information about a CA-issued certificate stored on the HSM to a file. Information about CSRs is maintained in the Sterling B2B Integrator database, while the actual keys are stored on the HSM.

To use the utility, first determine what action you want to perform. Then, use the GenCSR utility and identify the action in the command line. For each action, supply the arguments required for the action in the properties file. A sample properties file called `csr.properties.sample` is provided in the `/install_dir/install/properties` directory.

The GenCSR utility can be found in the `/install_dir/install/bin` directory.

The command syntax is: `GenCSR.sh -a ACTION -p PROPERTIES`

### GenCSR Parameters

The following table provides the parameters used when running the GenCSR script.

Parameter	Description	Valid Values
-a ACTION	The action to perform.	Valid actions are: <ul style="list-style-type: none"> <li>• CREATE</li> <li>• UPDATE</li> <li>• LIST</li> <li>• DELETE</li> <li>• GETPKCS10</li> <li>• GETCACERT</li> </ul>

Parameter	Description	Valid Values
-p PROPERTIES	The properties file that contains additional parameters needed for the actions. You need to include the path to the property file.	Name of a properties file.  For example: csr_create.properties

## Update the HSM Keystore with CA-Issued Certificates

Use the GenCSR utility with the update argument to add CA-issued certificate information to the HSM keystore.

### Procedure

1. Ensure the csr\_update.properties file is configured correctly.

The following table describes the parameters required in the csr\_update.properties file for the update argument.

Parameter	Description	Valid Values
provider	Name of keystore provider.	ERACOM or ERACOM.n
keystoretype	Name of the keystore used.	CRYPTOKI
certificate.request.Name	Name of the CSR to update.	Name assigned to a CSR
add.trusted	Identifies if the certificate information is added to the trusted certificate table.	True   false
ca.cert.file	Path and file name of the file in which to write information about the CA-issued certificate.	Valid path and file name of a CA-issued certificate file

2. Update the HSM Keystore.

The command syntax is: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

## List Certificate Signing Requests

Use the GenCSR utility with the list argument to display CSRs in the HSM database. No property file configuration is required for the list argument.

### About this task

The command syntax is: `./GenCSR.sh -a list`

## Delete a Certificate Signing Request

Use the GenCSR utility with the delete argument to delete a CSR. This utility deletes the CSR only. It does not delete system certificates that are updated with a CA-issued certificate.

### Procedure

1. Ensure that the cacert.properties file is configured properly. You must configure the property file before using the delete argument. The following table describes the parameters required in the cacert.properties file for the delete argument.

Parameter	Description	Valid Values
certificate.request.Name	Name of the CSR to delete.	Name of a CSR

Parameter	Description	Valid Values
keystoretype	Name of the keystore used.	CRYPTOKI
provider	Name of keystore provider.	ERACOM[.N]

2. Delete the CSR. The command syntax is `./GenCSR.sh -a delete -p ../properties/cacert.properties`

### Write CSR Information to a pkcs10 format

Use the GenCSR utility with the `getpkcs10` argument to write a CSR in pkcs10 format to the specified file.

#### Procedure

1. Ensure the `csr_getpkcs10.properties` file is configured correctly.  
The following table describes the parameters required in the `csr_getpkcs10.properties` file for the `getpkcs10` argument. You must configure the property file before using the `getpkcs10` argument.

Parameter	Description	Valid Values
certificate.request.Name	Name of the CSR.	Name assigned to a CSR
keystoretype	Name of the keystore used.	CRYPTOKI
csr.file	Fully qualified path to the file in which to write information about the CSR.	Path and file name of a file to write the CSR information

2. Write the CSR to a file.  
The command syntax is `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

### Move System Certificates to the HSM

You can move self-signed certificates or CA-issued certificates from the database to the HSM.

#### About this task

It is more secure to regenerate keys and certificates using `CreateSystemCert.sh` or `GenCSR.sh`.

To move self-signed certificates or CA-issued certificates from the database to the HSM:

#### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Stop Sterling B2B Integrator.
3. Start the database.
4. Export the system certificate to a PKCS12 file:  
`./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
5. Find the object ID of the system certificate to remove. Enter:  
`./RemoveSystemCert.sh -l`
6. Remove the system certificate from the database. Enter:

RemoveSystemCert.sh -r *xxxx*Where *xxxx* is the object ID of the certificate you wish to remove.

7. To import the system certificate that you exported to the HSM and create a corresponding database entry:

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

**Note:** If you move the OpsDrv, OpsKey, and UIKey to the HSM, use the exact name. Otherwise, Sterling B2B Integrator will not function properly. For all other system certificates, the name is not critical. When moving system certificates other than the OpsDrv, OpsKey, and UIKey, the object ID that is used by services and adapters changes. Reconfigure any services that use the system certificates that were moved.

## Write CA-Issued Certificate to a File

Use the GenCSR utility with the getcacert argument to write the certificate issued by the CA to a file.

### Procedure

1. Ensure the getcacert.properties file is configured correctly.

The following table describes the parameters required in the getcacert.properties file for the getcacert Action. You must configure the getcacert.properties file before using the getcacert argument.

Parameter	Description	Valid Values
certificate.request.Name	Name of the CSR.	Certificate name
keystoretype	Name of the keystore used.	CRYPTOKI
ca.cert.file	Fully qualified path to the file in which to write information about the CA certificate.	Name and path of a CA certificate file

2. Write the certificate to a file.

The command syntax is `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

## Generate Internal System Certificates (OpsDrv, OpsKey, UIKey) on the HSM

Three system certificates are installed with Sterling B2B Integrator to secure internal operations. Little security benefit is provided by moving them to the HSM. Your security policy can require that all certificates that contain private keys be stored on the HSM.

### About this task

When generating the Sterling B2B Integrator internal system certificates called OpsDrv, OpsKey, and UIKey on the HSM, use the exact names. Otherwise, Sterling B2B Integrator will not function properly.

To generate internal system certificates:

### Procedure

1. Navigate to `/install_dir/install/bin`.

2. Enter `./RemoveSystemCert.sh -l` to view certificates in the database. Note the object ID for each system certificate.
3. To delete the system certificates from the database by running the following command for each certificate: `./RemoveSystemCert.sh -r xxxx` where `xxxx` is the object ID of the certificate you want to remove.
4. Generate the system certificate on the HSM for each certificate, enter:  
`./CreateSystemCert.sh storetype provider autogen totrussttable signingbit  
keytype keysize keyname rfc1779rdnsequence serial validityindays [system  
passphrase] [store passphrase] [key passphrase]`

## Use nCipher and SafeNetEracom

### Key Store Provider Map

Sterling B2B Integrator has the keystore type that is unique across cryptographic service providers; it is able to define a mapping between keystore types and providers required for implementing the keystore object itself, signature algorithms, and key transport algorithms.

The key and key information abstraction object contains this information with a reference to a `com.sterlingcommerce.security.PrivateKeyInfo`.

This allows Sterling B2B Integrator to use a combination of keys on HSMs and in software stores in the database at the same time without additional configuration beyond the initial loading of the key or key information into the database. To Sterling B2B Integrator, the keys all look the same, regardless of where they are stored.

Mapping is implemented as a property called `KeyStoreProviderMap` in `security.properties`. It consists of a set of entries delimited by semi colons (;). Each entry has six elements delimited by commas and follow this format:

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

The elements are described in the following table:

Element	Description	Additional Information
KeyStoreType	The string type of the keystore	
KeyStoreProvider	The name of the cryptographic service provider that implements the keystore	
DoesAliasMatter	Whether the alias of keys must be unique for this keystore type	This can be either true or false. Keys have to have unique aliases in the case where there is only one keystore per device.
SignatureProvider	The name of the cryptographic service provider to use to create signatures using keys from the keystore	

Element	Description	Additional Information
EncryptionProvider	The name of the cryptographic service provider to use when decrypting information using keys in the keystore	This is mostly for RSA key transport operations
KeyOnHSM	Whether the keystore is on an HSM	

The string null is an acceptable value and will be treated as though no provider has been specified. An entry must have at least two values. If an entry contains less than six values, the values will be assigned from left to right to the keystore provider, whether the alias matters when storing the key, signature provider, encryption provider, and whether the key is on an HSM for the KeyStore type. The others will be treated as nulls and no specific provider will be requested for operations with keys of that type.

The default KeyStoreProviderMap is currently:

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

## Manage HSM Keys and Key Information

Sterling B2B Integrator has several java scripts for managing keys on HSMs.

The java programs are listed below.

Program	Purpose
com.sterlingcommerce.db.RemoveSystemCert	Both list and delete Sterling B2B Integrator system certificates. During a delete, the program makes a best effort to clear the key from the keystore and overwrite the keystore object in the database.
com.sterlingcommerce.db.CreateCertEx	Generate a key pair on an HSM and a self-signed certificate containing the public key of the key pair.
com.sterlingcommerce.security.util.CertificateSigningRequest	Generate a key pair on an HSM and create and manage an associated PKCS10 certificate signing request. The PKCS10 can be provided to an authority to get a certificate signed by the authority. This program can be used to then load that certificate into the keystore and associate it with the right key pair.
com.sterlingcommerce.db.ImportSystemCert	Import a private key and certificate in a supported format (PKCS12 or PEM) into a keystore on an HSM. Import information about a private key and certificate on an HSM into the Sterling B2B Integrator database.

## JDK Changes for nCipher HSM Support

In order for Sterling B2B Integrator to use nCipher HSMs, you must install the nCipher java cryptographic service providers. To install, copy the following jar files in the jre/lib/ext subdirectory of your JDK. Modify java.security to load the nCipher providers.

The following files are placed in /opt/nfast/java/classes by the nCipher installation program:

- rsaprivenc.jar

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

You should add the nCipher providers after the IBM JCE provider and before the Certicom provider. For example:

```
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
```

On Solaris systems with the SUN JDK, you should place the nCipher providers after the Sun JCA and JCE providers and before the Certicom provider. For example:

```
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
```

Set up a TLSProvider policy using the sample in security.properties. For example:

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

## JDK Changes for Eracom HSM Support

In order for Sterling B2B Integrator to use Eracom HSMs, you must install the Eracom java cryptographic service provider. To install, place the appropriate.jar files in the jre/lib/ext subdirectory of your JDK and then modify java.security to load the nCipher providers.

These files are placed in /opt/nfast/java/classes by the nCipher install program:

- jprov.jar
- jprov.jar

You should add the Eracom provider after the Certicom provider. For example:

```
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
```

**Note:** Eracom has a provider that can be specified for each slot on the card. For the provider for slot 8, use:

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

### **Linux Environment Changes for nCipher HSM Support**

nCipher recommends that you create a special user account for running the nCipher hardserver.

The account from which you run Sterling B2B Integrator needs to have equivalent permissions, or you need to run Sterling B2B Integrator from the nCipher special account or as root. If you do either of these and are using MySQL, you must change the permissions for MySQL, or start MySQL from your normal account before invoking run.sh.

### **Linux Environment Changes for Eracom HSM Support**

To use the Eracom device, you must supply additional information in environment variables to the session that accesses the device.

Recommended changes to PATH, LD\_LIBRARY\_PATH, and MANPATH are as follows:

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

In addition, if you are using a network device rather than a local PCI card, you must supply ET\_HSM\_NETCLIENT\_SERVERLIST, as follows:

```
ET_HSM_NETCLIENT_SERVERLIST=network_device_IP_OR_hostname
```

You should export these variables in tmp.sh.

---

## **Hardware Security Module (HSM) V5.2.6 or Later**

### **Hardware Security Module (HSM)**

HSM is a hardware-based security device that generates, stores, and protects cryptographic keys. You can store system certificates in a database by using Sterling B2B Integrator or on an HSM.

Sterling B2B Integrator supports the following HSM devices:

- SafeNet Luna SA
- nCipher nShield Connect

You can use the HSM to:

- Create system certificates on the HSM
- Import system certificates from Sterling B2B Integrator
- Export system certificates from Sterling B2B Integrator
- Remove system certificates from HSM
- View system certificate details for certificates on the HSM

## Sterling B2B Integrator Features for HSM Support

An entry is stored in the CERTS\_AND\_PRI\_KEY table by Sterling B2B Integrator for each key pair and certificate.

This entry contains information about:

- Keys and certificates, including the validity period, serial number, usage restrictions, issuer and subject used by the UI to display to the user without having to actually access the key or certificate.
- Normalizations of the distinguished name used by the system in searches
- Modifications to the record.
- Certificate revocation status information.
- Keystore type.
- References to a binary keystore object stored in the DATA\_TABLE. When a software keystore is used, the referenced object may contain key material. In the case of an HSM, it contains either reference information (nCipher) or a placeholder (Luna).

## HSM System Certificate Parameters

The following table provides the parameters for the CreateSystemCert, ImportSystemCert, and ExportSystemCert commands.

Parameter	Description
autogen	Whether to use system generated information to control access to the key and keystore. Must be set to false for keys on HSMs.
alias	The key name stored in the HSM. Only alias names containing characters a-z, A-Z, 0-9 or hyphen (-), and whose total length is no longer than the system GUID length.
Certtype	The certificate type to import. Four types of certificate files are supported: pkcs12, pkcs8, pem, and keystore. Sterling B2B Integrator only supports pem keys encrypted with DES or 3DES. Use keystore to list or import the keystore.
certname	The name to assign the certificate in the Sterling B2B Integrator database.
file	Keycert or PEM file to import.
keyname	The name of the Sterling B2B Integrator system key to create.
keypass	The PIN for the token protecting the SafeNet or nCipher HSM where the keystore resides.
key passphrase	The passphrase for the private key. This value is optional on the command line. If you do not provide it, you are prompted for it.
keysize	The length, in bits, of the RSA modulus. Valid values are 1024, 2048, 3072, or 4096
keystoretype	The keystore type to import. Valid values are nCipher.sworld, Luna and PKCS11IMPLKS (5.2.6.2 onwards).
keystoreprovider	The provider type. Valid values are nCipherKM, LunaProvider and IBMPKCS11Impl (5.2.6.2 onwards).
keytype	The public key algorithm. RSA is the only supported algorithm.
ObjectID	The ID of the system certificate.
pkcs12file	The pkcs12 file to import.

Parameter	Description
password	Store passphrase for the keycert or PEM file.
pkcs12storepass	The store passphrase for the PKCS12 file.
pkcs12keypass	The key passphrase used to encrypt the private key in the PKCS12 file.
provider	The provider of the keystore type. Valid values are nCipherKM, LunaProvider and IBMPKCS11Impl (5.2.6.2 onwards).
rfc1779rdnsequence	The distinguished name string field contains any of the fields identified in the Valid Values column. Only the CN field is required. Separate each field with a comma. Valid information: <ul style="list-style-type: none"> <li>• CN = CommonName</li> <li>• O = Organization</li> <li>• OU = Organization Unit</li> <li>• L = Location</li> <li>• ST = State</li> <li>• C = Country (provide a two-letter ISO3166-1 alpha-2 code)</li> </ul>
storetype	The keystore type. Valid values are nCipher.sworld, Luna and PKCS11IMPLKS (5.2.6.2 onwards).
signingbit	Sets the sign key usage bit for the self-signed certificate. Value values are true or false.
serial	The certificate serial number.
system passphrase	The Sterling B2B Integrator system passphrase. This value is optional on the command line.
store passphrase	The passphrase for accessing the keystore. This value is optional on the command line. If you do not provide it, you are prompted for it.
systempass	The Sterling B2B Integrator system passphrase.
storepass	The PIN for the token protecting the SafeNet or nCipher HSM where the keystore resides.
totrusttable	Determines if the certificate is added to the trusted certificate table. Value values are true or false.
validityindays	Length of time in days that the certificate is valid.

## Use a Hardware Security Module

### Create System Certificates to Store on the HSM

You can create a self-signed system certificate to store on the HSM.

#### Before you begin

Before you begin:

- Stop Sterling B2B Integrator.
- Ensure that the Sterling B2B Integrator database is running.

#### About this task

To create a self-signed system certificate to store on the HSM:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./CreateSystemCert.sh storetype provider autogen totrustrtable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`
3. If you did not provide the system passphrase, store passphrase, and key passphrase on the command line, you are prompted to enter them.

## List System Certificates Stored in the HSM

You can list information about system certificates stored in the HSM.

### About this task

To list information about system certificates stored in the HSM:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./ImportSystemCert.sh -keystore keystoretype keystoreprovider storepass keypass`

### Example

The following is an example of the command output:

```
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
```

**Note:** From V5.2.6.2 onwards, the valid value for Keystoretype is PKCS11IMPLKS.

## Import a HSM System Certificate to the Sterling B2B Integrator Database

Use this procedure when a key and certificate exist on the HSM and were added to the HSM independent of Sterling B2B Integrator. You must import the information for a system certificate that is stored on an HSM to the database before it can be used by Sterling B2B Integrator.

### About this task

Depending upon the method used to add the private key and certificate to the HSM, the list function may display duplicate entries for a single key and certificate pair.

You must obtain the system certificate alias before you can import information about a system certificate to the database.

To import the system certificate:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./ImportSystemCert.sh -keystore systempass certname alias keystoretype keystoreprovider storepass keypass`

## Remove System Certificates Stored in the HSM

### About this task

This procedure permanently deletes the system certificate from the HSM. The private key data it contains cannot be recovered.

To remove a system certificate stored in the HSM:

### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./RemoveSystemCert.sh -r xxxx`  
Where `xxxx` is the object ID of the certificate you want to remove.

## Export System Certificates

You can export system certificates from the Sterling B2B Integrator so that they can be imported into the HSM.

### About this task

System certificates on an HSM cannot be exported using `ExportSystemCert.sh`.

### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter: `./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
3. Enter your passphrase.

## Example: HSM System Certificate

You can import a system certificate to the HSM in `keycert`, `pkcs12`, or `pem` format. Importing a system certificate adds the key and certificate to the HSM and creates a corresponding entry in the Sterling B2B Integrator database.

If you import a `pem` type certificate and key, make sure that the private key is created in `DES-` or `triple-DES` encrypted format.

The following is a sample `pem` private key created in `triple-DES` format:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CE0243B4833BD321
RtN+AFGTmx6ER0cbo8fMXnMaRM/JcKIc3jBKYB5t6H6H5uvUrAmv+Si62QEttqg9V
x5r+GhiLcA9sd1lKpnIXYg63Y+egn8DsxdGUCqnC+HDU1RVHX0NWKJ3FwXukr9iN
WP4MBR+NXMSETaBA000B4oSRCWvxe1c2U2GItvUqJs0jLSILbahAgZk/j6LUDMy4
2FwoRtWZyGVz/gc+pN+b0wFHpbrZxd1YqZGRNKeZKTpXWslqxp5NDraB1lcmJ3vL
0RTnkwZnnyJ1Brc/Wyn1VfRK1gEEg8MPa3B9veat70ET/mLERuA4Ke8r0WAY5Y/w
7Yowicmwo4q7RLVLM1ZmvPF40XL8xIvaIUMOCW8/MNpanxZ4BB1CfTwQK9koJ7
9MT8K8ofu6V9TSK4Rw1cCpTKvatg/H72Ut39Yz185Ec+E8sV0Bti1pqVsYSt1g6
10805MqPym6gPo2NLpvk1iPLUZ1vIfthz+qb5cyXj1ng9aZSeRF/lytPLxSSy3LN
J9SZrnfhwbuhnyuQmco3SsCtYXnZ81cDHX+408sGqHA1zMwuqErrorUvwxD6ZnN1c
DTmKI826oows4Gtw48aEwjV41k8FXQsWQjDwJHjFNNvGiyszPjJvPvM8zL1Ewx0
mJFeNxBb0U3zgLs5aK/HHRn1/gz0BHwtr8bdFFBkplOVGnbW+mRVxmJ0vvPe7Zo+
sJXLEWC8Bm4k1V8H6ynx6aQJ8a62HqbjPvShq1VH2I+1iwbyE3DzxY5sHrzZA2rb
dHAbk3f0nBUvMegKI9Ye4ktLJf8yIQfsSBSJTEYXHqyx5ptoAE11IQ==
-----END RSA PRIVATE KEY-----
```

## Manage System Certificate Utilities

### HSM Key Pairs and Certificate Signing Requests

The GenCSR utility generates a key pair on an HSM and creates a PKCS10 certificate signing request (CSR) with the public key from that key pair. You can then submit the CSR to a Certificate Authority (CA).

When you receive a CA-issued certificate, use GenCSR to update the certificate. The system certificate is not available in Sterling B2B Integrator until it is updated with a CA-issued certificate.

You can also use this utility to view a list of CSRs, write information about a CSR to a file, delete a CSR, or write information about a CA-issued certificate stored on the HSM to a file. Information about CSRs is maintained in the Sterling B2B Integrator database, while the actual keys are stored on the HSM.

To use the utility, first determine what action you want to perform. Then, use the GenCSR utility and identify the action in the command line. For each action, supply the arguments required for the action in the properties file. A sample properties file called `csr.properties.sample` is provided in the `/install_dir/install/properties` directory.

The GenCSR utility can be found in the `/install_dir/install/bin` directory.

The command syntax is: `GenCSR.sh -a ACTION -p PROPERTIES`

### GenCSR Parameters

The following table provides the parameters used when running the GenCSR script.

Parameter	Description	Valid Values
-a ACTION	The action to perform.	Valid actions are: <ul style="list-style-type: none"><li>• CREATE</li><li>• UPDATE</li><li>• LIST</li><li>• DELETE</li><li>• GETPKCS10</li><li>• GETCACERT</li></ul>
-p PROPERTIES	The properties file that contains additional parameters needed for the actions. You need to include the path to the property file.	Name of a properties file.  For example: <code>csr_create.properties</code>

### Update the HSM Keystore with CA-Issued Certificates

#### About this task

Use the GenCSR utility with the update argument to add CA-issued certificate information to the HSM keystore.

#### Procedure

1. Ensure the `csr_update.properties` file is configured correctly.

The following table describes the parameters required in the `csr_update.properties` file for the update argument.

Parameter	Description	Valid Values
provider	Name of keystore provider.	IBMPKCS11IMPL (from V5.2.6.2 onwards) or nCipherKM or LunaProvider
keystoretype	Name of the keystore used.	PKCS11IMPLKS(from V5.2.6.2 onwards) or nCipher.sworld or Luna <b>Note:</b> The 'keystoretype' value should be synchronous with the 'provider' value.
certificate.request.Name	Name of the CSR to update.	Name assigned to a CSR
add.trusted	Identifies if the certificate information is added to the trusted certificate table.	True   false
ca.cert.file	Path and file name of the file in which to write information about the CA-issued certificate.	Valid path and file name of a CA-issued certificate file

## 2. Update the HSM Keystore.

The command syntax is: `./GenCSR.sh -a update -p ../properties/csr_update.properties`

## List Certificate Signing Requests

Use the GenCSR utility with the list argument to display CSRs in the HSM database. No property file configuration is required for the list argument.

### About this task

The command syntax is: `./GenCSR.sh -a list`

## Delete a Certificate Signing Request

Use the GenCSR utility with the delete argument to delete a CSR. This utility deletes the CSR only. It does not delete system certificates that are updated with a CA-issued certificate.

### Procedure

1. Ensure that the cacert.properties file is configured properly. You must configure the property file before using the delete argument. The following table describes the parameters required in the cacert.properties file for the delete argument.

Parameter	Description	Valid Values
certificate.request.Name	Name of the CSR to delete.	Name of a CSR
keystoretype	Name of the keystore used.	PKCS11IMPLKS(from V5.2.6.2 onwards) or nCipher.sworld or Luna
provider	Name of keystore provider.	IBMPKCS11IMPL (from V5.2.6.2 onwards) or nCipherKM or LunaProvider <b>Note:</b> The 'keystoretype' value should be synchronous with the 'provider' value.

2. Delete the CSR. The command syntax is `./GenCSR.sh -a delete -p ../properties/cacert.properties`

## Write CSR Information to a pkcs10 format

### About this task

Use the GenCSR utility with the `getpkcs10` argument to write a CSR in pkcs10 format to the specified file.

### Procedure

1. Ensure the `csr_getpkcs10.properties` file is configured correctly.  
The following table describes the parameters required in the `csr_getpkcs10.properties` file for the `getpkcs10` argument. You must configure the property file before using the `getpkcs10` argument.

Parameter	Description	Valid Values
<code>certificate.request.Name</code>	Name of the CSR.	Name assigned to a CSR
<code>keystoretype</code>	Name of the keystore used.	PKCS11IMPLKS (from V5.2.6.2 onwards) or nCipher.sworld or Luna
<code>csr.file</code>	Fully qualified path to the file in which to write information about the CSR.	Path and file name of a file to write the CSR information

2. Write the CSR to a file.  
The command syntax is `./GenCSR.sh -a getpkcs10 -p ../properties/csr_getpkcs10.properties`

## Move System Certificates to the HSM

You can move self-signed certificates or CA-issued certificates from the database to the HSM.

### About this task

It is more secure to regenerate keys and certificates using `CreateSystemCert.sh` or `GenCSR.sh`.

To move self-signed certificates or CA-issued certificates from the database to the HSM:

### Procedure

1. Navigate to `/install_dir/install/bin`.
2. Stop Sterling B2B Integrator.
3. Start the database.
4. Export the system certificate to a PKCS12 file:  
`./ExportSystemCert.sh keyname pkcs12filename pkcs12storepass pkcs12keypass`
5. Find the object ID of the system certificate to remove. Enter:  
`./RemoveSystemCert.sh -l`
6. Remove the system certificate from the database. Enter:  
`RemoveSystemCert.sh -r xxxx` Where `xxxx` is the object ID of the certificate you wish to remove.



- To import the system certificate that you exported to the HSM and create a corresponding database entry:

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

**Note:** If you move the OpsDrv, OpsKey, and UIKey to the HSM, use the exact name. Otherwise, Sterling B2B Integrator will not function properly. For all other system certificates, the name is not critical. When moving system certificates other than the OpsDrv, OpsKey, and UIKey, the object ID that is used by services and adapters changes. Reconfigure any services that use the system certificates that were moved.

## Write CA-Issued Certificate to a File

### About this task

Use the GenCSR utility with the getcacert argument to write the certificate issued by the CA to a file.

### Procedure

- Ensure the getcacert.properties file is configured correctly.

The following table describes the parameters required in the getcacert.properties file for the getcacert Action. You must configure the getcacert.properties file before using the getcacert argument.

Parameter	Description	Valid Values
certificate.request.Name	Name of the CSR.	Certificate name
keystoretype	Name of the keystore used.	PKCS11IMPLKS(from V5.2.6.2 onwards) or nCipher.sworld or Luna
ca.cert.file	Fully qualified path to the file in which to write information about the CA certificate.	Name and path of a CA certificate file

- Write the certificate to a file.

The command syntax is `./GenCSR.sh -a getcacert -p ../properties/getcacert.properties`

## Generate Internal System Certificates (OpsDrv, OpsKey, UIKey) on the HSM

Three system certificates are installed with Sterling B2B Integrator to secure internal operations. Little security benefit is provided by moving them to the HSM. Your security policy can require that all certificates that contain private keys be stored on the HSM.

### About this task

When generating the Sterling B2B Integrator internal system certificates called OpsDrv, OpsKey, and UIKey on the HSM, use the exact names. Otherwise, Sterling B2B Integrator will not function properly.

To generate internal system certificates:

## Procedure

1. Navigate to `/install_dir/install/bin`.
2. Enter `./RemoveSystemCert.sh -l` to view certificates in the database. Note the object ID for each system certificate.
3. To delete the system certificates from the database by running the following command for each certificate: `./RemoveSystemCert.sh -r xxxx` where `xxxx` is the object ID of the certificate you want to remove.
4. Generate the system certificate on the HSM for each certificate, enter:  
`./CreateSystemCert.sh storetype provider autogen totrussttable signingbit keytype keysize keyname rfc1779rdnsequence serial validityindays [system passphrase] [store passphrase] [key passphrase]`

## Configure nCipher and SafeNet Luna Devices

### Key Store Provider Map

Sterling B2B Integrator has the keystore type that is unique across cryptographic service providers; it is able to define a mapping between keystore types and providers required for implementing the keystore object itself, signature algorithms, and key transport algorithms.

The key and key information abstraction object contains this information with a reference to a `com.sterlingcommerce.security.PrivateKeyInfo`.

This allows Sterling B2B Integrator to use a combination of keys on HSMs and in software stores in the database at the same time without additional configuration beyond the initial loading of the key or key information into the database. To Sterling B2B Integrator, the keys all look the same, regardless of where they are stored.

Mapping is implemented as a property called `KeyStoreProviderMap` in `security.properties`. It consists of a set of entries delimited by semi colons (;). Each entry has six elements delimited by commas and follow this format:

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

The elements are described in the following table:

Element	Description	Additional Information
KeyStoreType	The string type of the keystore	
KeyStoreProvider	The name of the cryptographic service provider that implements the keystore	
DoesAliasMatter	Whether the alias of keys must be unique for this keystore type	This can be either true or false. Keys have to have unique aliases in the case where there is only one keystore per device.
SignatureProvider	The name of the cryptographic service provider to use to create signatures using keys from the keystore	

Element	Description	Additional Information
EncryptionProvider	The name of the cryptographic service provider to use when decrypting information using keys in the keystore	This is mostly for RSA key transport operations
KeyOnHSM	Whether the keystore is on an HSM	

The string null is an acceptable value and will be treated as though no provider has been specified. An entry must have at least two values. If an entry contains less than six values, the values will be assigned from left to right to the keystore provider, whether the alias matters when storing the key, signature provider, encryption provider, and whether the key is on an HSM for the KeyStore type. The others will be treated as nulls and no specific provider will be requested for operations with keys of that type.

The default KeyStoreProviderMap is currently:

```
nCipher = nCipher.sworld,nCipherKM,false,nCipherKM,nCipherKM,true
SafeNet Luna = Luna,LunaProvider,true,LunaProvider,LunaProvider,true
Use "PKCS11IMPLKS,IBMPKCS11Impl,true,IBMPKCS11Impl,IBMPKCS11Impl,true" for both nCipher and SafeNet
```

### JDK Changes for nCipher HSM Support

In order for Sterling B2B Integrator to use nCipher HSMs, you must install the nCipher java cryptographic service providers. To install, copy the following jar files in the jre/lib/ext subdirectory of your JDK. Modify java.security to load the nCipher providers.

#### Note:

1. The following setup is not required if you are creating new Keys or Certificates using "PKCS11IMPLKS" implementation from V5.2.6.2 onwards.
2. To continue using the existing Keys or Certificates after upgrade to V5.2.6.2, follow these steps.

These files are placed in /opt/nfast/java/classes by the nCipher installation program:

- jcetools.jar
- jutils.jar
- keySAFE.jar
- kmjava.jar
- nCipherKM.jar
- nfjava.jar
- rsaprivenc.jar

You should add the nCipher providers after the IBM JCE provider and before the Certicom provider.

You must also remove IBMJCEFIPS from the list.

For example:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ncipher.provider.km.nCipherKM
```

```
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

Use the following example from V5.2.6.2 onwards to support the existing Keys or Certificates.

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ncipher.provider.km.nCipherKM
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

## JDK Changes for SafeNet Luna HSM Support

In order for Sterling B2B Integrator to use SafeNet Luna HSMs, you must install the SafeNet Luna java cryptographic service provider. To install, place the appropriate.jar files in the jre/lib/ext subdirectory of the JDK and then modify java.security to load the Luna providers.

### Note:

1. The following setup is not required if you are creating new Keys or Certificates using "PKCS11IMPLKS" implementation from V5.2.6.2 onwards.
2. To continue using the existing Keys or Certificates after upgrade to V5.2.6.2, follow these steps.

These files are placed in /opt/nfast/java/classes by the nCipher install program:

- libLunaAPI.so
- LunaProvider.jar

You should add the LunaProvider after the IBM JCE provider and before the Certicom provider.

You must also remove IBMJCEFIPS from the list.

For example:

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.safenetinc.luna.provider.LunaProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.security.jgss.IBMJGSSProvider
security.provider.7=com.ibm.security.cert.IBMCertPath
security.provider.8=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.9=com.sterlingcommerce.security.provider.SCI
security.provider.10=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.11=com.certicom.jsse.provider.CerticomJSSE
```

Use the following example from V5.2.6.2 onwards to support the existing Keys or Certificates.

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.safenetinc.luna.provider.LunaProvider
security.provider.3=org.bouncycastle.jce.provider.BouncyCastleProvider
security.provider.4=com.certicom.ecc.jcae.Certicom
security.provider.5=com.sterlingcommerce.security.jcae.STERCOMM
security.provider.6=com.ibm.jsse2.IBMJSSEProvider2
security.provider.7=com.ibm.security.jgss.IBMJGSSProvider
security.provider.8=com.ibm.security.cert.IBMCertPath
security.provider.9=com.sterlingcommerce.security.keystoreprovider.SCIKS
security.provider.10=com.sterlingcommerce.security.provider.SCI
security.provider.11=com.sterlingcommerce.security.jsseimpl.spi.SCIKM
security.provider.12=com.certicom.jsse.provider.CerticomJSSE
```

## Configure HSM using IBM PKCS11IMPLKS (V5.2.6.2 or Later)

### Configure HSM using IBM PKCS11 IMPLKS Implementation (V5.2.6.2 or Later)

#### About this task

From version 5.2.6.2 onwards, the system supports IBM PKCS11 implementation for HSM devices. HSMs implement Java JCE API. This interface accesses the keys in the device.

#### Procedure

1. A new property file **hsm.properties.in** is added for supporting PKCS11IMPLKS/IBMPKCS11Impl.

The following table lists the properties that are specific to configure HSM.

Attribute	Description
HSM_KEYSTORE_TYPE	If HSM_ENABLED is set to <i>true</i> the attribute value must be <i>IBMPKCS11IMPLKS</i> .
HSM_KEYSTORE_PROVIDER	If HSM_ENABLED is set to <i>true</i> the attribute value must be <i>IBMPKCS11Impl</i> .
HSM_KEYSTORE_FILE	<Should be left blank>
HSM_ADAPTER_TYPE	ncipher or safeNetFor ncipher, run the following command while creating or updating Keys or Certificates -  For UNIX: export CKNFAST_OVERRIDE_SECURITY_ASSURANCES= "longterm;tokenkeys"  For Windows: set CKNFAST_OVERRIDE_SECURITY_ASSURANCES ="longterm;tokenkeys"
HSM_ENABLED	This attribute must be set to <i>true</i> for HSM support.
HSM_PRNG_ALGORITHM	If HSM_ENABLED is set to <i>true</i> the attribute value must be <i>PKCS11DeviceRNG</i> .
HSM_CONFIG_FILE_LOCATION	If HSM_ENABLED is set to <i>true</i> the attribute value must be set to the location of the IBMPKCS11 configuration file

2. Update or create the configuration file required for the HSM setup based on the HSM type.

For the HSM type, you can find the configuration file for the device as shown below or you can ask IBM support to get the configuration file. You can update any of the default settings as required. You must edit the *library* value if your location is different from the default.

For SafeNet Luna Device:

```
lunasa_5_0_jsse.cfgname = B2Bi
library=/usr/safenet/lunaclient/lib/libCryptoki2_64.so
description=Luna SA 5.0 IBM SSP config - JSSE
```

```
publickeyimportonly=false
slotListIndex = 0
disabledMechanisms = {
    CKM_MD5
    CKM_SHA_1
    CKM_MD5_HMAC
    CKM_SHA_1_HMAC
    CKM_DES_CBC
    CKM_DES_CBC_PAD
    CKM_DES_ECB
    CKM_DES3_CBC
    CKM_DES3_ECB
    CKM_DES3_CBC_PAD
    CKM_AES_CBC
    CKM_AES_ECB
    CKM_AES_CBC_PAD
    CKM_RC4
    CKM_SSL3_MASTER_KEY_DERIVE
    CKM_SSL3_KEY_AND_MAC_DERIVE
    CKM_SSL3_PRE_MASTER_KEY_GEN
    CKM_TLS_PRE_MASTER_KEY_GEN
    CKM_TLS_MASTER_KEY_DERIVE
    CKM_TLS_KEY_AND_MAC_DERIVE
    CKM_TLS_MASTER_KEY_DERIVE_DH
    CKM_TLS_PRF
    CKM_SHA256_HMAC
    CKM_SHA384_HMAC
    CKM_SHA512_HMAC
    CKM_EC_KEY_PAIR_GEN
    CKM_ECDSA_KEY_PAIR_GEN
    CKM_ECDH1_DERIVE
    CKM_ECDH1_COFACTOR_DERIVE
    CKM_ECMQV_DERIVE
    CKM_DH_PKCS_KEY_PAIR_GEN
    CKM_DH_PKCS_PARAMETER_GEN
    CKM_DH_PKCS_DERIVE
}
attributes (*, CKO_PRIVATE_KEY, *) = {
    CKA_SENSITIVE = true
    CKA_SIGN = true
    CKA_DECRYPT = true
    CKA_DERIVE=true}
attributes (*, CKO_PUBLIC_KEY, *) = {
    CKA_VERIFY = true
    CKA_ENCRYPT = true
    CKA_DERIVE = true}
attributes (*, CKO_SECRET_KEY, *) = {
    CKA_SENSITIVE = true
    CKA_ENCRYPT = true
    CKA_DECRYPT = true
    CKA_SIGN = true
    CKA_VERIFY = true}
```

For nCipher Device:

```
===== ncipher_gen2.cfg.jsse
#nCipher nShield, nForce - Generation 2 cards
name =B2Bi
library=/opt/nfast/toolkits/pkcs11/libcknfast.so
description= IBM SSP NCIPHER HSM ADAPTER config for JSSE

slotListIndex = 1
disabledMechanisms = {
    CKM_MD5
    CKM_SHA_1
    CKM_MD5_HMAC
    CKM_SHA_1_HMAC
    CKM_SHA256_HMAC
    CKM_SHA384_HMAC
    CKM_SHA512_HMAC
    CKM_EC_KEY_PAIR_GEN
    CKM_ECDSA_KEY_PAIR_GEN
    CKM_ECDSA
    CKM_ECDSA_SHA1
    CKM_ECDH1_DERIVE
    CKM_ECDH1_COFACTOR_DERIVE
    CKM_ECMQV_DERIVE
}
attributes(*, CKO_SECRET_KEY, *) = {
    CKA_ENCRYPT=true
    CKA_DECRYPT=true}
attributes(*, CKO_PRIVATE_KEY, *) = {
    CKA_TOKEN=false
    CKA_SIGN=true
    CKA_SENSITIVE=false}
attributes(GENERATE, CKO_PRIVATE_KEY, CKK_RSA) = {
    CKA_DECRYPT=true
    CKA_UNWRAP=true
    CKA_EXTRACTABLE=true}
attributes(GENERATE, CKO_PUBLIC_KEY, *) = {
    CKA_TOKEN=false
    CKA_VERIFY=true}
attributes(*, CKO_PUBLIC_KEY, CKK_RSA) = {
    CKA_ENCRYPT=true
    CKA_WRAP=true
    CKA_VERIFY=true}
attributes(IMPORT, CKO_PRIVATE_KEY, CKK_RSA) = {
    CKA_EXTRACTABLE=true
    CKA_DECRYPT=true
    CKA_UNWRAP=true
    CKA_DERIVE=true}
```

**Note:** SafeNet Luna does not allow you to import an externally-created private key. You must create and store them on the HSM device.





---

## Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

#### COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as shown in the next column.

© 2015.

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. 2015.

---

## Trademarks

IBM, the IBM logo, and [ibm.com](http://ibm.com) are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center<sup>®</sup>, Connect:Direct<sup>®</sup>, Connect:Enterprise<sup>®</sup>, Gentran<sup>®</sup>, Gentran<sup>®</sup>:Basic<sup>®</sup>, Gentran:Control<sup>®</sup>, Gentran:Director<sup>®</sup>, Gentran:Plus<sup>®</sup>, Gentran:Realtime<sup>®</sup>, Gentran:Server<sup>®</sup>, Gentran:Viewpoint<sup>®</sup>, Sterling Commerce<sup>™</sup>, Sterling Information Broker<sup>®</sup>, and Sterling Integrator<sup>®</sup> are trademarks or registered trademarks of Sterling Commerce<sup>®</sup>, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

---

## Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

### Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

### Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

### Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

### Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.





Product Number:

Printed in USA