Sterling Integrator®

Security

Version 5.0

Contents

Security Overview

Sterling Integrator Security Policy Overview

Sterling 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 are the provided out of the box:

- Role-based security provides users access to certain 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 with the application 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 password/passphrase - During installation, you create a system passphrase for your Sterling 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.
- Digital Certificates provides information about the identity of an entity. Digital certificates are issued by a certification authority (CA). The CA guarantees the validity of the certificate information.
- Federal Information Processing Standards (FIPS)
- Secure Socket Layering (SSL) is a protocol that provides secure communication over the Internet. It uses both symmetric and asymmetric cryptography

Additionally, the following security features can be configured:

- Security time out feature can be used to protect your system. For example, if you depart and come back to the computer and try to start working again, and if this time period is beyond the time out setting in your user account, you are prompted to log in again. Web Extensions also uses the same security time out feature
- 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 the traditional file and database permissions.

Network Deployment Planning

Before deploying Sterling Integrator, you must evaluate the different deployment options and determine which one best fits your budget, current infrastructure, and provides the most secure environment for your data.

Because Sterling Integrator handles critical and sensitve data, it should be deployed in a secure zone behind a firewall within your network. A firewall is a blockade between a secure internal network and an untrusted network such as the Internet. You can also use a firewall to secure one internal network from another on an intranet. If you do not deploy Sterling Integrator behind a firewall, you will be exposing your system to unwanted and possibly undetected attacks by unauthorized users.

Depending on your industry, there may be regulatory compliancies that require Sterling Integrator to NOT be deployed in a non secure zone (forward zone of a demilitarized zone) of a network.

When you use a firewall as your gateway to the Internet (or other network), you reduce the risk to your internal network considerably. This enables safe, secure e-business by controlling all communications to and from the Internet.

See the Perimeter Server topics in the documentation library for more information on Sterling Integrator deployment options.

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 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 application.

Groups 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

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

To search for a group:

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

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:

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

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:

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

To delete a group:

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 application deletes the group and displays the message: *The system update has completed successfully.*

Review the Group Name and ID

To review a group name and ID:

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 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

Two permissions may have the same name, although it is not recommended. The permission ID associated with a permission name must be unique. For example, the permission name Configuration with permission ID MBXADM1 is a different permission and grants different access than the permission Configuration with permission ID PLTADM10.

Permission naming conventions include:

- Names are case-sensitive.
- Two names with different capitalization are considered to be unique 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.

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	Admin Web App Permission, MyAccount
ADAPTER_UTILITIES	ADAPTER_UTILITIES	BEATuxedo, CDNetmaps, CDNetmapXref, CDNodes, SAPRoutes, SAPRouteXREF, SAPSuiteBuilder, UI Adapter Utilities
ADVANCED_SETUP	ADVANCED_SETUP	DeliveryChannels, DocumentExchange, Identities, Packaging, Profiles, Transports, UI Advanced Trading Profile Setup
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
Business Process	bpadmin	All permissions from the BPMONITOR and SERVICES subgroups, plus UI BP Manager, UI Business Process, UI Delete BP.

Group Name	Group ID	Permissions Inherited from the Group
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.
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: • AFT • Default • Community Management Operator, Participant, Participant Sponsor, or Sponsor Administration Management Console, Business Process Search Portlet, Cache Statistics Portlet, Cache Usage Portlet, Community Management Portlet, Community Statistics Portlet, Database Pool Usage Portlet, Database Status Portlet, Database Usage Portlet, Document Search Portlet, Document Tracking Portlet, Documents Processed Bar Chart Portlet, Documents Processed Time Series Portlet, Event Viewer Portlet, IFrame Portlet, Log File Viewer Portlet, Log File Viewer Portlet 2, ParticipatingCommunities Portlet, Peers Portlet, Queue Priority Statistics Portlet, Quick Links Portlet, RSS Feed Portlet, Sponsored Communities Portlet, System Alerts Portlet, Web Search Portlet, Web View Plus Portlet
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

Group Name	Group ID	Permissions Inherited from the Group
EBICS Administrators	EBICS_ADM	UI EBICS Menu, UI EBICS Subscription Manager, UI EBICS Order Type Manager, UI EBICS File Format Configuration, UI EBICS Order Type Configuration, UI EBICS Profile Manager, UI EBICS Bank Profile Configuration, UI EBICS Partner Profile Configuration, UI EBICS User Profile Configuration, UI EBICS Offer Manager, UI EBICS Offer Configuration, UI EBICS Contract Configuration, UI EBICS User Permission Configuration, UI EBICS Subscriber Key Validation UI Delete EBICS File Format Configuration, UI Delete EBICS Order Type Configuration, UI Delete EBICS Bank Profile Configuration, UI Delete EBICS Partner Profile Configuration, UI Delete EBICS User Profile Configuration, UI Delete EBICS User Permission Configuration, UI Delete EBICS Offer Configuration, UI Delete EBICS Contract Configuration
EBICS Operators	EBICS_OPERATOR	UI EBICS Menu, UI EBICS Subscription Manager, UI EBICS Order Type Manager, UI EBICS File Format Configuration, UI EBICS Order Type Configuration, UI EBICS Profile Manager, UI EBICS Bank Profile Configuration, UI EBICS Partner Profile Configuration, UI EBICS User Profile Configuration, UI EBICS Offer Manager, UI EBICS Offer Configuration, UI EBICS Contract Configuration, UI EBICS User Permission Configuration, UI EBICS Subscriber Key Validation
EBXML	EBXML	BPSS, BPSSExtension, CPA, UI EBXML
ENVELOPES	ENVELOPES	ControlNumberHistory, ControlNumbers, EDISequenceCheckQueue, 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
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

Group Name	Group ID	Permissions Inherited from the Group
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
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 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,

Group Name	Group ID	Permissions Inherited from the Group
		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
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

Group Name	Group ID	Permissions Inherited from the Group
		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
Web Suite Purchasers	wspurchaser	WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite Purchase Req View Template, WebSuite Query Business Process, WebSuite Query LIst Template, WebSuite Self Registration Business Process
Web Suite Suppliers	wssupplier	WebSuite ASN Send Business Process, WebSuite ASN Template, WebSuite ASN View Template, WebSuite Change Password Confirm Template, WebSuite Change Password Template, WebSuite Confirm Send Template, WebSuite Draft Save Business Process, WebSuite Email Notification Business Process, WebSuite Email Notification Template, WebSuite Invoice Send Business Process, WebSuite Invoice Template, WebSuite Invoice View Template, WebSuite Load Business Process, WebSuite Menu Business Process, WebSuite PO Ack Send Business Process, WebSuite PO Ack Template, WebSuite PO Ack View Template, WebSuite PO to Advance Ship Notice Template, WebSuite PO to Invoice Template, WebSuite PO to PO Ack Template, WebSuite PO Turn Business Process, WebSuite PO View Template, WebSuite Query Business Process, WebSuite Query LIst Template, WebSuite Remittance Advice View Template, WebSuite Self Registration Business Process

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 > SWIFTNET Correlation	SWIFTNETCorrelation (GISADM9) plus UI BP Monitor (BPMONITOR) and UI SWIFTNet Routing Rule (SWIFTNET_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)
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)

From the Administration Menu > Business Process, UI Resource	Permission Name / Permission ID
Business Process > Message Entry Workstation	Message Entry Workstation Home (MESSAGE_ENTRY_HOME)

From the Administration Menu > Trading Partner, UI Resource	Permission Name / Permission ID
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)
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)

From the Administration Menu > Trading Partner, UI Resource	Permission Name / Permission ID
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)
Trading Partner > Odette FTP Partner Profile > Logical Partner Contract	OftpLogicalPartnerContract (ASSETOFTP4)

From the Administration Menu > Trading Partner, UI Resource	Permission Name / Permission ID
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)

From the Administration Menu > Deployment, UI Resource	Permission Name / Permission ID
Deployment > Services > Installation/Setup	Installation/Setup (PLTADM9) plus UI Services (SERVICES)
Deployment > Services > Configuration	Configuration (PLTADM10) plus UI Services (SERVICES) and UI BP Manager (BPMANAGE)
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)

From the Administration Menu > Deployment, UI Resource	Permission Name / Permission ID
Deployment > EBXML > BPSS	BPSS (ASSETADM7) plus UI EBXML (EBXML)
Deployment > EBXML> BPSS Extension	BPSSExtension (ASSETADM8) plus UI EBXML (EBXML)
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 (ASSETADMIN50)
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 > 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)

From the Administration Menu > Deployment, UI Resource	Permission Name / Permission ID
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)

From the Administration Menu > e-Invoicing, UI Resource	Permission Name / Permission ID
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)

From the Administration Menu > Operations, UI Resource	Permission Name / Permission ID
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)

From the Administration Menu > Operations, UI Resource	Permission Name / Permission ID
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 Integrator Admin group
Federated Systems	UI Federated Systems (FEDERATED_SYSTEMS)

From the Administration Menu > Accounts, UI Resource	Permission Name / Permission ID
Groups	UI Groups (GROUPS) plus UI Accounts (ACCOUNTS)
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 application. Like custom permissions, they provide access to the different modules within the system.

Search for Permission Names

To search for a permission:

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

Before you begin you need to know the following information:

Field	Description
Permission ID	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. Permission IDs: • They must be unique. • They are case-sensitive. • 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.
Permission Name	Name of the permission you are creating. Required. A permission name does not need to be unique. Permission names are case-sensitive.
Permission Type	Permission type of the permission you are creating. Required. Permission types include: • UI – Allows access to specific menu items in the interface. UI Permissions with a Permission ID prefixed by _DENY_ deny access to that particular resource or action. For example, if you add a permission, _DENY_BPMANAGE to a user or a group, the user or group will not be able to access BP Management UIs. • Mailbox – Allows access to specific mailboxes in the application. • Template – Allows access to specific Web templates. • BP – Allows access to specific business processes. • Tracking – Allows access to specific document tracking options. • Community – Allows access to specific community management options. • Web Service • Service • eInvoicing • Other – Allows access to resources that are not identified by one of the preceding types.

To create a permission:

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 have need to change the name of a permission to reflect the permission more closely, you edit a permission name. You cannot change the permission ID. If you need to edit the permission ID, you must create a new permission.

To edit a permission name:

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. If the permission you are deleting is the only permission 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 to the application, but has no access to any menu items.

To delete a permission:

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 application deletes the permission and displays the message *The system update completed successfully.*

Review the Permission Name and ID

To review a permission name and ID:

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 permisssion 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 is 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

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 accounts authentication can be either:

- Local – Authentication is completed against the Sterling Integrator database.
- External – Authentication is completed against an LDAP server. External authentication does not require the Sterling Integrator LDAP adapter, which is used with business processes and enables Sterling Integrator to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI). If you do not have a license for single sign on or LDAP in the application, all 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

Use this checklist to create an user account:

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

Before creating an external user account, you must:

1. Stop Sterling 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 Integrator.

Search for User Accounts

To search for an user account:

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

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.

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 characters long. 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 characters long. 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. Sterling Integrator 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 on the application 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: • Admin UI – Accesses the Admin Console pane in the application dashboard only. • AS2 UI – Accesses the AS2 Edition interface only. • UCCNET UI – Access to the UCCnet Edition interface only. • Dashboard UI – Accesses dashboard interface. Refine by choosing a Dashboard Theme.

Field	Description
Dashboard Theme	Predefined dashboard that the user account has access to. Required if accessibility is set as Dashboard UI. The following are dashboard theme options: • Default • Operator • Participant • Participant Sponsor • Sponsor • AFT
First Name	User's first name. Required.
Last Name	User's last name. Required.
E-mail	User's e-mail address.
Pager	User's pager number.
Preferred Language	User's preferred language. Select from: English, French, Japanese, or Spanish.
Manager ID	User ID of the user's manager.
Identity	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. The default value is **Hub Organization**.

To create a user account:

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 **First Name**.
16. Enter the **Last Name**.
17. Enter the **E-mail address**.
18. Enter the **Pager number**.
19. Select the **Preferred Language**.
20. Enter the **Manager ID**.
21. Select the **Identity**.
22. Click **Next**
23. Review the user account settings.
24. Click **Finish**.
    The application creates the user account and displays the message: *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. Sterling Integrator will authenticate the external user ID on the external LDAP server.

Edit User Accounts

To edit an user account:

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 can not remove the Admin Web App Permission or MyAccount.
11. Make any changes to the user information and click **Next**.
12. Review the user account settings.

13. Click **Finish**.

Delete User Accounts

To delete an user account:

1. From the **Administration Menu**, select **Accounts** > **User Accounts**.
2. Locate the user account 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 application deletes the selected user account and displays the message: *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 you see when you log in to the application.

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.

To update your account information:

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 **First Name, Last Name, E-mail, Pager, Manager ID**, or **Identity** 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.
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 application to autocomplete searches based on strings that you have entered previously, then select **Autocomplete for searches**.
11. If you want the application 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 application saves the new account information and displays the message, *Your update has completed successfully*.

Single Sign On

Single Sign On

Single Sign On (SSO) is an authentication process that enables users to access several applications and only have to enter one user name and password. Previously, a user 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 and enables this application to communicate with local or remote LDAP servers using a Java Naming Directory Interface (JNDI).

Sterling Integrator supports SSO from CA SiteMinder, SSP, and other applications.

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

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).

You can configure the SSO to redirect to an external HTTP page (instead of the Sterling 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.debug) {
          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 Integrator allows a custom implementation class for Single Sign On (SSO) plug-ins on other single sign on applications and servers. You must add a new implementation class SSO_AUTHENTICATION_CLASS.<n>=<New class entry> in security.properties file to implement a 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, HttpServletResponse response,
 int reason, String sessionType)
throws SSOAuthenticationException;
public boolean authenticatePage(HttpServletRequest request)
```

```
throws SSOAuthenticationException, SSOException;
}
```

SSOException class

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

SSOAuthenticationException class

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

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 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 CA SiteMinder Checklist

Before you can configure Single Sign On (SSO), you must have knowledge of SSO and of CA SiteMinder. Use this checklist to configure SSO with CA SiteMinder:

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

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

Configure Properties Files for Single Sign On with CA SiteMinder

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

1. Stop Sterling 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 n-1 classes failed
SSO_AUTHENTICATION_CLASS.1=com.sterlingcommerce.woodstock.security.authentication.SS
 OProviderDefault
## 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 Sterling Commerce 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 CA SiteMinder or your SSO application configuration.	SM_USER This is the value in CA SiteMinder.	Must match the entry in CA SiteMinder or your SSO application.
SSO_PAGE_AUTHENTICATION_ENABLED	Enables or disables SSO authentication on every page	False	True–To authenticate SSO on every page. **Note:** Change only if custom SSO Provider Class is provided.
SSO_AUTHENTICATION_CLASS.n	Implementation class to provide authentication support.	com.sterlingcommerce.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 Integrator.

Configure CA SiteMinder Secure Proxy Server

Before you configure the CA SiteMinder Secure Proxy Server, you must:

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

To configure the CA SiteMinder Secure Proxy Server:

1. Add the necessary forwarding rules for Sterling 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 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="/ws">
   <nete:forward>http://acme.gis.com:12400$0</nete:forward>
</nete:case>
<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="/certwiz">
   <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="/ssdk">
   <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="/communitymanagement">
   <nete:forward>http://acme.gis.com:12400$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 Integrator does not support CA SiteMinder 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 CA SiteMinder Policy Server Secure Realms

For Sterling Integrator to work with CA SiteMinder Secure Proxy Server, the CA SiteMinder Policy Server Administrator must create Secure Realms around each of the URL patterns being forwarded by the Secure Proxy Server. These Security Realms must have the necessary rules assigned for authentication and authorization. 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:
/ws/*	Standard application interface, using the http://host:port/ws format
/mbi/*	Application Mailbox interface
/dashboard/*	Application dashboard interface, using the http://host:port/dashboard format
/communitymanagement/*	Application community management interface through the dashboard interface
/datastore/*	Datastore components
/portlets/*	Application portlet components in the dashboard interface
/ssdk/*	Service Developer's Kit components
/help/*	Context-sensitive help components
/webxtools/*	Web Extensions Utilities
/certwiz/*	Certificate Wizard components
/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 Integrator Custom Password Policy is a security feature that 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. 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

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, such as a numeral, capital letter, !, @, #, $, %, ^, &, or *
- User must change default password during initial log in
- 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 to the application 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 application prompts the user for corrections. Once all conditions set in the password policy are met by the user changing the password, the application 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 log in 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 application.

Installation Password or Passphrase

During installation, you create a system passphrase for your Sterling 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 application running as a non-interactive service. It can be stored in the clear on other platforms in security.properties so you don 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

Use the following checklist to implement a customer password policy:

Task	Custom Policy Password Checklist
1	Specify the Java class implementing the password policy (passwordPolicyExtensionImpl property) in the customer_overrides.properties file.
2	Add the implementation class jar to the classpath.
3	Define error message.

Example - Custom Policy Password

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

To search for a password policy:

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 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.

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 user is prompted to change the password when this time period expires. The default is 0, which means the password never expires. You can change this number to any number you want, there is no maximum. The expiration count down starts the first time a user logs in to the application 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 application 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, such as numeral, capital letter, !, @, #, $, %, ^, &, 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:

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

To edit the password policy:

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 associated with that specific password policy can still log in, but the user will not be forced to change the password. If the user does change the password, no validation is completed against the new password.

To delete a password policy:

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 application notifies you of impending password expirations by placing a message in the System Alerts section of the application Admin Console Home page. 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 application, 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:

1. Stop Sterling 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 the application.

   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

You can:

- Log in using any other computer that has access to the application.
- 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 in the application. This allows you to try to log in using the locked computer again.

Define Error Message for Custom Password Policy

The 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:

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

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:

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

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

1. Navigate to the directory where the password extension class files are located.
2. Enter: `javac -cp /install_dir/jar/woodstock.jar test/policy/extension/*.java`
3. Enter: `jar cf <new_filename>.jar <path_to_class_file>/<Custom_Impl>.class`

   Where <new_filename>.jar is the name of the new Jar file to be created and where <Custom_Impl>.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 the installation directory.
5. Navigate to the bin directory.
6. Enter: `Install3rdParty.sh userExit 1_0 -j <path_to_user_exit_jar>`

LDAP Authentication

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

Lightweight Directory Access Protocol (LDAP) is a set of protocols used to access information 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 with the application 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.

User account authentication does not require the LDAP adapter, which is used with business processes and enables the application 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 to the application; however, those users who have external accounts do not have access to the application until the LDAP server is working.

Before you can configure LDAP with Sterling 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 application 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

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=falseBelow the ##LDAP Authentication
```

LDAP Authentication Configuration Checklist

Use this checklist to configure LDAP with Sterling Integrator:

Tasks	LDAP Configuration Checklist
1	Configure LDAP in one of the following modes: • Password Comparison Mode • Password Binary Mode
2	Configure LDAP with Sterling Integrator
3	Verify LDAP configuration

Configure LDAP in Password Binding Mode

To configure LDAP in a password binding mode:

Enter your **user ID** and **password** from your external user account into the application.

The application:

- 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 application binds to the LDAP repository as a user.
- Failure – The application cannot bind to the LDAP repository as a user.

Configure LDAP in Password Comparision Mode

To configure LDAP in a password comparison mode:

1. Enter your **user ID** and **password** from your external user account into the application.
2. The application attempts to bind to the LDAP repository with credentials enabling execution of necessary queries.
3. The application searches for the user in the LDAP directory with the proper userid.
4. The application retrieves the user password from the LDAP directory.
5. The application 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 application. If the passwords do not match, you are not authenticated and not permitted access.

Configure LDAP with Sterling Integrator

To configure the application 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 will not be overwritten by a patch installation.

To configure LDAP authentication:

1. Stop Sterling 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
#LDAP_SECURITY_TRUSTSTORE	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.
#LDAP_SECURITY_TRUSTSTORE_PASSWORD	Password that allows access to the truststore.Optional. Use only if you are using SSL.	changeit	Password allowing access to the local truststore.
#LDAP_SECURITY_KEYSTORE	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.

Parameter	Description	Shipped Value	Change to
#LDAP_SECURITY_KEYSTORE_PASSWORD	Password that allows access to the keystore. Optional. Use only if you are using SSL.	password	Password allowing access to the local keystore.
#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 application supports only simple authentication.	simple	No change
#authentication_<number>.principle	Identity of the principle to authenticate, which enables the application 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 application to perform queries.	Sterling	Local password that goes with your local principle.

Parameter	Description	Shipped Value	Change to
#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.
#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 (sAMAccount Name=<userid>)
#authentication_<number>.with_user_bind	Specifies whether to authenticate a user according to a successful bind. False – The application extracts the value of the user password from the LDAP server and performs a comparison to the user credentials provided. True – The application 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 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 application identifies LDAP servers from the authentication_policy.properties file. The application authenticates external users when the users log in to the application.

Verify LDAP Configuration

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

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.

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:

(**GRAPHICS NEED TO BE IMPORTED LATER for the SYMBOLS)**

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

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.

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

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.

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

To search for a user news message:

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

To edit an user news message:

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

To delete an user news message:

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: *The system update completed successfully.*

Document Encryption

Document Encryption Feature Overview

Document encryption is a feature provided with Sterling Integrator. This feature allows for the configuration of an additional layer of security beyond the traditional file and database permissions. If you have integrated Sterling File Gateway with Sterling Integrator, it uses the same document encryption feature for protecting data at rest. Sterling File Gateway is a managed file transfer product that is used for secure and automated edge communications with trading partners.

The document encryption feature is intended to protect data at rest from being viewed by an unauthorized user. 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. If you do you must update the value of CERT_NAME in the customer_overrides.properties file.

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:

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 Integrator.

Enable Document Encryption for File System and Database Documents

To encrypt file system and database documents:

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 Integrator.

Enable Document Encryption for Database Documents

To encrypt database documents:

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 Integrator.

Enable Document Encryption for File System Documents

To encrypt file system documents:

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 Integrator.

Disable Document Encryption for Documents

The default configuration at installation is no encryption.

To disable document encryption:

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 Integrator.

Certficates

Digital Certificates

Sterling Integrator provides a Certificate Wizard 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. You can use the Certificate Wizard to generate the certificate or it can be generated externally.
- 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 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 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. In the application, trusting a CA root means that you trust all certificates issued by that CA. If you elect not to trust a CA root, Sterling 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 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 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 generally 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

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 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 can also explicitly not trust a self-signed certificate of a trading partner.

Expiration Dates for Certificates

If an adapter and servlet are used for inbound communications (for example, receiving AS2 data from trading partners), you must monitor the expiration dates of the system certificates to ensure the certificates are valid. Before the certificates expire, they must be replaced with valid certificates.

System Cerificate Parameter Definitions

If an adapter and servlet are used for inbound communications (for example, receiving AS2 data from trading partners), you must monitor the expiration dates of the system certificates to ensure 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.
Certtype	The certificate type to import. Four types of certificate files are supported: pkcs12, pkcs8, pem, and keystore. Sterling 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: • ERACOM • ERACOM.n (if you are importing certificates to a slot other than the first position)

Parameter	Description
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.

Certificate Wizard

Sterling Certificate Wizard

The Sterling Certificate Wizard is a Web-deployed application. The wizard enables you to create the following files:

- 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 (key cert.txt). If you generate key certificates using the standard format (default) with certain cipers, the output certificate will error when imported into the Sterling Integrator. It is recommended that you use the PKCS12 Format for the key certificates.
- Trusted root files – The trusted root file (trusted.txt) contains a list of trusted sources that enable the certificate wizard to validate a key certificate and ensure a secure connection.

See the wizard online help for information on generating a Certificate Signing Request (CSR), creating a key certificate, and validating a key certificate.

Download and Install the Sterling Certificate Wizard

To download the Sterling Certificate Wizard:

1. Access IBM Web Management (IWM) to access Sterling Legacy downloads, see *https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-SterlngLegacyreq*

   Note: You must have an IBM ID and Password and your company's access key. If you do not have an IBM ID and Password, see *https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=swg-SterlngLegacydl* to generate an ID login.

2. On the Sterling Legacy Software Request page, in the Entitlement area, type your access key.
3. Select the option that best describes your company or organization.

4. Select the type of role you have in acquiring software solutions.
5. Click **Submit**
6. On the Downloads page, select *Sterling Certificate Wizard, version 1.3.00 patch 2 build 197 Version 1.3.00*
7. Click **Submit.**
8. Select either the Unix or Windows download version that you want to use and confirm licensing to initiate the download.

Start the Sterling Certificate Wizard

You must download and install the Sterling Certificate Wizard before you can start the wizard.

To start the Sterling Certificate Wizard:

1. Click **Start** > **Programs**.
2. Select **Certificate Wizard (version number)** > **Certificate Wizard**.

   The Certificate Wizard is displayed.

   See the wizard online help for information on generating a Certificate Signing Request (CSR), creating a key certificate, and validating a key certificate.

Generate a Certificate Signing Request (CSR) Using the Certificate Wizard

To generate a CSR using the Certificate Wizard:

1. Start the Certificate Wizard.
2. Select **Generate CSR**.
3. Enter the client computer name in the **Common** field.
4. Enter **Country**, **State/Province**, and **City/Locality**.
5. Enter the **Organization/Company Name**.
6. Enter the **Organization Unit**.
7. Enter your **Email Address**.
8. Click **Next**.
9. If you want the pseudo-random number generator (PRNG) to generate a random number for the public/private key pair, enter any random sequence of characters until processing stops.
10. In the Message dialog box that indicates enough random input is now available (random generated number for the public/private key pair), click **OK** and then click **Next**.
11. Enter the **Private Key Length**.

    Valid values are:

    • 512
    • 768
    • 1024
    • 2048
    • 4096

    The key length 1024 provides a good balance between security, interoperability, and efficiency. The key length 4096 is the most secure, but also the slowest, and may not work with some applications.

12. Enter the **Passphrase**.

    Passphrase must not be more than 20 characters in length.

13. Enter the passphase a second time in **Confirm Passphrase**.
14. Click **Next**.
15. Enter the **Key file name**.

    Either accept the default directory or click **Browse** and select another directory to save the PKCS12-formatted private key (privkey.txt is the default file name) file.

16. Enter the**CSR file name**

    Either accept the default directory or click **Browse** to select another directory to save the CSR (csr.txt is the default file name) file.

17. Review the information.
18. Click **Next** to create the CSR.

Create a Key Certificate Using the Certificate Wizard

To create a key certificate using the Certificate Wizard:

1. Start the Certificate Wizard.
2. Select **Key Certificate**.
3. Select the key certificate you want to generate from **Output Keycert/Keystore Format**.

   Valid values are Standard, JKS, and PKCS12.

4. Enter the directory or click **Browse** to select the directory to which you have saved the private key file (privkey.txt).
5. Specify the passphrase associated with the private key in the **Private Key Passphrase**.
6. Enter the directory or click **Browse** to select the directory to which you have saved the Digitally-signed (cert.crt) certificate from the CA.
7. Either accept the default directory or click Browse to select another directory to save the key certificate (keycert.txt) file.
8. Click **Generate** to create the key certificate.

Validate a Key Certificate Using the Certificate Wizard

To validate a key certificate using the Certificate Wizard:

1. Start the Certificate Wizard.
2. Select **Verify Certificate**.
3. Enter the **Passphrase**.
4. Select the key certificates to verify.

   Enter the full path to directory and file name or click **Browse** to select the directory and files.

5. Click **Verify**.

   A message displays that includes the verification results for each file you selected.

Certificate Tasks

Create a Self-Signed Certificate

To create a self-signed certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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.
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 (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.)
    - 2048
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**.

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 have the option to include or exclude the status information. Because the status information is compiled in real time, you may not want to include it.

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:

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 Integrator.

Configure Thumbprint Displays

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

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

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

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: • SHA-256 • SHA-384 • SHA-512

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

Search for CA Certificates

To search for a CA certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
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. The following fields are configurable in the system.

Certificate Summary Field	Description
System Name	The Certificate Name is the database label. It is used to refer to this certificate in the GUI and the application stores this name in its database. 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. You can change a certificate name to a shorter or more recognizable name when checking in or editing the certificate.
Thumbprint	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.
Status	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.

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 UI

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:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
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	1. Click **Import** from **JVM**. 2. Accept the default password that appears in the password field and click **Next**. The default keystore password is supplied by Sun Microsystems. If the password field is empty, the system still uses the default password.
Import from File – Imports certificates saved as a file on a local drive	1. Click **Import** from **File**. 2. Enter the Filename or click **Browse** to select a CA certificate file. Click Next. You may ignore the password that appears in the password field. There is no need to erase the entry.

   Available certificates are listed with a summary of identifying information. All certificates are selected by default.
4. Click the checkboxes 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

Common CA certificates are contained in a JKS keystore that is part of the JVM that is shipped with Sterling 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 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:

1. Navigate to the installation directory.
2. Navigate to the bin directory.
3. Enter this command:

   (UNIX) `./ImportCACerts.sh`

   (Windows) `ImportCACerts.cmd`

   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.

4. Following the prompts, enter Y (not case-sensitive) for any certificate you want to import.
5. For each certificate accepted, accept the suggested Certificate Name or edit it based on your file naming conventions.
6. 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.

   Tip: 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.

7. 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

To edit a CA certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
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

To delete a CA certificate:

1. From **Administration Menu**, select **Trading Partner > Digital Certificates > CA**.
2. Next to **Alphabetically**, click **Go!**
3. Next to the CA certificate you want to delete, click **delete**.

Search for System Certificates

To search for a system certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > System.**
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 in Sterling Integrator

To edit a system certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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 Integrator

To identify a system certificate:

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 (for example, receiving AS2 data from trading partners), you must monitor the expiration dates of the system certificates to ensure the certificates are valid.

To check the expiration date of a system certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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 Integrator

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

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 Integrator

Export a copy of the system certificate to your local disk before you delete it. The OpsDrv, OpsKey, doccrypto, ASISslCert, B2BHttp, DefDBCrypt, and UIKeys are system certificates that should never be deleted.

To delete a system certificate:

1. From **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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. The following procedure exports only the public certificate, not the private key, and provides you with a public certificate to send to a trading partner.

To check out a system certificate:

1. From **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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 Windows 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 Windows should open the file.
7. Click **Close** In the Check Out System Certificate dialog box.

   The System Certificate page is displayed.

Search for Trusted Certificates

To search for a trusted certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
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

Trusted certificates may 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:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
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

To edit a trusted certificate:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
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

To delete a trusted system certificate:

1. From **Administration Menu**, select **Trading Partner > Digital Certificates > Trusted**.
2. Next to **Alphabetically**, click **Go!**
3. Next to the trusted certificate you want to delete, click **delete**.

Import PKCS12 System Certificates

To import a PKCS12 system certificate:

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

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:

1. From the **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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

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

To import a pem system certificate:

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

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

Import Key System Certificates

To import a key system certificate:

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

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

Import Keystore System Certificates

To generate a keystore system certificate on an HSM:

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

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

Check In Key System Certificates

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

To check in a key system certificate:

1. From **Administration Menu**, select **Trading Partner > Digital Certificates > System**.
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**.

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 Integrator

The Certicom Government Service Edition (GSE) is a FIPS 140-2 Level 1 certified cryptographic module distributed with Sterling Integrator. GSE is a low-level cryptographic tool kit written in Java that implements a variety of 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.
- Funnels 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 the you install Sterling Integrator.

Before you begin, you should verify that you have a license for operating in FIPS mode before it is enabled. The will check your license at start up and will not start if FIPS mode is enabled but not licensed.

To manually enable FIPS mode:

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 the server. This is necessary for the changes to be recognized in the system.

Disable FIPS Mode

To manually disable FIPS mode:

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 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

To configure an HTTP proxy server:

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

To configure an SSP proxy server:

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

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

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

Edit Proxy Servers

To edit a proxy server configuration:

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

Deleting a proxy server configuration may cause errors in some features of Sterling 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:

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

SSL

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

The SSL protocol provides server authentication and client authentication:

- 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:

- 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 the SSL protocol, 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 Certificate Wizard to generate a CSR and get a certificate from a CA

Cipher Strength Settings

To implement a cipher strength setting, contact Customer Support.

Earlier Versions of SSL

To enable an earlier version of SSL, contact Customer Support.

Client Adapters for SSL

The following client adapters support SSL:

- FTP Client adapter
- HTTP Client adapter
- Connect:Direct 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

The following server adapters support SSL:

- FTP Server adapter
- HTTP Server adapter
- 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.

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 Integrator. To create a self-signed certificate:

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 Integrator as a CA certificate by selecting **Trading Partners** > **Digital Certificates** > **CA** > **Check In New Certificate**.

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 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 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.

Disable SSL Empty Records for CBC-Mode Cipher Suite

If you selected the CBC-mode cipher suite, and SSL does not work, disable SSL Empty Records:

1. Edit the tmp.sh file.
2. Find the server flag for the OS you are configuring and add:

   ```
   -DDisableSSLEmptyRecords=true
   ```

Copyright

Additional copyright information is located on the Sterling Integrator 5.0 Documentation Library:

http://www.ibm.com/support/docview.wss?uid=swg27023835