Sterling Commerce

Role-Based Security

Platform IFC 1.0

Sterling Commerce
An IBM Company

Contents

Managing Role-Based Security

The application requires system passwords for administrative functions and uses role-based security to provide different levels of access to different users within the organization.

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

A *user account* contains the groups the user belongs to, the permissions associated with each group or user, and the password policy applied to the user. *Groups* are collections of permissions and other groups that are required by a user for access to different modules. *Permissions* provide access to the different modules within the application and are the foundation of role-based security. *Password policies* are sets of security decisions that you make and apply to different user accounts according to security policies in your company.

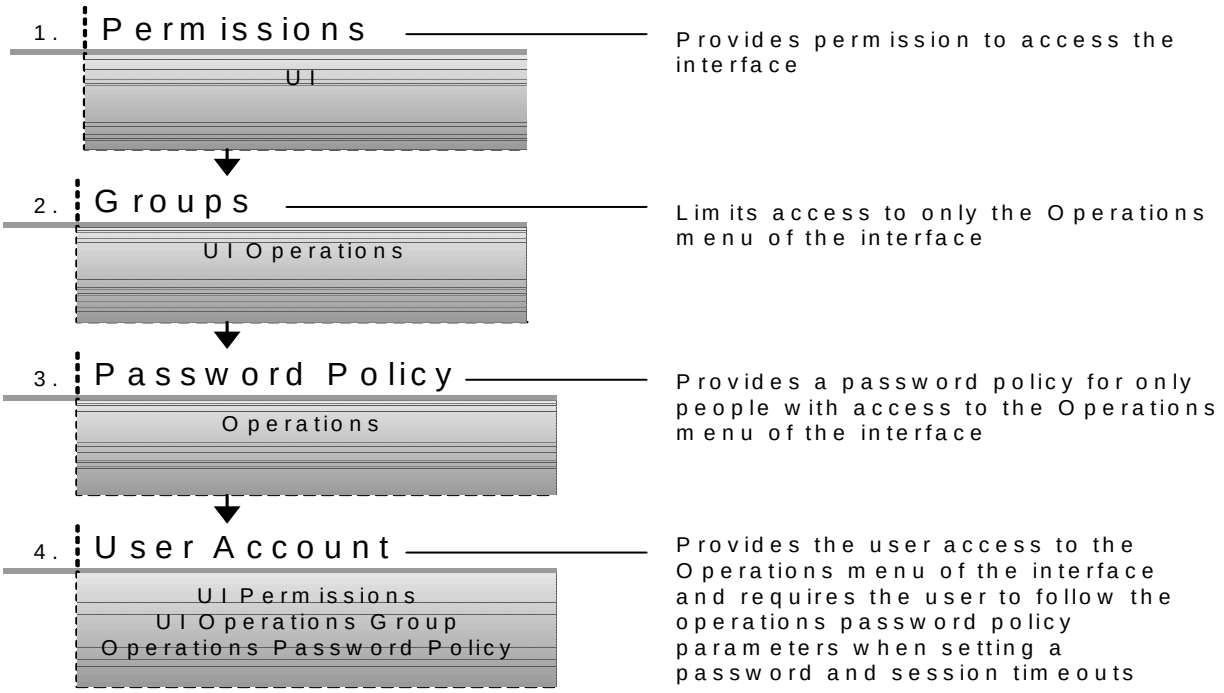
The user account is linked to the application user name and password. Each time you log in, the application verifies you as a valid user and grants access to only the areas you are allowed to use according to the permissions assigned to you by the application system administrator.

Role-based security also helps direct messages and documents to the appropriate user within the application Web Extensions. In this circumstance, the Web Extensions Human Interaction Event service pulls the approving authority's name and address from the application database and routes the document to that person. This routing feature helps you manage message queues.

Managing role-base security includes the following sequential tasks to create user accounts and assign permissions:

1. Creating permissions according to the modules the users require access to.
2. Creating groups according to the permissions you created.
3. Creating a password policy to assign to user.
4. Creating the user account using the permissions, groups, and password policy you created.

The following figure shows the relationships between permissions, groups, password policies, and user accounts:



Role-Based Security Example

Tom, the application system administrator, creates a user account for Joe, an employee at ABC Company. Tom sends Joe a unique user name and password to access the application.

User	User Name	Password
Joe	Joe_Employee	employee

Joe logs in to the application using Joe_Employee (user name) and employee (password) and is verified as a valid user. Joe works in Finance and is given access to only those parts of the application that he needs to complete his job of receiving and viewing expense reports from other employees in the company. Each user can have different permissions and group associations, which allows for great flexibility in providing secure access to the application.

The following table lists Joe's user account settings:

User Account	Value	Description
Identity	ABC Company	User's company name
Password	employee	User's password

User Account	Value	Description
Manager ID	Janet_Manager	User's manager
Groups	Accounts Admin	Groups the user belongs to
First Name	Joe	User's first name
Last Name	employee	User's last name
Email	joe.employee@abc.com	User's e-mail address
Pager	555-555-5555	User's pager number

The following table lists Joe's permission settings:

Permission	Value	Description
Session Timeout	60	Length of time in minutes before the session times out.
Web Suite Confirm Send Template	Active	Access to the Web Suite Confirm Send template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Draft Save Business Process	Active	Access to the Web Suite Draft Save Business Process template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Email Notification Business Process	Active	Access to the Web Suite E-mail Notification Business Process template is enabled. If Joe were not allowed access to the template, this would be be inactive.
Web Suite Email Notification Template	Active	Access to the Web Suite Email Notification template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Expense Report View Template	Active	Access to the Web Suite Expense Report View template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Load Business Process	Active	Access to the Web Suite Load Business Process template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Menu Business Process	Active	Access to the Web Suite Menu Business Process template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Query Business Process	Active	Access to the Web Suite Query Business Process template is enabled. If Joe were not allowed access to the template, this would be inactive.
Web Suite Query List Template	Active	Access to the Web Suite Query List template is enabled. If Joe were not allowed access to the template, this would be inactive.

Managing Permissions

Permissions provide access to the different modules within the application and are the foundation of role-based security.

Use Permissions to:

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

Managing permissions includes the following tasks:

- Creating a permission
- Searching for a permission
- Editing a permission name
- Deleting a permission

Before you create, edit, or delete a permission, decide which the application 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.

Use the following table to assign permissions needed for common functions:

UI Resource	**Permission ID**	**Permission Name**
BusinessProcess	BPMANAGE	UI BP Manager
Manager	BPMANAGE	UI BP Manager
CurrentProcesses	BPMONITOR	UI BP Monitor
CurrentDocuments	BPMONITOR	UI BP Monitor
CurrentActivities	BPMONITOR	UI BP Monitor
CentralSearch	BPMONITOR	UI BP Monitor
Manager	BP_DELETE	UI Delete BP
AdvancedSearch	BPMONITOR	UI BP Monitor
BusinessProcess	BPMONITOR	UI BP Monitor
DataFlows	BPMONITOR	UI BP Monitor
Documents	BPMONITOR	UI BP Monitor
ComSessFlows	BPMONITOR	UI BP Monitor
Correlation	BPMONITOR	UI BP Monitor
BPSSCorrelation	BPMONITOR	UI BP Monitor

ebXMLCorrelation	BPMONITOR	UI BP Monitor
EDICorrelation	BPMONITOR	UI BP Monitor
EDIINT	BPMONITOR	UI BP Monitor
GENTRANServerforUNIX	BPMONITOR	UI BP Monitor
SWIFTNetDocumentTracking	BPMONITOR	UI BP Monitor
TradingPartners		
BasicSetup	BASIC_SETUP	UI Basic Trading Profile Setup
AS2Setup	AS2_SETUP	UI AS2 Trading Profile Setup
Advanced	ADVANCED_SETUP	UI Advanced Trading Profile Setup
Identities	ADVANCED_SETUP	UI Advanced Trading Profile Setup
Transports	ADVANCED_SETUP	UI Advanced Trading Profile Setup
DocumentExchanges	ADVANCED_SETUP	UI Advanced Trading Profile Setup
Delivery Channels	ADVANCED_SETUP	UI Advanced Trading Profile Setup
Packaging	ADVANCED_SETUP	UI Advanced Trading Profile Setup
Profiles	ADVANCED_SETUP	UI Advanced Trading Profile Setup
DigitalCertificates		
CA	CA_CERTS	UI CA Certs
Trusted	TRUSTED_CERTS	UI Trusted Certs
System	SYSTEM_CERTS	UI System Certs
DocumentEnvelopes	ENVELOPES	UI Envelopes
Envelopes	ENVELOPES	UI Envelopes
ControlNumbers	ENVELOPES	UI Envelopes
TransactionRegister	ENVELOPES	UI Envelopes
ControlNumberHistory	ENVELOPES	
EDISequenceCheckQueue	ENVELOPES	UI Envelopes
Contracts	CONTRACTS	UI Contracts
CodeLists	CODELISTS	UI Codelists

SSH	SSH	UI SSH
SFTPAccount	SSH	UI SSH
RemoteHostKey	SSH	UI SSH
LocalUserKey	SSH	UI SSH
RemoteUserKey	SSH	
Deployment		
Services	SERVICES	UI Services
Installation	SERVICES	UI Services
Configuration>	SERVICES	UI Services
Schedules	SCHEDULER	UI Services
Maps	MAPS	UI Maps
Ext Rule Libraries	MAPS	UI Maps
XSLT	XSLT	UI XSLT
WebExtensions	WEB_EXTENSIONS	UI Web Extensions
WebTemplates	WEB_EXTENSIONS	UI Web Extensions
WebResources	WEB_EXTENSIONS	UI Web Extensions
Utilities	WEB_EXTENSIONS	UI Web Extensions
Schemas	SCHEMAS	UI Schemas
Mailboxes	MAILBOX	UI Mailbox
Configuration	MAILBOX	UI Mailbox
VirtualRoots	MAILBOX	UI Mailbox
RoutingRules	MAILBOX	UI Mailbox
Messages	MAILBOX	UI Mailbox
Ebxml	EBXML	UI EBXML
BPSS	EBXML	UI EBXML
BPSSExt	EBXML	UI EBXML
CPA	EBXML	UI EBXML

ResourceManager		
ResourceTags	DEPLOYMENT	UI Deployment
ImportExport	IMPORT_EXPORT	UI Import/Export
AdapterUtilities		
SapSuite	ADAPTER_UTILITIES	UI Adapter Utilities
SapRoutes	ADAPTER_UTILITIES	UI Adapter Utilities
SapRoute	ADAPTER_UTILITIES	UI Adapter Utilities
SapRouteXRef	ADAPTER_UTILITIES	UI Adapter Utilities
SyncEngine	ADAPTER_UTILITIES	UI Adapter Utilities
TradingPartners	ADAPTER_UTILITIES	UI Adapter Utilities
DataPoolProfile	ADAPTER_UTILITIES	UI Adapter Utilities
BEATuxedo	ADAPTER_UTILITIES	UI Adapter Utilities
ServiceSDK	ADAPTER_UTILITIES	UI Adapter Utilities
PGP	ADAPTER_UTILITIES	UI Adapter Utilities
SWIFTNetRoutingRule	SWIFTNET_ROUTING_RULE	UI SWIFTNet Routing Rule
LocalHostKey	SSH_LCL_ID_KEY	UI SSH Local Identity Key
Web Services	WEB_SERVICES	UI Web Services
Manager	WEB_SERVICES	UI Web Services
SchemaMappings	WEB_SERVICES	UI Web Services
WSDL	WEB_SERVICES	UI Web Services
Security Token	WEB_SERVICES	UI Web Services
Operations		(perm field empty)
System		(perm field empty)
Troubleshooter	OPERATIONS	UI Operations
Performance	OPERATIONS	UI Operations
Tuning	OPERATIONS	UI Operations

Statistics	OPERATIONS	UI Operations
JVM monitor	OPERATIONS	UI Operations
Support Tools		
SQL Manager	SQLMANAGER	UI SQL Tool
Support Case	SUPPORT_CASE	UI Support Case Tool
Logs	SYSTEM_LOGS	UI Logs
Licenses	LICENSES	UI Licenses
Cluster	CLUSTER	tbd
Node Status	CLUSTER	tbd
Reports	REPORTS	UI Reports
ThreadMonitor	OPERATIONS	UI Operations
JDBCMonitor	OPERATIONS	UI Operations
ArchiveManager	ARCHIVE-UI	UI Archive
LockManager	LOCK_MANAGER	UI Lock Manager
MessageMonitor	OPERATIONS	UI Operations
Accounts		
Groups	GROUPS	UI Groups
Permissions	ACCOUNTS	UI Accounts
UserAccounts	USER_ACCOUNTS	UI User Accounts
PwdPolicy	ACCOUNTS	UI Accounts
UserNews	ACCOUNTS	UI Accounts
MyAccount	none	(perm field empty)

Creating a Permission

When you create a permission, you set access to a module that can be assigned to different users.

To create a permission:

1. From the **Accounts** menu, select **Permissions**.

   The Permissions page opens.
2. In the Create section, next to Create a new Permission, click **Go!**

3. In the Permissions page, complete the following fields and click **Next**.

Caution: The permission ID must match exactly 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.

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 Name	Name of the permission you are creating. Required.
Permission Type	Permission type of the permission you are creating. Required. Permission types include: ◆ UI – Allows access to specific menu items in the interface. ◆ 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. ◆ Other – Allows access to resources that are not identified by one of the preceding types.
Note: If you upgrade from a previous version of the application, the existing permissions are set to Other by default. You may need to edit each permission to apply a new permission type.	

4. In the Confirm page, review the permission settings, and click **Finish** to save the new permission.

You can now edit permission names, delete permissions, and assign users to them.

Searching for a Permission

After you create a permission, you can search for that permission to edit the permission or review the permission for deletion.

To search for a permission:

1. From the **Accounts** menu, select **Permissions**.
2. In the Permissions page, complete one of the following actions:
   - Under Search in the **Permission Name** field, type either a portion of the name or the entire name of the permission you are searching for, and click **Go!** The Permissions page opens, listing all of the permissions 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 permission you are searching for. Selecting ALL lists all of the permission in the application. Click **Go!** The Permissions page opens, listing all of the permissions that match your search criteria.

3. Depending on your task, complete one of the following actions:
   - To change the permission settings, click **edit**. For more information, see *Editing a Permission Name* on page 14.
   - To delete the permission from the application, click **delete**. For more information, see *Deleting a Permission* on page 14.

Editing a Permission Name

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 **Accounts** menu, select **Permissions**.
2. In the Permissions page, locate the permission you want to edit by using either the Search or List options.
3. In the Permissions page, next to the permission you want to edit, click **edit**.
4. In the Permissions page, type a new permission name, make any changes to the permission type, and click **Next**.
5. In the Confirm page, review the change and click **Finish** to save the edited permission.

Deleting a Permission

As you define permissions, you may find that some are more generic and no longer useful. Others may not have any users assigned. Deleting unused permissions simplifies the accounts management function.

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.

Caution: Do not remove the application Admin group from the administrator user in the Accounts wizard, or the UI Accounts permissions in the Groups wizard. If you do, the system administrator will no longer be able to administer the application, including not being able to modify the administrator’s own permissions.

Caution: If you make either of these changes unintentionally, contact Sterling Commerce Customer Support to obtain a script that restores the default administrator rights.

To delete a permission:

1. From the **Accounts** menu, select **Permissions**.
2. In the Permissions page, locate the permission you want to delete by using either the Search or List options.
3. In the Permissions page, in the Select section next to the permission you want to delete, click **delete**.

4. In the Confirm page, verify that the permission information matches the permission you want to delete, and click **Delete** to delete the permission.

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

Managing Groups

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.

Before you create, edit, or delete a permission group, decide which the application 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 groups.

Caution: Do not remove the application Admin group from the administrator user in the Accounts wizard, or the UI Accounts permissions in the Groups wizard. If you do, the system administrator will no longer be able to administer the application, including not being able to modify the administrator's own permissions.

Caution: If you make either of these changes unintentionally, contact Sterling Commerce Customer Support to obtain a script that restores the default administrator rights.

Managing groups includes the following tasks:

- ✦ Creating a group
- ✦ Searching for a group
- ✦ Editing a group
- ✦ Deleting a group

Creating a Group

When you create a group, you set multiple permissions for users that perform the same job.

To create a group:

1. From the **Accounts** menu, select **Groups**.

   The Groups page opens.
2. Under Create, next to Create a new Group, click **Go!**
3. In the New Group page, complete the following fields and click **Next**.

Field	Description
Group ID	Group ID for the group you are creating. Required.

Field	Description
Group Name	Group name of the group you are creating. Required.
Owner	Name of the owner for the group. The group owner has two primary roles: ◆ Administrative contact for the group when changes to the group are needed. The owner contacts the system administrator to request changes. ◆ Routing device. For example, if a group is created for a development department and all development department employees send time sheets using the application, the Owner field can be used to route all of the time sheets to the departmental manager.
Identity	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. Select a trading partner identity from the list.

4. In the Assign Subgroups page, do you want to filter groups by name?
   - If Yes, under Filter Data in the **By Name** field, type either a portion of the name or the entire name of the group you want to filter for and click the filter button to the right of the field.
   - If No, go to step 5.
5. In the Assign Subgroups page in the Available pane, select the group or groups you want to assign to this group.
6. Complete one of the following actions and click **Next**.
   - Click the right double-arrow to move all groups from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected groups to the Assigned pane.
   - Click the left double-arrow to move all groups from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected groups to the Available pane.
7. In the Assign Permissions page, do you want to filter permissions?
   - To filter by name, under Filter Data in the **By Name** field, type either 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. The following table describes the permission types:

Permission Type	Description
UI	Allows access to specific menu items in the interface.
Mailbox	Allows access to specific mailboxes in the application.
Template	Allows access to specific Web templates.

Permission Type	Description
BP	Allows access to specific business processes.
Other	Allows access to resources that are not identified by one of the preceding types. **Note:** If you upgrade from a previous version of the application, the existing permissions are set to Other by default. This is because permission type was not available in releases before the application 3.0.

- If you do not want to filter permissions, go to step 8.

8. In the Assign Permissions page in the Available pane, select the permission or permissions you want to assign to this group.
9. Complete one of the following actions and click **Next**.
   - Click the right double-arrow to move all permissions from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected permissions to the Assigned pane.
   - Click the left double-arrow to move all permissions from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected permissions to the Available 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; the associated permissions display in the confirm page.
10. In the Confirm page, review the permission settings, and click **Finish** to save the new group.

Searching for a Group

After you create a group, you can search for that group to edit it or review the group for deletion.

To search for a group:

1. From the **Accounts** menu, select **Groups**.
2. In the Groups page, complete one of the following actions:
   - Under Search in the **Group Name** field, type either a portion of the name or the entire name of the group you are searching for, and click **Go!** The Groups page opens, listing all of the groups 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 group you are searching for. Selecting ALL lists all of the groups in the application. Click **Go!** The Groups page opens, listing all of the groups that match your search criteria.
3. Depending on your task, complete one of the following actions:
   - To change the group settings, click **edit**. For more information, see *Editing a Group* on page 19.
   - To delete the group from the application, click **delete**. For more information, see *Deleting a Group* on page 20.

Editing a Group

When you edit a group, you change access permissions for the users assigned to that group. For example, users may need additional permissions assigned if the scope of responsibility changes.

To edit a group:

1. From the **Accounts** menu, select **Groups**.
2. In the Groups page, locate the group you want to edit by using either the Search or List option.
3. Click **edit** next to the group you want to edit.
4. Type a new group name for the group you are editing, make any changes to the **Owner** and **Identity** fields, and click **Next**.
5. In the Assign Subgroups page, do you want to filter groups by name?
   - If Yes, under Filter Data in the **By Name** field, type either a portion of the name or the entire name of the group you want to filter for and click the filter button to the right of the field.
   - If No, go to step 6.
6. In the Assign Subgroups page in the Available pane, select the group or groups you want to assign to this group.
7. Complete one of the following actions and click **Next**.
   - Click the right double-arrow to move all groups from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected groups to the Assigned pane.
   - Click the left double-arrow to move all groups from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected groups to the Available pane.
8. In the Assign Permissions page, do you want to filter permissions?
   - To filter by name, under Filter Data in the **By Name** field, type either 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. The following table describes the permission types:

Permission Type	Description
UI	Allows access to specific menu items in the interface.
Mailbox	Allows access to specific mailboxes in the application.
Template	Allows access to specific Web templates.
BP	Allows access to specific business processes.

Permission Type	Description
Other	Allows access to resources that are not identified by one of the preceding types. **Note:** If you upgrade from a previous version of the application, the existing permissions are set to **Other** by default. This is because permission type was not available in releases before the application 3.0.

- If you do not want to filter permissions, go to step 9.

9. In the Assign Permissions page in the Available pane, select the permission or permissions you want to assign to this group.
10. Complete one of the following actions and click **Next**.
    - Click the right double-arrow to move all permissions from the Available pane to the Assigned pane.
    - Click the right single-arrow to move selected permissions to the Assigned pane.
    - Click the left double-arrow to move all groups from the Assigned pane to the Available pane.
    - Click the left single-arrow to move selected groups to the Available pane.
11. In the Confirm page, review the changes you made to the group, and click **Finish** to save the edited or new group.

Deleting a Group

As you define groups, you may find that some are more generic and no longer useful. Others may not have any users assigned. Deleting unused groups simplifies the accounts management function.

Caution: Do not remove the application Admin group from the administrator user in the Accounts wizard, or the UI Accounts permissions in the Groups wizard. If you do, the system administrator will no longer be able to administer the application, including not being able to modify the administrator's own permissions.

Caution: If you make either of these changes unintentionally, contact Sterling Commerce Customer Support to obtain a script that restores the default administrator rights.

To delete a group:

1. From the **Accounts** menu, select **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*.

Managing 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.

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.

The default password policy includes the following values:

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

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, however, log in using any other computer that has access to the application.

To unlock the user account, you must do one of the following:

- Wait 30 minutes and the lock expires allowing you to try to log in 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 again.

You can set this lock out number to any value that you want in the ui.properties.in file in the *install_dir*/install/properties directory. For more information, see *Editing the Lock Out Parameter* on page 24.

Managing password policies includes the following tasks:

- Creating a password policy
- Searching for a password policy
- Editing a password policy
- Deleting a password policy
- Editing the lock out parameter
- Editing the password expires message value

Creating a Password Policy

You create a password policy to assign the policy to user accounts. This streamlines your security operations when adding new users. You do not need to associate a password policy with a user account, but it does help in managing your security. A user account cannot have more than one password policy associated with it.

For more information about password policies and the default password policy, see *Managing Password Policies* on page 21.

To create a password policy:

1. From the **Accounts** menu, select **Password Policy**.
2. In the Password Policy page, next to Create a new Password Policy, click **Go!**
3. In the Password Policy page, complete the following fields and click **Next**.

Field	Description
Policy ID	ID that identifies the password policy in the database.
Policy Name	User-friendly name that displays in the user interface when any reference is made to the password policy.

Field	Description
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 5.
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.

4. In the Confirm page, review the password policy settings, and click **Finish**.

You can now edit and delete password policies, and assign password policies to user accounts.

Searching for Password Policies

To search for a password policy:

1. From the **Accounts** page, select **Password Policy**.
2. In the Password Policy page, complete one of the following actions:
   - Under Search in the **Password Policy Name** field, type either a portion of the name or the entire name of the password policy you are searching for, and click **Go!** The Password Policy page opens, listing all of the password policies 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 password policy for which you are searching. Selecting ALL lists all of the password policies in the application. Click **Go!** The Password Policy page opens listing all of the permissions that match your search criteria.
3. Depending on your task, complete one of the following actions:
   - To change the password policy, click **edit**. For more information, *Editing a Password Policy* on page 24.
   - To delete the password policy from the application, click **delete**. For more information, *Deleting a Password Policy* on page 24.

Editing a Password Policy

To edit the password policy:

1. From the **Accounts** menu, select **Password Policy**.
2. In the Password Policy page, locate the password policy you want to edit by using either the Search or List options.
3. In the Password Policy page, next to the password policy you want to edit, click **edit**.
4. In the Password Policy Settings page, make the appropriate changes, and click **Next**.
5. In the Confirm page, review the password policy settings, and click **Finish** to save your changes.

The application saves the edited password policy settings and displays the message, *The system update has completed successfully*.

Deleting a Password Policy

Note: 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 **Accounts** menu, select **Password Policy**.
2. In the Password Policy page, locate the password policy you want to delete by using either the Search or List options.
3. In the Password Policy page, next to the password policy you want to delete, click **delete**.
4. In the Confirm page, click **Delete** to delete this password policy.

Editing the Lock Out Parameter

The lock out parameter is the setting for how many consecutive times you can attempt to log in before being locked out of further log in attempts on a specific computer. You have the following options after being locked out. 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.

You can set this lock out number to any value that you want in the ui.properties.in file in the *install_dir*/install/properties directory.

Note: 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 only, and if you shut down and restart the application, the changes you made to the ui.properties file are overwritten by the ui.properties.in file.

To change the lock out parameter:

1. Stop the application.
2. In the *install_dir*/install/properties directory, locate ui.properties.in.
3. In a text editor, open ui.properties.in.
4. Locate the **ConseFailedAttempts= 0** entry.
5. Highlight and change the 0 to the new number of log in attempts.
6. Save the ui.properties.in file under the same name in the same location.
7. In the *install_dir*/install/bin directory run the **setupfiles** script.
8. 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.

Editing the Password Expires Message Value

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.

Caution: 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 only, and if you shut down and restart the application, the changes you made to the ui.properties file are overwritten by the ui.properties.in file.

To change the password expires message value:

1. Stop the application.
2. In the *install_dir*/install/properties directory, locate ui.properties.in.
3. In a text editor, open ui.properties.in
4. Locate the **MsgPwdExpires= 15** entry.
5. Highlight and change the 15 to the new number of days.
6. Save the ui.properties.in file under the same name in the same location.
7. In the *install_dir*/install/bin directory run the **setupfiles** script.
8. 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.

Managing User Accounts

Note: In the Admin user account, change the initial password from installation to a different password to secure the Admin user account.

User accounts work with permissions to provide security for the application and your organization. These features make it possible to regulate which users have access to each module in the application and what functions each user is to perform. Removing a user account prevents a specific person from accessing the application.

You must be assigned permission to the Accounts module to create user accounts.If you skip a required field, a message prompts you to supply the missing information.

Managing user accounts includes the following tasks:

- Creating a user account
- Searching for a user account
- Editing a user account
- Deleting a user account

Creating a User Account

When you create a user account, you specify a login ID and password, permissions, and contact information for a specific user.

If you are creating an external user, you can specify an alternative authentication method (generally LDAP). You must do the following before creating an external user account:

1. Stop the application.
2. Specify the alternative authentication method by adding or modifying an authentication configuration in the authentication_policy.properties.in file. The properties need to follow this format: authentication_4.xxx=xxx_value.
3. Run setupfiles.sh.
4. Start the application.

To create a user account:

1. From the **Accounts** menu, select **User Accounts**.

   The User Accounts page opens with the Select section listing all existing user accounts.
2. In the Create section, next to Create a new Account, click **Go!**
3. In the New Account page, select the type of authentication for the user:
   - Local – Authentication is completed against the application database.
   - External – Authentication is completed against an LDAP server. External authentication does not require the application 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).

Note: 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 database. To create an external user account, you must have the application license for single sign on or LDAP.

4. Complete the following fields and click **Next**.

Field	Description
User ID	User ID for the user account you are creating. The user ID must be at least five characters long. Required. **Note:** For only the MySQL database, 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 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 only)	Type the password a second time. Required for local users. This field does not display for external users.
Policy (Local 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. For more information about password policies, see *Managing Password Policies* on page 21. **Note:** The expiration date is calculated by the application from the first date that the user logs on with this password.
Authentication Host (External only)	The Lightweight Directory Access Protocal (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.
SSH Authorized User Key (Sterling Integrator Only)	Public key used to authenticate remote users. Obtain this key from your trading partner. Key must be checked in prior to creating the user account, then select the correct one from the list.
Session Timeout	Amount of time that you cannot interact with 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 – Access to only the Admin Console pane in the application dashboard. ◆ AS2 UI – Access to only the AS2 Edition interface. ◆ Dashboard UI – Access to dashboard interface. You refine this choice by choosing a dashboard theme below.

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: ◆ Operator ◆ Participant ◆ Participant Sponsor ◆ Sponsor

5. In the Groups page, complete one of the following actions and click **Next**.

   If you selected the AS2 UI as the accessibility option, all groups and permissions associated with the specific UI are automatically assigned. Proceed to step 6.

   - Click the right double-arrow to move *all* groups from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected groups from the Available pane to the Assigned pane.
   - Click the left double-arrow to move *all* groups from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected groups from the Assigned pane to the Available pane.

6. In the Permissions page, complete one of the following actions and click **Next**.

   - Click the right double-arrow to move *all* permissions from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected permissions from the Available pane to the Assigned pane.
   - Click the left double-arrow to move *all* permissions from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected permissions from the Assigned pane to the Available pane.

   By default, the permissions associated with the groups this user is assigned to are already selected. You can assign to the user permissions not associated with a group.

7. In the User Information page, complete the following fields and click **Next**.

Field	Description
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. English or Japanese.
Manager ID	ID of the user's manager.

Field	Description
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**.

8. In the Confirm page, review the user account settings, and click **Finish** to create the user account.

   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 application, and then log back in with the external user ID or account. The application will authenticate the external user ID on the external LDAP server.

Searching for a User Account

To search for a user account:

1. From the **Accounts** menu, select **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 opens, listing all of the user accounts 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 user account you are searching for. Selecting ALL lists all of the user accounts in the application. Click **Go!** The Accounts page opens, listing all of the user accounts that match your search criteria.
3. Depending on your task, complete one of the following actions:
   - To change the user accounts settings, click **edit**. For more information, see *Editing a User Account* on page 29.
   - To delete the group from the application, click **delete**. For more information, see *Deleting a User Account* on page 31.

Editing a User Account

To edit a user account:

1. From the **Accounts** menu, select **User Accounts**.
2. Locate the user account you want to edit by using either the Search or List options.
3. In the Select section next to the user account you want to edit, click **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** field.
6. Make any changes to the **Policy ID** field.
7. Make any changes to the **Session Timeout** field and click **Next**.
8. Make the appropriate changes by completing one of the following actions and clicking **Next**.

   If you selected the AS2 UI as the accessibility option, all groups and permissions associated with the specific UI are automatically assigned. Proceed to step 8.

   - Click the right double-arrow to move *all* groups from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected groups from the Available pane to the Assigned pane.
   - Click the left double-arrow to move *all* groups from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected groups from the Assigned pane to the Available pane.
9. Make the appropriate changes by completing one of the following actions and clicking **Next**.
   - Click the right double-arrow to move *all* permissions from the Available pane to the Assigned pane.
   - Click the right single-arrow to move selected permissions from the Available pane to the Assigned pane.
   - Click the left double-arrow to move *all* permissions from the Assigned pane to the Available pane.
   - Click the left single-arrow to move selected permissions from the Assigned pane to the Available pane.

   By default, the permissions associated with the groups this user is assigned to are already selected. You can assign to the user permissions not associated with a group.
10. Make the appropriate changes to the following fields and click **Next**.

Field	Description
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. English or Japanese.
Manager ID	ID of the user's manager.

Field	Description
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.

11. Review the user account settings, and click **Finish** to create the user account.

    The application creates the user account and displays the message. *The system update completed successfully*.

Deleting a User Account

You can delete a user account as needed to maintain the security of the application.

User accounts work with access permissions to provide security for the application and your organization. These features make it possible to regulate which users have access to each module in the application and which functions each user can perform.

To delete a user account:

1. From the **Accounts** menu, select **User Accounts**.
2. Locate the user account you want to delete by using either the Search or List options.
3. In the Select section next to the user account you want to delete, click **delete**.
4. Do you want to delete this user account?
   - If Yes, click **Delete**.

     The application deletes the selected user account and displays the message, *The system update completed successfully*.
   - If No, click **Cancel**.

   Note: To delete an Admin (super user) account, you must first remove the user account from the Admin group. Once you have removed the user from the Admin group, the delete option displays for the user account, and it can be deleted successfully.

Managing System Passwords

During installation, you create a system passphrase (highly complex string longer than 16 characters) and enter passwords for accessing your database. The system passphrase is required to start the system and to access protected system information. If you lose or forget your passphrase, you will not be able to start the system; therefore, it is recommended that you store your passphrase securely offline.

The system passphrase is not stored anywhere by the system by default, 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't 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.

Database passwords can be encrypted in the configuration files where they are stored.

Security Time Out

In addition to password protection, the application also uses a security time out feature 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. For more information about setting the session time out, see *Creating a User Account* on page 26.

Encrypting Database Passwords

A password is used by the application to connect to its database. The password is stored as clear text in a property file on the system. If the security policies at your company require you to encrypt these passwords, you can do so after you install the application. Encrypting these passwords is optional.

To encrypt the database password used by the application in UNIX, follow these steps:

1. Stop the application.
2. Run /*install_dir*/install/bin/enccfgs.sh.
3. Run /*install_dir*/install/bin/setupfiles.sh.
4. Run /*install_dir*/install/bin/deployer.sh.
5. Run run.sh to start the application.
6. Enter your passphrase.

To encrypt the database password used by the application in Windows, follow these steps:

1. Stop the application.
2. Run /*install_dir*/install/bin/enccfgs.cmd.
3. Run /*install_dir*/install/bin/setupfiles.cmd.
4. Run /*install_dir*/install/bin/deployer.cmd.
5. Run startWindowsService.cmd to start the application.

6. Enter your passphrase.

Changing a Password

To change a password after all passwords have been encrypted:

1. Clear the changes made to sandbox.cfg.
2. Repeat the previous procedure, specifying the new password.

Decrypting a Password (Windows)

To decrypt a password in Windows:

1. Run *install_dir*\install\bin\decrypt_string.cmd *encrypted_password.* Do not enter a space in the value for *encrypted_password*.

   You are prompted for the passphrase. This is the passphrase that you entered during installation.
2. Edit *install_dir*\properties\sandbox.cfg by replacing the encrypted password in the DB_PASS property with the password that was returned in step 1. Include the “ENCRYPTED:” string.
3. Run *install_dir*\install\bin\setupfiles.cmd.
4. Restart the application.

Decrypting a Password (UNIX)

To decrypt a password in UNIX:

1. Run *install_dir*/install/bin/decrypt_string.sh *encrypted_password*. Do not enter a space in the value for *encrypted_password*.

   You are prompted for the passphrase. You entered the passphrase during installation.
2. Edit *install_dir*/install/properties/sandbox.cfg to replace the encrypted password in the DB_PASS property with the password that was returned in step 1. Include the “ENCRYPTED:” string.
3. Run *install_dir*/install/bin/setupfiles.sh.
4. Restart the application.

Using Lightweight Directory Access Protocol (LDAP)

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.

Note: User 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).

User accounts in the application that are authenticated using LDAP are external user accounts, meaning they are authenticated outside of the application. User accounts that are not authenticated using LDAP are internal accounts, meaning that they are authenticated against the database of the application.

Note: 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.

Using LDAP In the application

Before you can use LDAP with the application, you must set up your user accounts that are authenticated against the LDAP server as external accounts. LDAP works with the application to authenticate you as you log in to the application.

The LDAP authentication process includes the following steps if you are using the password comparison mode:

1. You type 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 to the application.

The LDAP authentication process includes the following steps if you are using the LDAP binding mode:

1. You type 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's distinguished name (DN) from the LDAP directory.
5. The application attempts to bind to the LDAP repository using the user's DN and password.
6. Authentication is either:
   - Success – If the application binds to the LDAP repository as a user.
   - Failure – If the application cannot bind to the LDAP repository as a user.

LDAP Prerequisites

Before you can use LDAP with the application, you must have:

- Knowledge of LDAP.
- Access to an installed and configured LDAP server containing user information.
- The location of the LDAP server.
- Installed security certificates in the Keystore and Truststore, if you are using SSL.
- Created the application external user accounts for each user that will authenticate through your LDAP server. For more information, see *Creating a User Account* on page 26.
- The location of your Keystore and Truststore, if you are using SSL.

Editing the authentication_policy.properties.in File

To configure the application to use LDAP, you must edit the authentication_policy.properties.in file located in your *install_dir*/install/properties directory. You can also use the customer_overrides.properties file to set property values that will not be overwritten by a patch installation.

To edit the authentication_policy.properties.in file:

1. Stop the application.
2. In your *install_dir*/install/properties directory, locate the authentication_policy.properties.in file and open the file in a text editor.
3. In authentication_policy.properties.in, locate the ## GIS/LDAP Authentication configuration entry.

   The following example shows the GIS/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 authentication method. 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 proper LDAP 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 properties would be replaced if
# the customer already used LDAP authentication as configured in security.properties.
#
#########################################################################

#########################################################################
#
# LDAP Server <number> Authentication Configuration
#
#########################################################################
#
authentication_<number>.className=com.sterlingcommerce.woodstock.security.LDAPAuthen
tication
# authentication_<number>.display_name=LDAP Server agrona <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
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.
#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.

Parameter	Description	Shipped Value	Change to
#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.
#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 (sAMAccountName=<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.

4. Save the authentication_policy.properties.in file using the same name in the same directory.
5. Run *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.

6. Start the application.

   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.

7. In the System Logs page, 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.

Using Single Sign On

Single sign on (SSO) is an authentication process enabling a person accessing several applications to type only one user name and one password to access all applications that the person has permission to. Previously, a person logged in to each application individually and may have required several user names and passwords to manage. Single sign on solves this problem.

Note: (Sterling Integrator only) User 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).

The application allows SSO through integration with Netegrity SiteMinder and other applications.

Single sign on in the application is limited to the following components:

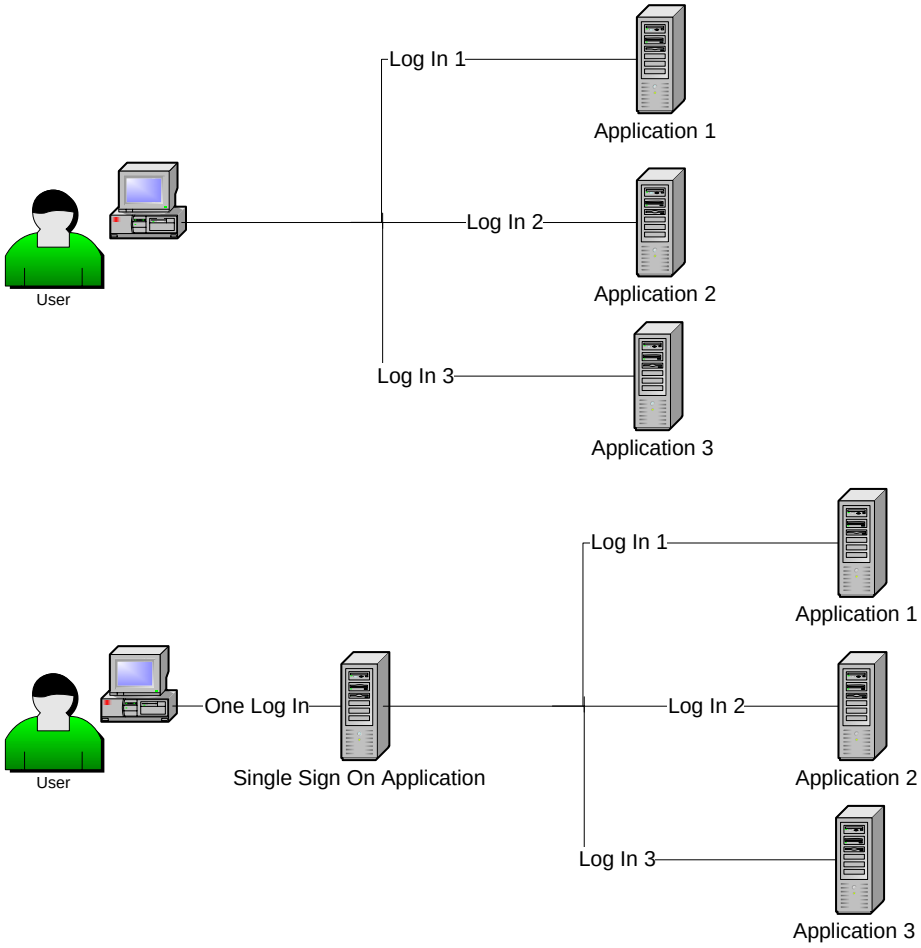
- Administration Interface
- Mailboxing Interface
- Dashboard Interface
- AFT Interface
- MyAFT Interface

Before Using Single Sign On

Before you can use single sign on with the application, you must have:

- Knowledge of SSO.
- Knowledge of Netegrity SiteMinder or your Single Sign On application.
- Netegrity SiteMinder installed and configured with a reverse proxy server.
- Edited the security.properties file in your *install_dir*/install/properties directory for the application to use single sign on.

The following figures show an authentication process without single sign on capability and an authentication process with single sign on capability:



Before you can use single sign on with the application, you must edit the security.properties file in your *install_dir*/install/properties directory for the application to use single sign.

To edit the security.properties file:

1. Stop the application.
2. In your *install_dir*/install/properties directory, locate the security.properties file and open the file in a text editor.
3. In security.properties, locate the ## SSO Authentication configuration entry.

   The following code sample shows the SSO Authentication configuration parameters:

```
## SSO Authentication configuration

## enable sso authentication  (true, false) default=false
SSO_AUTHENTICATION_ENABLED=true

## http header variable that contains externally authenticated userid
SSO_USER_HEADER=SM_USER
```

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

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

5. Save the security.properties file using the same name in the same directory.
6. Start the application.

The changes to the security.properties file are applied and you can now begin using SSO to authenticate users.

Netegrity Secure Proxy Server 1.1 Configuration

Before you can use Single-Sign On with the application, you must configure your secure proxy server to work with the application.

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

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

This document contains the following sections:

- ✦ Configuring the Netegrity Secure Proxy Server
- ✦ Configuring Netegrity Policy Server

Configuring the Netegrity Secure Proxy Server

To configure the Netegrity Secure Proxy Server:

1. Add the necessary forwarding rules for the application 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 the application 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 the application does not support Netegrity Cross Server Scripting policy enforcement.

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

3. Save the proxyrules.xml file in the same location and using the same file name to complete the configuration.

Configuring Netegrity Policy Server

For the application to work with Netegrity Secure Proxy Server, the Netegrity 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.

The following table describes the URL patterns that require secure realms:

URL Pattern	Enables Access To
/ws/*	Standard the application interface, using the http://host:port/ws format
/mbi/*	The application Mailbox interface
/dashboard/*	The application dashboard interface, using the http://host:port/dashboard format
/communitymanagement/*	The application community management interface through the dashboard interface
/datastore/*	Datastore components
/portlets/*	The 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

Editing My Account Information

The 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 as needed 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 edit your My Account information:

1. Select **Accounts > My Account**.
2. Do you want to change the account password?
   - If Yes, in the **Old Password** field, type your current password and type a new password in the **New Password** field. Type the new password again in the **Confirm New Password** field.
   - If No, go to step 3.
3. Type or select any changes in the appropriate fields.
4. Do you want to change the Welcome page, otherwise known as the application Admin Console Home page, from the default Standard page?
   - If Yes, from the list next to Welcome Page, select the page you want to display when you log in to the application. The following pages are available:

Page Name	Description
Standard (Default)	Displays system alerts, access to different tools and tips.
Troubleshoot	Displays the System Troubleshooting page, enabling you to view system and activities statuses, and turn on and off specific system components.
Service Config	Displays the Service Configuration page, enabling you to create new service configurations and search for existing service configurations.
BP Monitor	Displays the Business Process Monitor page, enabling you to view and monitor business process information in the application.

   - If No, select Standard from the list.
5. 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.
6. 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.
7. Do you want to reuse browser windows for pop-up displays?
   - If Yes, clear the check box next to Do not reuse windows for pop-up display.
   - If No, select the check box next to Do not reuse windows for pop-up display.

8. Do you want the application to remember the search-by values? This option saves the last value you typed in each of the Search fields.
   - If Yes, select the check box next to Remember search-by values.
   - If No, clear the check box next to Remember search-by values.
9. Click **Save**.

   The application saves the new account information and displays the message, *The system update completed successfully*.
10. Log out of the application and log back in to see the changes you made to your account.

Index

P

R

S

T

U