

Associated Connect[®]

Reference Guide: Premier Lockbox Security Administrator



Table of Contents

Associated Connect Access	3
Available Services	3
Sign-In and Security	3
Administrative Privileges	4
Assigning User ID Privileges	4
Maintaining User IDs	5
User ID Release	5
User ID Reporting	6
Audit Activity Report	7
Create a Group ID	7
Edit a Group ID	8
Assign a Group ID	8

Associated Connect Access

Associated Connect provides secure, single sign-on access to your business and commercial banking services through AssociatedBank.com/Business or AssociatedBank.com/Commercial.

Available Services

Once signed in, users can access a wide range of online banking functions:

Banking	Account Balances, ACH Origination Check Inquiry, Image Search, Positive Pay, Stop Payments, Transfers and Wire Transfers
Account Summary	View balances and transaction details
Cash Management	Bill Pay*, Cash Ordering, Checkview, FX Manager, Lockbox, Remote Deposit and Trade Services
Transmission and Reporting	Document Center, Export Tools and File Transfer

*Some services within the bill payment service have service charges. Please refer to the Business Fee Schedule or the applicable Checking Product Disclosure for details. (1276)

Sign-In and Security

Access to Associated Connect requires identity verification through one of two methods:

High-Risk Services	• Sign in with your username and password. • Verify identity using multi-factor authentication (MFA) with a unique access code from a mobile or physical token.
Low-Risk Services	• Sign in with your username and password. • Verify identity using a unique access code sent by text message (SMS) to your registered mobile number.

For help with tokens, see the Multi-Factor Authentication and Password Management Guide or contact Customer Care at 800-728-3501.

Associated Bank does not charge a fee to download our digital applications; however, transactional fees may apply. Carrier message and data rates may apply; check your carrier's plan for details. Visit AssociatedBank.com/disclosures for Terms and Conditions for your service. (1406)



Administrative Privileges

A Security Administrator is an individual user that has additional privileges regarding the security of a Company's users. Each Customer ID is required to have a minimum of two Security Administrators assigned, but three or more are strongly recommended.

Assigning User ID Privileges

Security Administrators are responsible for assigning User ID privileges (services, capabilities, accounts, etc.). To do this, once in the Premier Lockbox portal, select **Admin > Manage User Access** from the menu. Then, select the **Users** tab to bring up a list of users in the system to take action on. Click **Action** next to the user you wish to modify, then select **Modify Services**.

Manage User Access

Registration code: R

Activity **Users** User Groups

Action	User ID	User Name	Group	Status	Pending Action	Last Updated User
Action...	12345JohnDoe01	John Doe		Active		12345SUPERUSER
Action...	12345JohnDoe02	John Doe		Active		12345SUPERUSER
	12345JohnDoe03	John Doe		Active		12345SUPERUSER
Copy To	12345JohnDoe04	John Doe		Active		12345SUPERUSER
Modify Profile	12345JohnDoe05	John Doe		Active		12345SUPERUSER
Modify Services	12345JohnDoe06	John Doe		Active		12345SUPERUSER
Action...	12345JohnDoe07	John Doe		Active		12345SUPERUSER

A service list will be displayed with all services that can be entitled to the user. Find the service you want to entitle and select **Action**, then **Add** for the service you want to entitle. Depending on the service, a window will then appear allowing you to entitle that service to specific accounts or lockboxes. Once you have selected the proper options, click **Save**.

Modify User Services

Search

Action	Service	Status	Pending Action	Last Updated Date/Time
Actions ▾	AUTOMATED LOCKBOX	Entitled		Nov 14, 2020, 12:49:07 PM EST
Actions ▾	DIGITAL ARCHIVE	Not Entitled		
Add	EVENT MANAGER	Not Entitled		
	RELATED BANK SERVICES	Not Entitled		

All Security Administrator actions are dual-release and requires that a second Security Administrator approve the action before it will take effect in the system. See User ID Release selection for more

information on how to release an ID.

Maintaining User IDs

Security Administrators are responsible for assigning User ID privileges (services, capabilities, accounts, etc.). To do this, once in the Premier Lockbox portal, select **Admin > Manage User Access** from the menu. Then, select the **Users tab** to bring up a list of users in the system to take action on. Click **Action** next to the user you wish to modify, then select **Modify Services**. The following screen will display.

Modify User Services				
				Search
Action	Service	Status	Pending Action	Last Updated Date/Time
Actions ▼	AUTOMATED LOCKBOX	Entitled		Nov 14, 2020, 12:49:07 PM EST
Actions ▼	DIGITAL ARCHIVE	Entitled		Nov 15, 2020, 10:49:25 AM EST
Modify	EVENT MANAGER	Not Entitled		
Remove	RELATED BANK SERVICES	Not Entitled		

Select the **Actions** option next to the service you wish to modify. User ID Maintenance includes the following functions: **Modify** and **Remove**.

- **Modify:** To modify services currently entitled to the user.
- **Remove:** To remove access to a service the user is currently entitled to.

User ID Release

A second Security Administrator is required to approve all User ID maintenance requests. Once logged in the second administrator can click on the Task Central link that says Manage User Access, or can navigate to **Admin > Manage User Access**. Then in the **Activity** tab, for any pending change, select **Actions**, then **Release**. You can also select **View Changes** if you would like to see what permissions were changed before releasing.

Transactions Resources Communications Reporting Admin

Manage User Access

Registration code: Reports

Activity Users User Groups

Action	ID	Name	Type	Status	Pending Action	Last Updated User
Actions Reject Release View Changes	XXXXX	XXXXXXXXXXXX	User	Pending	Modify Service	XXXXX

User ID Reporting

User ID Reports allow the Lockbox Administrator to pull reports of users and groups within the company. The reports show current entitlement information for ID's as it currently exists in the system. The reports do not show any updates to ID's in a pending authorization status. Lockbox Admins can request a detailed report of entitlements for ID's within the company. All User ID's, all Group ID's, or a combined report may be requested. To request an ID Report from the Lockbox Premier module select **Admin > Manage User Access** from the menu. Next select the **Reports** button, and choose **ID**. This will open a selection window where you can choose the type of report you are looking for.

The Customer ID field will be pre-filled. The following report options are available:

- Summary or Detail Report Data
- Report Type (User, Group, or All)
- An Output Format:
 - Advanced provides a dynamic report with the ability to expand/collapse areas of the report
 - PDF provides a fully expanded version of the report in PDF format that you can save to your PC

Select **Generate** to produce the report.

Audit Activity Report

The Audit Activity Report provides Security Administrators with the ability to view All Users or an individual user's activity. This report can be requested for All Applications or select applications. The Start and End dates must be within 90 calendar days from the current date, and the Date Range cannot be greater than 14 calendar days at a time. If you want to view one specific day leave the End date field blank. To request an Audit Activity Report select **Admin > Audit** from the menu in the Lockbox Premier module.

Select the Report Format you want to view. There are two options available:

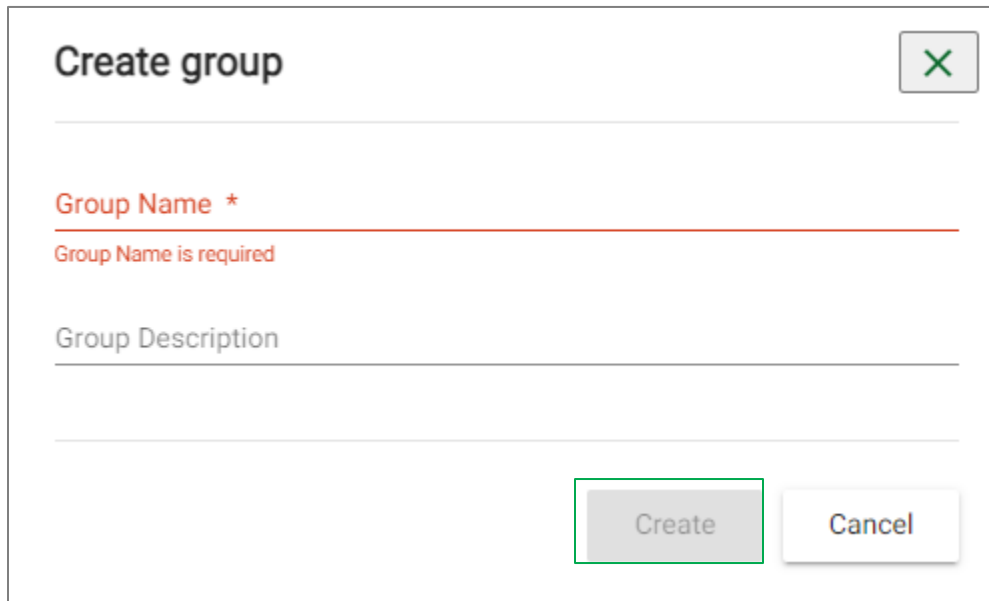
- **HTML:** This version has a toolbar button to view the report as a PDF, enabling the user to view the report in PDF format directly from the HTML output screen
- **PDF:** The PDF version, as displayed in Adobe, also includes bookmarks allowing rapid scrolling to the bookmarked content. This version can be saved and archived locally

Click **Generate Now** once selections are made.

Create a Group ID

Security Administrators can create a Group ID, assign users to the group, and modify the group so that all users always have the same entitlements. This saves time when adding new services or accounts to multiple users as the action can be done at the group level. To create a Group ID select **Admin > Manage User Services** from the menu in the Lockbox Premier module. Then select the **User Groups** tab, and click the **Create Group** button.

Enter a Group Name and Description (e.g. Customer Service Team). Select Create to add the new group profile to the system. This feature is single release and does not require that another Lockbox Administrator release this request.



Create group [X]

Group Name *

Group Name is required

Group Description

Create Cancel

Edit a Group ID

Modification can be made to a group after a Group ID has been created. Select **Admin > Manage User Services** from the menu in the Lockbox Premier module. Then select the **User Groups** tab Click **Action** next to the group to be modified and then make your changes as you would for a User ID. A second Lockbox Administrator will also need to log in to release the changes the same way they would for a user change.

Assign a Group ID

To assign a user to a Group from the Lockbox Premier module you should select **Admin > Manage User Services** from the menu in the Lockbox Premier module. Next select the **Users** tab. Select **Action** next to the **User ID** that you want to add to the group and then select **Modify Profile**. A Modify User Profile window will pop up. In this window, under the **Security Settings** section, select the appropriate Entitlement Group from the drop-down box, and select **Save**. The User ID will then need to be released by a second Security Administrator.

Modify User Profile

32/50

Confirm Email

johndoe@xxxxxxx.com

Security Settings

Date Format *

Company Level

Expiration Days

365

Global ID

Disabled

Entitlement Group

Save

Reset

Cancel

All trademarks, service marks and trade names referenced in this material are the property of their respective owners.
Member FDIC. (7/26)