



Security Manager Guide

December 2012



Table of Contents

1. Welcome to CitiDirect BESM	6	3. Getting Started with CitiDirect.....	15
The Activation Process.....	6	System Requirements.....	15
Using This Guide.....	6	Browser Security Settings.....	16
2. Security Manager Role Overview	6	Login Guidelines.....	16
Advanced Planning.....	7	Using Challenge Response.....	17
Analyze the Structure of Your Organization.....	7	Using a Secure Password	19
Analyze Your Operational Structure and Workflow.....	7	Log in with a SafeWord™ Card – Host 2	20
Roles and Responsibilities	8	Log in with Multi-Factor Authentication – Host 9 & User ID	20
Onsite Activation Steps.....	9	Using a Digital Certificate.....	21
Client Linkage	10	SafeWord Card Tips	23
CitiDirect Default Settings.....	10	Secure Password Tools and Policies	24
Release Communications	11	Assistance	25
Release Summary.....	11	Customer Security Tips	25
Release News.....	11	Registration, Check My PC and Installation.....	26
Broadcast Messages.....	11		
Maintaining CitiDirect Security	11		
CitiDirect Security Components.....	12		
Best Practices for Security Managers	13		
Best Practice for All CitiDirect Users	14		



4. General Navigation.....	35	5. System Setup and Maintenance.....	42
The CitiDirect Welcome Screen.....	35	Library Maintenance.....	43
Portal Page.....	35	Benefits of Using Libraries.....	44
Help.....	35	Types of Library Data.....	44
My Settings.....	36	Access to Libraries.....	44
Applet Page.....	37	Viewing Library Records.....	45
Inbox.....	38	Adding Records to a Library.....	47
CitiDirect Support Website.....	38	Modifying or Repairing Library Records.....	50
Company Name/Client ID.....	38	Authorizing Library Records.....	52
Close Button.....	38	Deleting Library Records.....	55
Preferences.....	39	Client Preferences.....	58
Online Help.....	39	Viewing Client Preferences.....	58
Summary Forms.....	39	Modifying or Repairing Client Preferences.....	60
Tabs.....	40	Authorizing Client Preferences.....	63
Action Buttons.....	40	Flow Maintenance.....	65
Detail Forms.....	41	Viewing Current Flow Controls.....	66
Library Lookup Button.....	41	Modifying or Repairing Flow Controls.....	68
Searching and Sorting Records.....	41	Creating New Flow Controls.....	72
		Authorizing Flow Controls.....	75
		Deleting Flow Controls.....	78
		Access Profile.....	80
		Viewing Access Profiles.....	81
		Modifying or Repairing Access Profiles.....	83
		Creating New Access Profiles.....	86
		Authorizing Access Profiles.....	88
		Deleting Access Profiles.....	91



5. User Setup and Maintenance.....	93	6. CitiDirect® Online Banking Reports and Inquiries.....	165
User Setup	95	Security Manager Reports	166
Create User	95	Audit Reports.....	167
User Worklist.....	99	Audit Log Summary Report.....	167
View All Users.....	109	Audit Log Detail Report.....	173
User Group Maintenance	112	Access Management Reports	178
Create User Group.....	112	Account Management Summary Report.....	178
User Group Worklist.....	116	Access Profile Detail Report.....	183
View All User Groups	122	Logon Activity Report.....	187
User Group Association Maintenance	124	User Profile and Entitlements Report.....	192
Create User Group Association.....	124	Security Manager Inquiries	197
User Group Association Worklist.....	129	Inactive User Inquiry	197
View All User Group Association.....	135		
User Entitlements	137		
Assigning User Entitlements	138		
Authorizing User Entitlements.....	140		
Modifying or Repairing User Entitlements	144		
CitiDirect BE Mobile User Setup	151		
Access Profile – Onboarding:	151		
Entitling Client Security Manager Onboarding:.....	155		
Entitling Users – Client Security Manager.....	156		
Functional and Run-Time Users	161		
Functional User	161		
Run-Time User	163		

7. Security Manager Support Functions.....	199
SafeWord Platinum Card Distribution	199
Replacing SafeWord Platinum Card Security Credentials.....	200
Secured Password Rules	203
Risk-Based Authentication and Secure Passwords	203
Answers/Locked IDs	204
Changing a User's Security Credential Type.....	204

Welcome to CitiDirect BESM

CitiDirect BESM, the powerful transaction and information delivery application from Citigroup, centralizes your corporate banking functions to give authorized users around the world access to accounts and information in a web-based environment.

Designed to help you streamline processes, CitiDirect[®] offers a high level of internal and external security measures that protect the integrity of your data throughout each transaction.

The Activation Process

The activation process starts when services of Citibank are sold, and ends when your organization is fully implemented and able to use the CitiDirect BE application. The following steps, coordinated by Citi, are included in the activation process.

1. The input of your organization's information (completion of the Client Definition form).
2. Activation of accounts (if necessary).
3. Linking your accounts to the CitiDirect application.
4. Creation of initial Security Manager Profile.

Using This Guide

This guide will assist you in understanding the events that will take place during activation, the approximate order in which they will occur and your role as a Security Manager. Once the initial activation is completed, this guide can be used as a reference tool for the CitiDirect application, user maintenance and to assist in audit activities.

This guide also provides you with the information needed for many of the basic setup and administrative functions within the CitiDirect application. It includes the procedures for setting and maintaining CitiDirect configuration parameters, enacting security measures and populating libraries.

Note: Some regional and country-level products/services may require advanced setup techniques that go beyond the scope of this guide. For assistance with advanced security management techniques, contact your local Implementation Manager.

Security Manager Role Overview

As a new (or migrating) Security Manager for CitiDirect (henceforth CitiDirect will imply CitiDirect BE in this document), it is important that you understand the processes for enabling users within your organization to access and make transactions with CitiDirect.

To protect your company's information and to comply with legal and regulatory guidelines, CitiDirect is delivered with a predefined setting that all administrative and transaction-processing functions require authorization. This central principle of security management is called maker-checker. CitiDirect requires that each client identify and set up three Security Managers (two are primary security managers and one backup) for their organization during the Client Definition phase of activation.

Note: Security Managers are not required to be located at a single site, but they must have access to CitiDirect.

Advanced Planning

The security infrastructure and functionality built into CitiDirect BE are designed to meet strict global banking compliance standards and integrate with your own corporate information security standards and workflows.

To successfully implement CitiDirect, you must understand the unique needs and operational flows of your organization. The quality of the information you gather in this planning stage will directly impact the effectiveness and pace of your activation.

Working with your CitiDirect Implementation Manager, you need to gather key information before initiating and executing on-site activation of CitiDirect. Sample questions you should answer prior to activation are:

Analyze the Structure of Your Organization

1. Is your organization centralized? Is it managed as a single entity, with one Client Definition for all users, all regions, all countries, etc.?
2. Is your organization decentralized? For example, is it managed regionally, with various treasury centers or shared service centers in different locations?
3. Is your organization managed with a combination of the above? For example, regional definitions but the treasury department links to all definitions.
4. Are there remote Security Managers? What is their role?
5. Do you have initiators of transactions in one location and authorizers in another location?

Analyze Your Operational Structure and Workflow

1. Who are your users?
2. From what location will they be accessing CitiDirect?
3. What are their roles? (Data input, authorizing, final approval, etc.)
4. What are their transaction inputs and authorization amount limits?
5. At what times of the day, week and month do they need access to CitiDirect?
6. To which products, accounts, actions, functions, currencies and reports/inquiries do they need access?
7. From which products, actions, functions, accounts, currencies and reports/inquiries should they be restricted?
8. Who requires reporting access only?
9. Any special rules, requirements and privileges?
10. Are there individuals within your organization who have specific or unique privileges that need to be accommodated in the workflow?
11. How does your organization manage its treasury and accounting operations? For example, are there levels of authorization required on wire payments, checks, etc.?
12. Do you have different authorization levels based on free-format versus preformatted (predefined, saved) transactions?
13. Are there specific file formats used for batch processing that require setup?

Roles and Responsibilities

The three key roles in the activation process and their associated high-level responsibilities are listed below. Familiarizing yourself with these roles and responsibilities will help you to understand each of the process steps to manage the expectations within your organization.

Citi

1. Completes Client Definition forms that establish your organization as a client and provides subscription to the product and applications to be used.
2. Records pertinent to Security Manager information provided on the Client Definition forms. Security Managers named in this process receive the information required to set up CitiDirect locally.
3. Assigns the CitiDirect services your organization needs via Solution Packaging.
4. Links your organization with the appropriate accounts and financial products.
5. Delivers standardized default access profiles and flow controls.

Security Manager/Project Coordinator

1. Receives the appropriate setup documentation and security credentials.
2. Registers at www.citidirect.com.
3. Installs CitiDirect BE locally. Participates in Security Manager training coordinated by the local Implementation Manager.
4. Reviews the Citi-defined settings for the products/services their organization uses.
5. Defines client preferences and other organization specific information.*
6. Reviews flow controls for CitiDirect services.*
7. Reviews libraries and performs maintenance as necessary.
8. Creates users, user groups and user group associations.
9. Creates access profiles to set or define entitlements.
10. Assigns user entitlements to link access profiles to users.
11. Communicates and assists end users with installation and access.
12. Performs regular audit and security maintenance.

CitiDirect® End Users

1. Receives CitiDirect security credentials.
2. Completes CitiDirect installation.
3. Self-trains with the CitiDirect Basics guide and other materials provided by Citi.
4. Sets personal preferences using the My Preferences feature.
5. Begins working in CitiDirect.

*CitiDirect BE is delivered with standardized (Default) client preferences and flow controls. It is the responsibility of the Security Manager to review these settings with their Citibank Implementation Manager to determine that the coverage provided by these default settings is adequate.

Onsite Activation Steps

Transitioning to CitiDirect BE requires that several critical steps be completed. As Security Manager, you will perform the tasks listed below:

Task	Description
Set Client Preferences	<p>Client Preferences are key settings for the input forms used within CitiDirect® Online Banking. These settings affect how every user at your organization will experience CitiDirect.</p> <p>As Security Manager, you will use the Client Preferences service class to maintain and modify preference settings for transaction prefix ID, auto save frequency and base currency for payments, etc. CitiDirect is delivered with preferences predefined; however, preferences are customizable to fit your business and operational needs.</p>
Add Records to Libraries	<p>There are three types of libraries supported on the CitiDirect BE application: Citi-maintained, Shared (both Citi and the Client share the information and maintenance) and Client-defined.</p> <p>As a Security Manager, the creation and standardization of libraries early in the activation process allows you to organize your end users' access later in the process. Libraries are associated with specific products. Ask your Citi implementation Manager which libraries you will need to set up first.</p>
Define Flow Maintenance	<p>Flow Maintenance allows you to control the flow of your organization's processes within CitiDirect Online Banking. Flow Maintenance enables you to quickly and efficiently specify the workflow that transactions, service requests and libraries must follow before Citi can process them.</p> <p>Predefined CitiDirect flow controls are delivered with each service class, but can be customized to meet your organization's needs. If you do not customize your flow control criteria, CitiDirect-defined controls for the service class will remain in effect.</p>
User Maintenance	<p>The self-service module in CitiDirect portal will allow you to create user, creating user groups and associating user to user groups. You will be able to provide subscription to CitiDirect for your users.</p> <p>Access Profile enables you to define and control access to groupings activities within the CitiDirect application. The choice of services available for you to group into an access profile is derived from the solution packages assigned to your organization by Citi.</p> <p>After being grouped by role, activity or product, access profiles are assigned to individual user profiles via user entitlements. If a new CitiDirect service or solution is enabled for your organization, the simple task of adding that service to an access profile will enable all users assigned that access profile the ability to use the new service.</p>
Link User Entitlements	<p>The User Entitlements service class enables you to assign access profiles by linking them to individual user profiles. In most cases, the access profile and user profile are created prior to this step.</p>

Notes:

1. The events listed above are not necessarily sequential. Some events can occur concurrently.
2. A series of sub-steps support each of the activities listed.
3. Detailed procedural steps to accomplish these tasks are provided in this guide.
4. After completing the initial setup in the sequence above, you may need to repeat an activity step (for example, create a new user, add a new access profile, etc.) independent of the setup process detailed here.

Client Linkage

CitiDirect BE provides the facility for companies to link with their subsidiaries via the Client Linkage feature within CitiDirect. Client Linkage supports a centralized system administration model and remote authorization access for clients with decentralized operations. Client linkage can be utilized to support your Contingency of Business Plan (access to another site/definition if local users experience system access issues or emergencies).

The Client Linkage functionality requires advanced security management methods not detailed in this guide. If your organization makes use of this functionality, please contact Citi for assistance with setup.

CitiDirect Default Settings

CitiDirect BE is delivered with default client preferences, flow controls and basic Security Manager Access Profiles in place. You are responsible for reviewing these CitiDirect-defined settings with your Implementation Manager to determine that the coverage is adequate.

Service classes and their CitiDirect-defined settings are displayed within Flow Maintenance.

Notes:

1. These defaults do not require changes for CitiDirect BE to function.
2. With each new release of CitiDirect BE, you should review the default settings of any new product or service. Details of these service upgrades can be found in Release News, which is published with each new CitiDirect release and posted on www.citidirect.com.

Category	Service Class
Flow Maintenance	Client Preferences Access Profile Export Profile Flow Maintenance Automated File and Report Delivery Libraries User Profiles User Entitlements Payments

Release Communications

Citi periodically updates CitiDirect BE features and functionality in the form of a new release. New releases often feature global legal and regulatory changes, upgrades and enhancements to existing products and services, and the introduction of new products, services and functionality. In conjunction with each new release, Citibank provides Release Summary and a Release News, which provides the details for the enhancements. These are posted on www.citidirect.com in the Customer Support section.

Release Summary

The Release Summary is a high-level list of service upgrades and changes planned in an upcoming release. It is posted on portal.www.citidirect.com several weeks prior to a release so that you can initiate any preparation required for your organization.

Release News

Release News contains detailed descriptions of the changes and enhancements within the new release and provides steps for procedures as needed. It is posted on www.citidirect.com closer to the release date.

Broadcast Messages

Broadcast Messages are used to communicate important information directly to you from Citi. They appear immediately after you sign onto CitiDirect. These messages often inform you of platform or system changes.

Maintaining CitiDirect Security

Local security management and maintenance of CitiDirect Security is an ongoing process. Below are details regarding security components, user authentication and a list of best practices for Security Managers and all CitiDirect end users.

CitiDirect Security Components

CitiDirect BE security consists of the components described below:

1. **Encryption:** Data encryption protects data from being viewed by people who are not authorized users. CitiDirect uses Secure Sockets Layer (SSL) Version 3, a protocol designed to provide privacy between a web server and client, using 128-bit encryption enabled by digital certificates.
2. **User Entitlement and Authorization:** As a Security Manager, you are responsible for assigning user access profiles to the users in your organization. Each time authenticated users sign onto CitiDirect, the application references this profile to control their authorized level of access and functions.
3. **User Authentication:** CitiDirect employs five methods for accessing the application: a SafeWord™ Platinum card or Secured Password. A SafeWord card is a credit-card-sized device that generates a dynamic password each time a user signs onto CitiDirect. CitiDirect validates this password to ensure that the user is authenticated. Dynamic passwords greatly reduce the risk of an unauthorized party gaining access to CitiDirect by guessing or obtaining a password. If the user is accessing CitiDirect for view-only purposes (reports, inquiries and the View tab in payments modules only), he or she can sign on with a CitiDirect Secured Password (a static ID). Other login methods are being illustrated under Login Guidelines in Getting Started with CitiDirect.
4. **Machine Tagging** provides an extra layer of security for Secured Password access by registering a user's computer details to establish a baseline profile. Future logins are compared against the profile for assessment of extraordinary activity that may require additional review. The CitiDirect server uses heuristic analysis to determine if the user's logon pattern or profile is consistent with prior usage patterns, and returns a risk score based on the security algorithm. If the score exceeds a set threshold, users are prompted to answer three secret questions prior to being granted access to CitiDirect. These questions and answers were previously established between the user and CitiDirect upon initial setup of a Secured Password-based user ID.

SafeWord™ Platinum Card Authentication: The SafeWord card is a Citi-supplied physical hardware device that is used in conjunction with a prompt that appears on the CitiDirect challenge/response screen each time a user signs onto CitiDirect. In order to use the SafeWord card, the cardholder must enter the proper Personal Identification Number (PIN) into the card. After the proper PIN is entered, the cardholder enters the challenge that appears on the CitiDirect sign-on screen. The SafeWord card generates a dynamic password and the user enters this dynamic password into the response field on the CitiDirect challenge/response screen. Upon successful sign-on, the user will have access to the functions included in his or her assigned access profile. Once an employee is set up as a SafeWord card user, Security Managers are responsible for the explanation of initial sign on, rules and relevant support. In some instances, the Security Manager may also be responsible for the central distribution of credentials to users within their organization.

Secured Password Authentication Method: The Secured Password authentication method is available to users who have view-only access to CitiDirect functions.

Note: Secure credentials such as SafeWord cards, user IDs and secured passwords must be protected from loss or inadvertent disclosure to unauthorized users. The client is legally responsible for any financial loss occurring as a result of transactions made with lost, stolen or otherwise misused security credentials.

Best Practices for Security Managers

Security Managers are responsible for security services and supporting documentation. They must implement a secure process to authenticate requests to add, change, modify or delete users from CitiDirect. Designated Security Managers should maintain the practices listed below:

1. Run and review an audit report of user activity daily, or as designated by your own internal audit/control procedures.
2. Ensure that a process is in place to review users who have been disabled from CitiDirect, and that you follow up on any suspicious disablement, such as the same person becoming disabled from CitiDirect on a regular basis. If users become disabled on a recurring basis, you must follow up to make sure they are aware of this, and review their sign-on procedures to ensure that they are entering the correct information.
3. If you identify unusual activity, such as persistent unsuccessful sign-on attempts from the same source, report this to your supervisor for review. If necessary, report this activity to your Citi representative for follow-up.
4. Ensure a process is in place to identify and immediately remove all users who change jobs or leave the organization. This should include a process to obtain their SafeWord card prior to their leaving and immediately deleting any current SafeWord card IDs or Secured Password IDs and related passwords.
5. Ensure a process is in place to collect and dispose of SafeWord cards no longer in use.
6. It is recommended that Security Managers only perform transactions that do not conflict with their security administration function. However, as responsibilities differ from organization to organization, you should follow your specific corporate standards.
7. Perform a quarterly (or as designated by your own internal audit procedures) review of all users on CitiDirect by running the Inactive User inquiry. Obtain supervisory approval and confirmation that they are all still authorized and that their entitlements are still current. This should include an entitlement review to prevent conflicting entitlements and the circumvention of the segregation of duties.
8. Maintain all approved user documentation for audit and review purposes.
9. Never transfer or internally reissue SafeWord cards between users. This ensures an accurate audit trail for transactions and other platform activities.
10. It is recommended that any changes to flow maintenance be done after end-of-day processing is completed. All changes should be validated before the next process date.
11. Have a backup or continuity of business process in place that ensures backup to cover a person on vacation. Security Managers who will be out of the office should not give their cards to their designated backup. Each backup must have a unique SafeWord card.

Best Practice for All CitiDirect Users

Below are the best security practices that all CitiDirect BE users should follow in order to maintain security at all times. We recommend that this information be provided to all CitiDirect users in your organization. This list should be used as discussion points when introducing CitiDirect to your staff.

SafeWord™ Platinum Card Security

1. You are responsible for all activities performed using your SafeWord card and Personal Identification Number (PIN).
2. Upon receipt of your SafeWord card, make sure that your PIN mailer arrived unopened. If you receive an opened PIN mailer, report this to your Security Manager immediately.
3. Once you have successfully accessed CitiDirect, personalize your PIN (set your own).
4. Never write down your PIN.
5. Never store your PIN with your card.
6. Never give your PIN to anyone else for any reason.
7. Keep your SafeWord card with you at all times or leave it in a secured location.
8. Never give your SafeWord card to anybody else to use.

Secured Password Security

1. You are responsible for all activities performed with your User ID and Secured Password.
2. Upon receipt of your static ID and Secured Password, ensure that they have been received in an uncompromised manner. If you receive your Secured Password from a single source, it is likely that the originating source is aware of your password. You should immediately sign onto CitiDirect and change the password to something only you know (see the next bullet regarding initial sign-on).
3. The first time you sign on with a Secured Password, CitiDirect automatically displays the Change Password dialogue box. The application will always force the user to change their Secured Password at initial sign-on. If it does not, immediately report it to your Security Manager.
4. Choose a Secured Password that cannot be easily guessed. Passwords must consist of letters and numbers.
5. Never write down your Secured Password.
6. Do not share your Secured Password with anyone.
7. If you believe that your Secured Password has become known to anyone else, change it immediately. If necessary, report the circumstances of this to your supervisor or Security Manager.
8. CitiDirect will force you to change your Secured Password every 30 days.

Getting Started with CitiDirect

The CitiDirect BE employs secure login processes to ensure that data is safe and accessible only to authorized users.

In order to log in, along with your User ID, you also need a Secure Password or a SafeWord Card that generates dynamic passwords or a Digital Certificate. Only an authenticated combination of your User ID and Secure Password or the password generated by the SafeWord Card or a valid Digital Certificate will allow you to log into the CitiDirect BE.

System Requirements

The minimum software requirements to run CitiDirect BE on your Personal Computer (PC) are listed below:

Windows® Operating Systems:

CitiDirect BE is certified to operate on the Microsoft Operating Systems listed below excluding versions indicated:

1. Windows® XP Excluding: Arabic OS
2. Windows® Vista Excluding: Arabic OS
3. Windows® 7 Excluding: Arabic OS

Apple® Mac Operating Systems:

1. Version 10.5 and higher

Internet Browsers:

1. Microsoft Internet Explorer (IE)
2. IE 7.0 with Windows XP
3. IE 7.0 with Windows Vista
4. IE 8.0 with Windows XP
5. IE 8.0 with Windows Vista
6. IE 8.0 with Windows 7
7. IE 9.0 with Windows Vista
8. IE 9.0 with Windows 7
9. Safari version 4.0.1 and higher
10. Firefox 10 ESR

Note: pop-up blocker must be disabled.

Mobile Browsers:

CitiDirect BE Mobile (m.citidirect.com) currently supports native Mobile browsers for the major smart phones (iPhones, BlackBerry, Androids, Nokia, etc.) as well as most of Mobile browsers such as Opera Mini.

DISCLAIMER: Customer will use CitiDirect BE in accordance with the system specifications provided by Citibank. Customer acknowledges that Citibank has no responsibility for Customer's use of CitiDirect BE with a system that does not comply with such specifications.

Browser Security Settings

Users need to ensure their browser security settings are set properly so CitiDirect BE portal services will run properly.

These settings can be found and set in your browser as follows:

IE browser versions – from the IE Browser Tools menu go to Internet Options and select the Security tab.

Listed below are the Security Settings that must be enabled.

1. **Enable – Initialize and script ActiveX controls not marked as safe**
2. **Enable – Run ActiveX controls and plug-ins**
3. **Enable – Active Scripting**
4. **Enable – Allow Programmatic clipboard access**

If you have an Internet Zone set below “High,” these security settings will be set properly for CitiDirect BE.

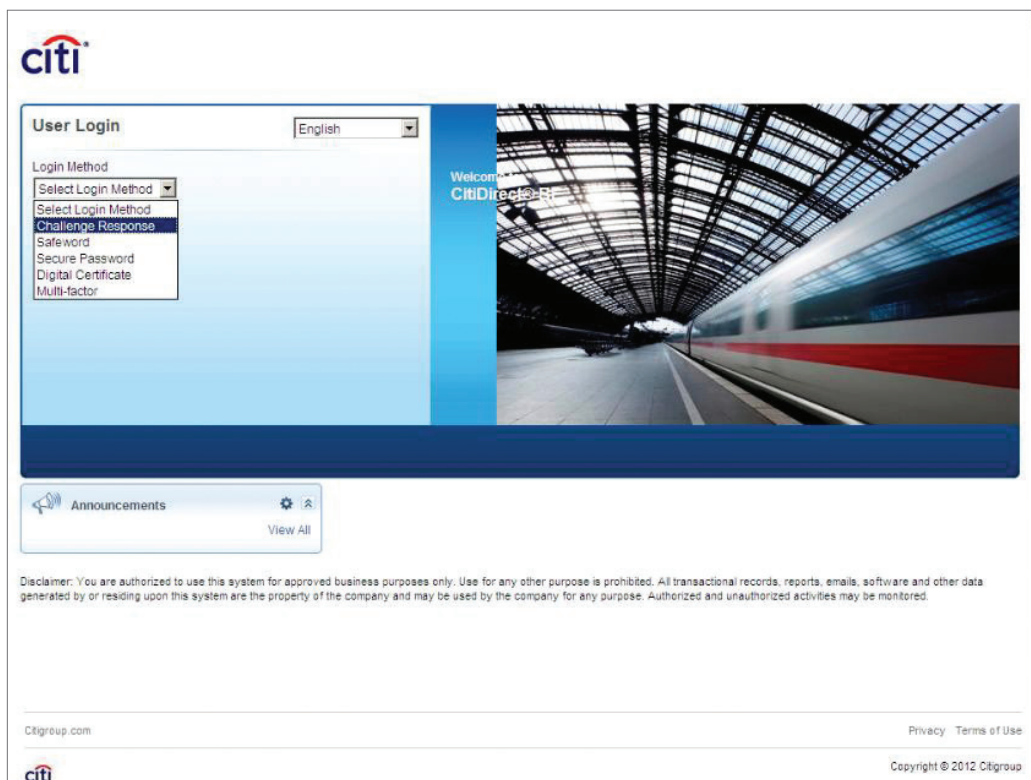
If you have an Internet Zone set as “High,” these security settings will need to be enabled under “Custom Settings.”

Firefox browser versions – from Firefox Browser “Tools” menu go to Options and select the “Content” tab, ensure the setting “Enable JavaScript” is checked.

All other security settings are enabled in Firefox and do not require any user actions.

Login Guidelines

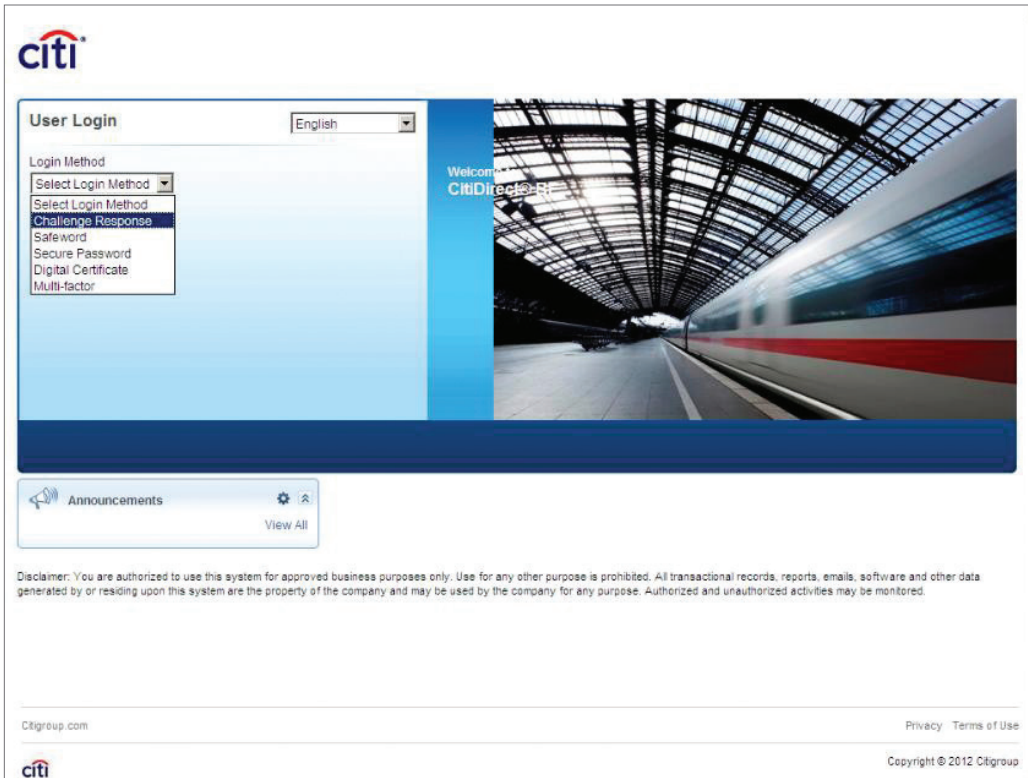
Go to the CitiDirect website at portal.citidirect.com. A screen will appear as below whereas in Login Method, you need to choose the login method applicable for you. Contact your CitiDirect Implementation Manager to know about your login method.



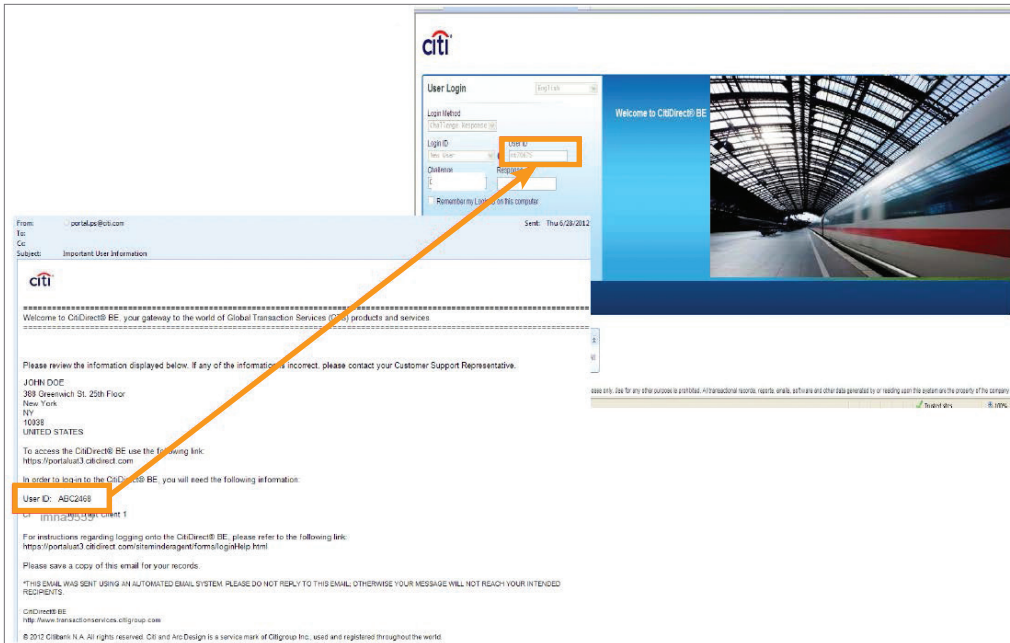
Using Challenge Response

Once you have received a SafeWord card and Personal Identification Number (PIN), you can login in CitiDirect BE using challenge response.

1. Go to the CitiDirect website at portal.citidirect.com.
2. A screen will appear as below whereas in Login Method, Challenge Response is to be chosen from the dropdown list:



3. In the user ID field, enter the unique user ID provided within the welcome message e-mail (delivered upon initial setup within CitiDirect BE application). Below is an illustration of the login process.



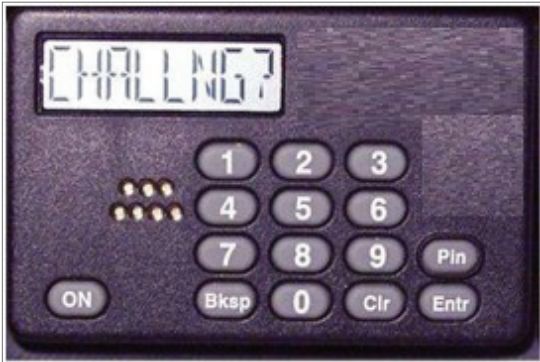
- To generate the required password, you must turn on your SafeWord Card by pressing the "ON" button, and then enter you unique PIN.



- When the screen in the SafeWord Card will prompt for the "Host?" enter 9.



- The challenge displayed on the BE login page is to be entered to generate eight character password.



- Enter the password response provided by the SafeWord card to proceed to the BE portal home page.



- If you check "Remember my Login ID on this computer," you can choose your Login ID from the list in order to log on in the future.
- If you forget your user ID and cannot locate welcome e-mail, your security manager or anyone with admin view can go and retrieve your ID. Also it is to be remembered that the serial number of the SafeWord Card located at the back of the physical card will be your user ID.

Using a Secure Password

After you have received your User ID and Secure Password from the "Important User Information" e-mail notification, please follow these steps to log in:

- Select Secure Password as your Authentication Mode.
- If your Login ID does not appear in the Login ID field, click the dropdown and select New User, then type your User ID in the User ID field.
- If your Login ID appears already in the Login ID field, go to the step below. (Note: Your Login ID is auto populated in the Login ID field if you previously selected "Remember my Login ID on this computer" during your previous login.)
- Enter your User ID and Secure Password in the appropriate space provided.
- Click Login.

Log in with a SafeWord Card – Host 2

A SafeWord™ card and Personal Identification Number (PIN) is required to log into CitiDirect BE.

1. Select SafeWord as your Authentication Mode.
2. If your Login ID does not appear in the Login ID field, click the dropdown and select new user, then type your User ID in the User ID field.
3. If your Login ID appears already in the Login ID field, go to the step below (Note: Your Login ID is auto populated in the Login ID field if you previously selected “Remember my Login ID on this computer” during your previous login.
4. Press ON to activate your SafeWord card.



5. At the ENTR PIN prompt, enter your four-digit PIN.
6. At the HOST? Prompt, enter the number “2.”
7. Enter your User ID and generated dynamic password in the appropriate space provided. (See Using a SafeWord Card to generate a dynamic password for more instructions.)
8. Click Login.

Log in with Multi-factor Authentication – Host 9 & User ID

Before getting started, you will need the following:

1. Your existing SafeWord card
2. SafeWord card PIN
3. Temporary Password e-mail you received from CitiDirect BE

Please use these steps to log in:

1. Navigate to: <https://portal.citidirect.com>.
2. Select your country, then hit Go. This will bring you to the CitiDirect BE User Login screen.
3. Select Multi-factor from the dropdown in the Login Method field. The Login ID and User ID fields will appear.
4. Select New User in the Login ID field. In the User ID field, input the serial number located on the back of your SafeWord Card. Press the Login or Continue button.

Note: If you would like to store your login information locally, click the checkmark box next to Remember my Login ID on this Computer.

5. The Challenge Response fields appear.
6. You must now input a dynamic password generated by using your SafeWord card’s numeric keys and your PIN.



- a. Activate your SafeWord Card and enter your four-digit PIN at the Enter PIN prompt.
 - b. At the host? Prompt, enter the number "9."
 - c. At the CHALLENGE? prompt, enter the CitiDirect BE Challenge which appears in the Challenge Field on your computer screen.
7. In the Response field on your computer screen, enter the response displayed on the SafeWord Card. Ensure that your cursor appears in the Response field before entering.
 8. A Password field will appear. Enter your Password and click Login. For first-time users, you will be prompted to change your temporary password. After your password is saved, you will be prompted to set Security Questions and Answers. These Security Questions and Answers will be used to allow you to change your password in the future. After your Security Questions are saved, you will be granted access to CitiDirect BE.

Note:

If you did not receive a password for Multi-factor login via e-mail, follow the below process to acquire your temporary password.

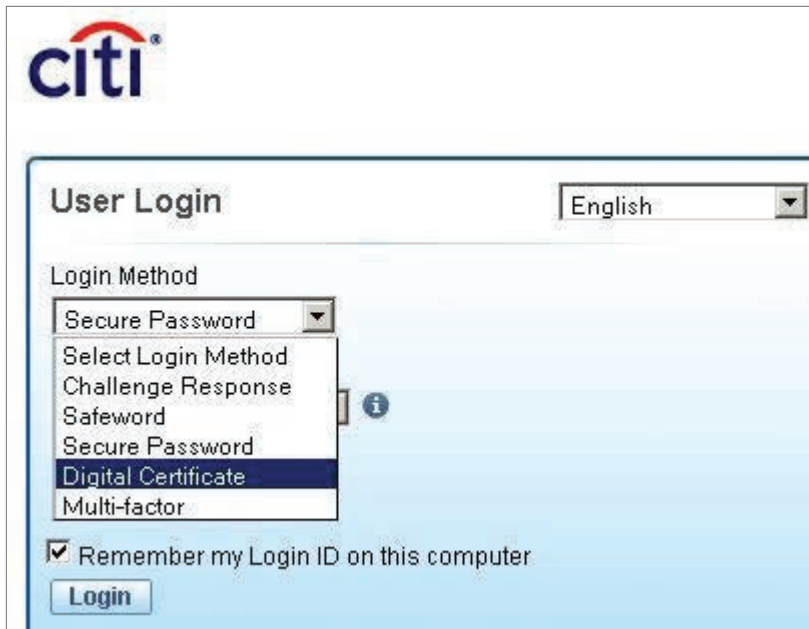
After completing steps 1 - 8, a password field will appear along with a message: "Don't know your password? Click here to reset your password." Click on the indicated link to acquire a temporary password.

You will be prompted to input your e-mail address twice, and then click on Reset Password. You will be sent an e-mail with your temporary password. Upon receipt, log in using the Multi-factor process. The first time you log in, you will be prompted to change your temporary e-mail and set up security questions.

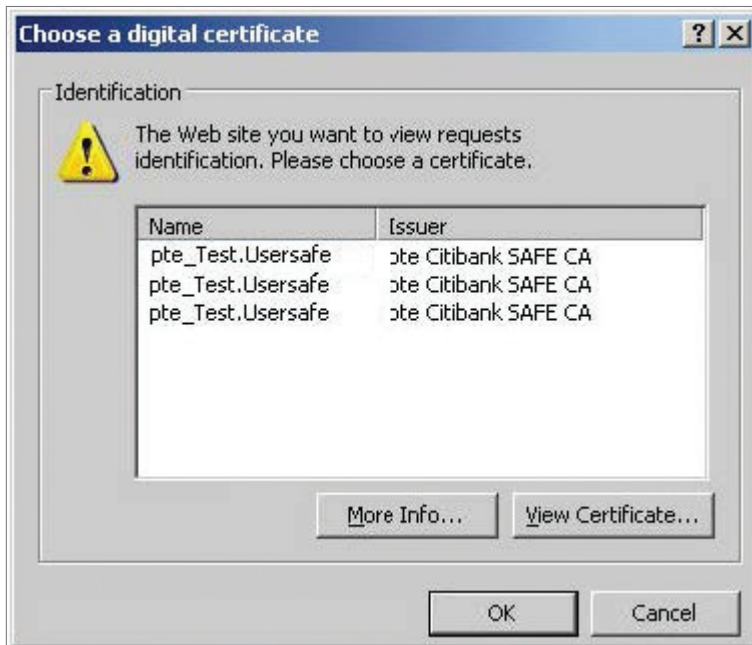
Using a Digital Certificate

You can log on with a digital certificate only after you have downloaded a valid portal logon certificate into your Citi authorized Smartcard/USB Token. If you do not know which certificate is your logon certificate, contact your Customer Support Representative.

1. Select digital certificate as your authentication mode.

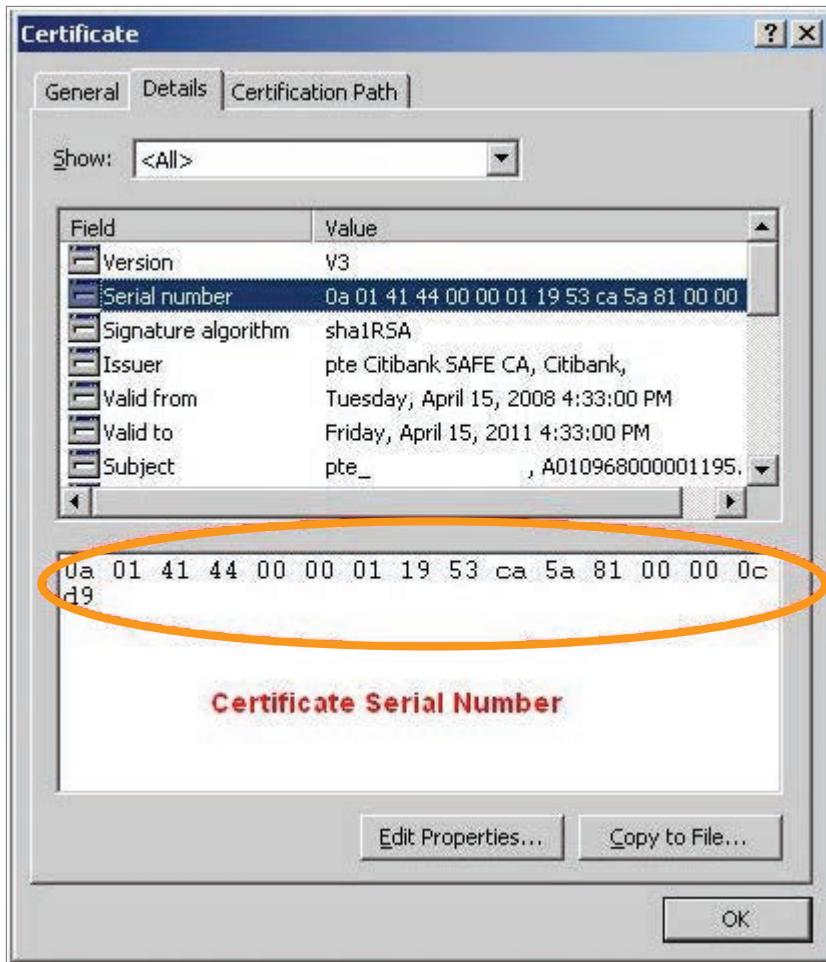


2. You will be prompted with a window displaying a list of digital certificates on your device.



3. Select the appropriate logon certificate and click OK.

Note: To verify that you are using the correct certificate click on View Certificate details. The details tab of the dialogue box will contain the certificate serial number.



4. The certificate will be verified and you will be prompted with a window to enter your PIN.
5. Enter PIN and click OK.

SafeWord Card Tips

Using a SafeWord Card to generate a dynamic password

When you received your SafeWord card, you also received a unique PIN and your host number. You will need that information to generate a dynamic password that is required to log in. Please follow these steps:

1. Switch on your SafeWord Card.
2. At the prompt, enter your unique PIN.
3. Now enter your host number.
4. A password is generated – key in this password in the password field on the CitiDirect BE login screen.

Please note that for some users the displayed dynamic password will contain a hyphen (-). The hyphen should not be entered as part of the password.

New SafeWord card

Citigroup SafeWord Administrators will issue new card and PIN mailer for the users created on CitiDirect BE within a period of ten U.S. business days after receipt of "Important User Information" e-mail notification.

Existing SafeWord card

Citigroup SafeWord Administrators will enable access to existing SafeWord card for the users created on CitiDirect BE within a period of three U.S. business days after receipt of "Important User Information" e-mail notification. If you have not received your SafeWord card and PIN mailer or you encounter any problems accessing the CitiDirect BE, please contact your Implementer or Customer Support Representative.

Secure Password Tools and Policies

Secure Password Tools

1. Forgotten Secure Password – If you have forgotten your password – [click here](#). You will receive a temporary secure password through "Important User Information" e-mail notification.
2. Change Secure Password – If you know your password and want to change it – [click here](#).

Password Policies

Expiration

1. Once the password has expired, the user will be forced to change their password before continuing. A warning will appear for the last five days before a password is about to expire.
2. Once the password expires, the user will be forced to change their password before continuing.
3. Password expires if not changed within 180 days.

Locking

1. Access to CitiDirect BE will be disabled after six successive incorrect passwords.

Composition

1. The minimum password length is 6 characters.
2. The maximum password length is 15 characters.
3. The maximum repeating character length is two.
4. Password should have at least one alphabet and one number.

Restrictions

1. The minimum number of days before a password can be reused is 90.
2. The minimum number of passwords before reuse is six.

Assistance

In case you encounter any of the following problems please contact your CitiDirect BE Customer Support Representative:

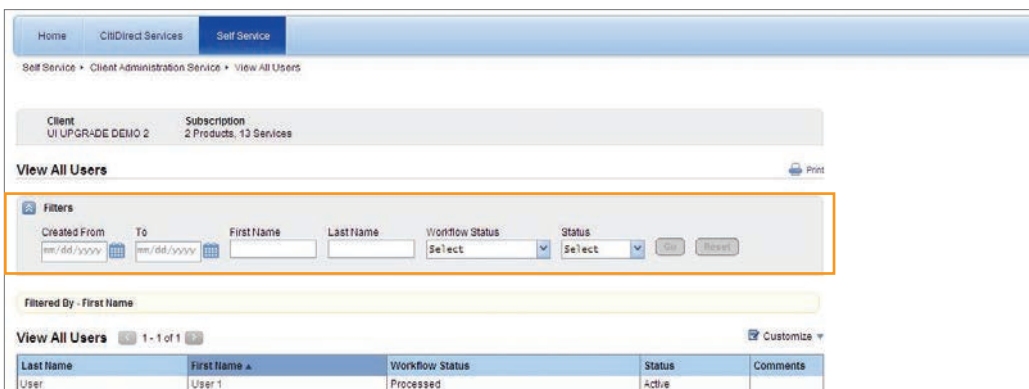
- Unable to generate dynamic password
- Lost your SafeWord™ Card
- Forgot your PIN
- Forgotten User ID
- User locked
- Unable to log in

Customer Security Tips

1. Do not reveal the One Time Password (OTP) generated by the security card to anyone.
2. Ensure that anti-virus, anti-spyware and firewall software is deployed on the customer's personal computers, especially when the personal computers are linked via broadband connections, digital subscriber lines or cable modems.
3. Update the anti-virus and firewall products with security patches or newer versions on a regular basis.
4. Remove file and printer sharing in customer's computers, especially when those computers have Internet access via cable modems, broadband connections or similar setups.
5. Make regular backup of critical data.
6. Log off the online session and turn off the computer when not in use.
7. Do not install software or run programs of unknown origin.
8. Delete junk or chain e-mails.
9. Do not open e-mail attachments from strangers.
10. Do not disclose personal, financial or credit card information to unknown websites.
11. Do not use a computer or a device that cannot be trusted.

Note for Security Manager

The user with Admin Access View will need to go into Admin -> Users -> View All Users. When the users are displayed, double click on the desired user.



Last Name	First Name	Workflow Status	Status	Comments
User	User 1	Processed	Active	

Once the user details are displayed, the user ID that is needed to log in can be found under the User Alias section.

Self Service > Client Administration Service > View All Users

Client
UI UPGRADE DEMO 2

Subscription
2 Products, 13 Services

View All Users > View Details Print

View All Users

Workflow Status: Processed Status: Active

General Information

User Alias: User	Employee ID: 1234	First Name: User 1	Last Name: User	Middle Name:	Initials:
Building/Floor/Room: 123	Street Address 1: XYZ Street	Street Address 2:	Street Address 3:	Country US	
State/Province/Territory: DE	City: jersey city	Zip/Postal Code: 1234	Time Zone: Eastern Time (US & Canada)	Telephone:	
Email: user1@citi.com	User Manager				

CitiDirect Information

SDR User Account Type: Omnibus Account User	User ID 51040100		
CitiDirect Time Zone: Eastern Time (US & Canada)	User Allow Access To Days: 11/29/2012 to 11/29/2025	User Allow Access To Time: 12:00 AM to 11:59 PM	Days of Week: SUN, MON, TUE, WED, THU, FRI, SAT

1 - 1 of 1

Credential Type	Credential ID
<input type="checkbox"/> Safeword ID	Dummy


Registration, Check My PC and Installation

This section describes the three-step process starting with Registration at www.citidirect.com. You must be registered to run Check My PC and install CitiDirect.

Register at www.citidirect.com by following the steps below.

1. Go to www.citidirect.com.
2. Click the Registration link on the CitiDirect menu as shown below.

CitiDirect® Online Banking



Home
About CitiDirect
Getting Started
Customer Support
Trade Advisor
Payment Advisor

Language Preference:

English ▼


- CitiDirect News
- Solutions & Services
- FAQs
- Contacts
- Other Links
- Client Academy
- Transaction Services
- New Functionality - Trade Advisor Mobile

• Site Map

• Registration

• Already Registered

CitiDirect® Online Banking



Welcome to CitiDirect® Online Banking, Citibank's Web-based banking platform. CitiDirect puts all your corporate banking functions in one security-protected place, giving you around the globe, centralized access to your account information in real time right from your computer or mobile device.

CitiDirect News

- [Citi Launches New Trade Functionality On CitiDirect BE Mobile](#) Trade Transaction Status Available on Trade Advisor - Mobile
- [E-mail Fraud on the Rise](#) What you should know about fraudulent e-mails and how to protect yourself.

[View All...](#)

Solutions & Services

An ever-expanding suite of solutions and services designed for today's global economy.


Collections
Liquidity
Netting
Trade
Insurance Letters of Credit

- [Collections Initiation and Reporting Availability](#) List of countries where this service is available.

[View All...](#)

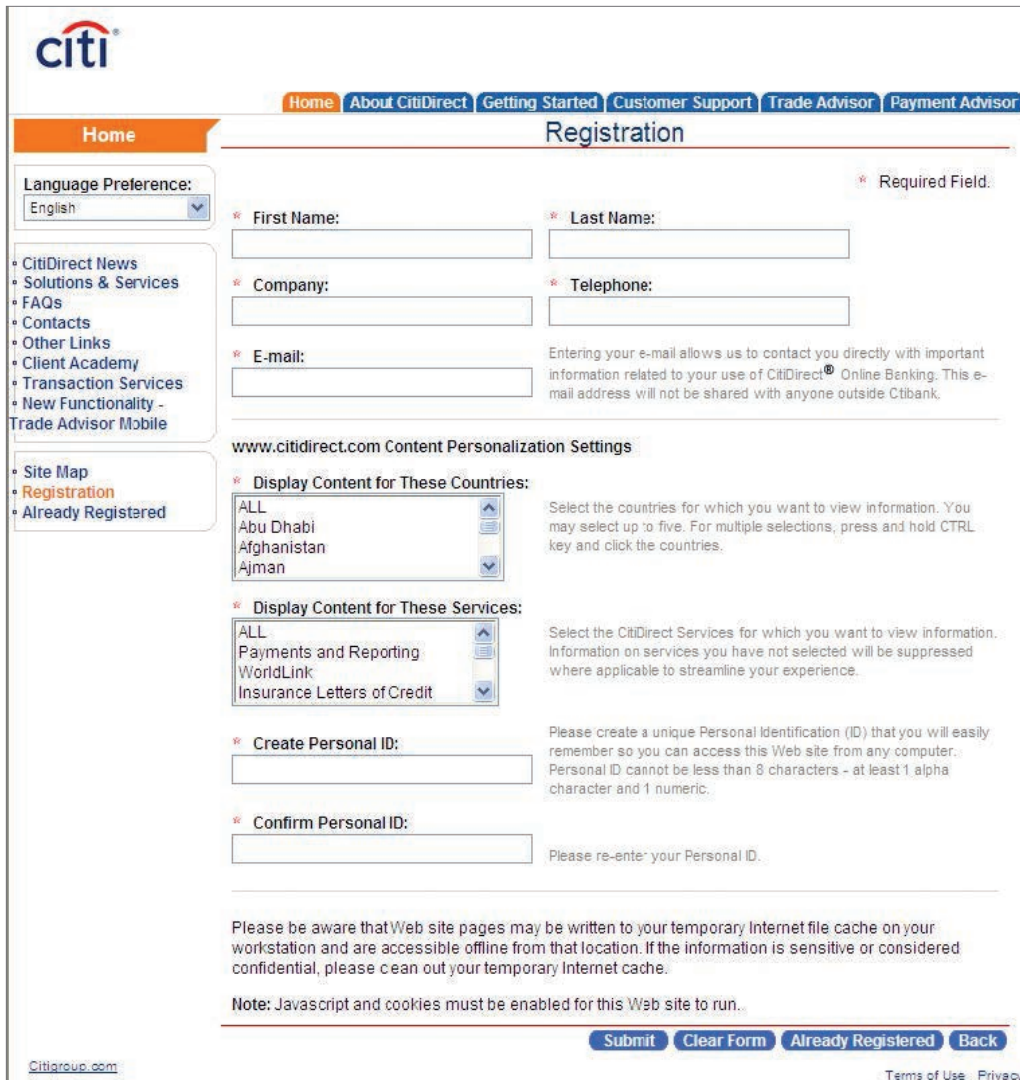
[Citigroup.com](#)

[Terms of Use](#) [Privacy](#)



Copyright © 2003 - 2013 Citigroup Inc.

Note: To register and run Check My PC in a language other than English, choose a language from the Language Preference field on the www.citidirect.com home page.



Registration

* Required Field.

* First Name:

* Last Name:

* Company:

* Telephone:

* E-mail: Entering your e-mail allows us to contact you directly with important information related to your use of CitiDirect® Online Banking. This e-mail address will not be shared with anyone outside Citibank.

www.citidirect.com Content Personalization Settings

* Display Content for These Countries:

ALL, Abu Dhabi, Afghanistan, Ajman

Select the countries for which you want to view information. You may select up to five. For multiple selections, press and hold CTRL key and click the countries.

* Display Content for These Services:

ALL, Payments and Reporting, WorldLink, Insurance Letters of Credit

Select the CitiDirect Services for which you want to view information. Information on services you have not selected will be suppressed where applicable to streamline your experience.

* Create Personal ID: Please create a unique Personal Identification (ID) that you will easily remember so you can access this Web site from any computer. Personal ID cannot be less than 8 characters - at least 1 alpha character and 1 numeric.

* Confirm Personal ID: Please re-enter your Personal ID.

Please be aware that Web site pages may be written to your temporary Internet file cache on your workstation and are accessible offline from that location. If the information is sensitive or considered confidential, please clean out your temporary Internet cache.

Note: Javascript and cookies must be enabled for this Web site to run.

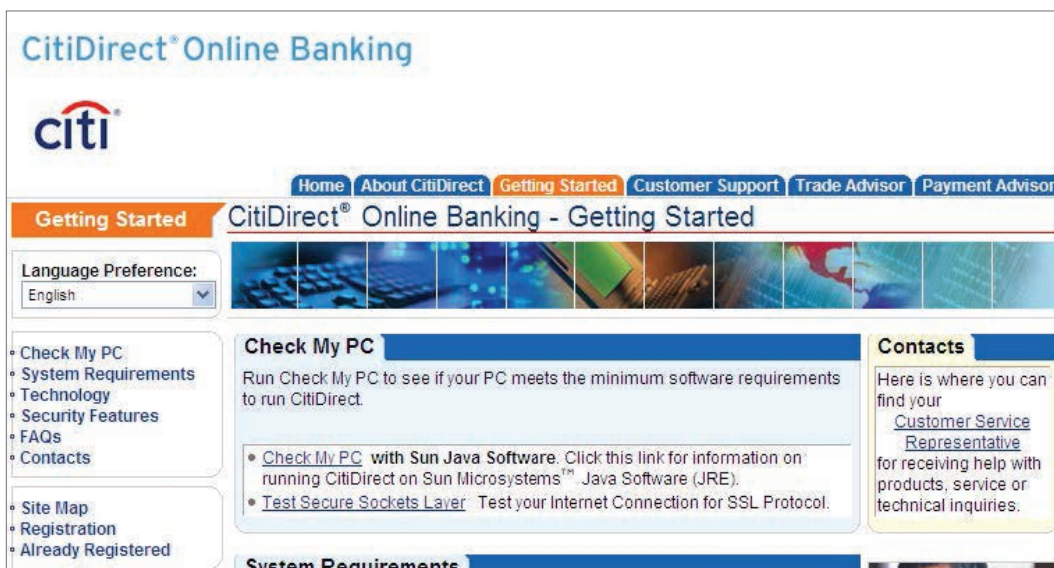
[Submit](#) [Clear Form](#) [Already Registered](#) [Back](#)

[Citigroup.com](#) [Terms of Use](#) [Privacy](#)

3. All fields are required to register. Click the Submit button. You are returned to the www.citidirect.com home page.
4. Click the Getting Started tab.




5. Click the Check My PC link.



6. Click the Check My PC with Sun Java Software button to determine if your computer meets the minimum requirements to run CitiDirect.

CitiDirect® Online Banking



Home
About CitiDirect
Getting Started
Customer Support
Trade Advisor
Payment Advisor

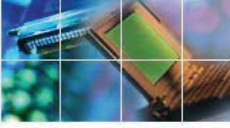
Getting Started

Language Preference:
English ▼

- Check My PC
- System Requirements
- Technology
- Security Features
- FAQs
- Contacts

- Site Map
- Registration
- Already Registered

Welcome to Check My PC



A quick and easy program, **Check My PC** will determine whether your PC meets the minimum software requirements to run CitiDirect® Online Banking. Upon completion of the program, you can view a detailed report containing your PC's Check My PC results.

Get ready to install CitiDirect by:

- Reviewing the system requirements and Internet Explorer settings required for CitiDirect Online Banking. Click the link at right to go to System Requirements.
- Running Check My PC to determine if your PC meets the requirements to run CitiDirect. This program will also check to make sure your machine meets our recommended level of connectivity and throughput.

Note: You must be registered at this Web site to run Check My PC. If you are not, please click the **Registration** link on the left navigation bar to complete the registration process.

- If your PC is **ready** for CitiDirect, you can install the CitiDirect software directly from this site.
- If it is **not ready**, you will be provided with details on the components on your PC that need to be adjusted or installed in order to run CitiDirect.

Contacts

Here is where you can find your [Customer Service Representative](#) for receiving help with products, service or technical inquiries.

Related Links

- [System Requirements](#)
- [CitiDirect Security](#)

[CitiGroup.com](#)
Check My PC with Sun Java Software
Back

[Terms of Use](#)
[Privacy](#)


Copyright © 2003 - 2013 Citigroup Inc.

7. You will see the Details from Check My PC.

CitiDirect® Online Banking

Home
About CitiDirect
Getting Started
Learning Center
Customer Support
Notifications
Trade Advisor
Payment Advisor

Getting Started

Language Preference:
English

- Check My PC
- System Requirements
- Technology
- Security Features
- FAQs
- Contacts

- Site Map
- Update Registration
- Add A Service
- Log-out

Check My PC - Ready For CitiDirect® Online Banking

Your Personal Computer (PC) has met the software requirements to run CitiDirect® Online Banking. You can now install the CitiDirect software.

Before installing CitiDirect Online Banking, you may want to take these steps:

- View the results of the **Check My PC** program for details.
- Ensure that you have your security credentials, which are required to sign-on to CitiDirect. If you do not have security credentials, please contact your CitiDirect Security Manager.

Note: You do not need security credentials to install CitiDirect, but will need them to sign-on.

Details from Check My PC:

Run Date: 15-Jan-2013
Run Time: 15:51:19 EST
Name: :

	Software: Pass	
	Internet Explorer:	7.0
	Cookies:	Enabled
	Sun® Java™ software (Virtual Machine):	JavaPlugin.160_29
	Operating System:	Windows XP en-us
	Access Permissions:	Pass
	SSL Status:	Enabled
	Connectivity and Throughput: Pass	
	Normal Download:	6 ms (68000 ms recommended)
	Secure Download (File):	2 ms (62000 ms recommended)
	Secure Download (Burst):	1 ms (6400 ms recommended)
	Processing and Throughput:	1 ms (97000 ms recommended)
	Source IP Status:	Single (Single recommended)

Frequently Asked Questions

For more detailed information, review our list of Frequently Asked Questions.

- [Why can't I see my new CitiDirect® account on the Payments screen?](#)
- [CitiDirect BE Mobile - Trade Advisor Frequently Asked Questions](#)
- [Does CitiDirect® Online Banking contain real-time information?](#)
- [Why is CitiDirect® running slowly?](#)
- [* I clicked Payments on the Navigation Bar and the Summary Form did not appear. Why?](#)
- [Pop-up Blockers Affecting Your CitiDirect Access](#)
- [Do I have to keep back up files for Import?](#)
- [How can I obtain a personal digital certificate to use with AFRD?](#)
- [Do I need a Web server SSL certificate and a personal digital certificate to use AFRD?](#)
- [What is the purpose of the Automated File and Report Delivery \(AFRD\) Utility?](#)
- [Do I need a dedicated Web server to use AFRD?](#)
- [CitiDirect Event Notification FAQs](#)
- [Security Update for CitiDirect® Online Banking](#)
- [What are the system requirements to run the AFRD Utility?](#)
- [How do I properly add a link to my Favorites list for the CitiDirect® Web site?](#)
- [How do I generate a response from my SafeWord™ card?](#)
- [In what languages is CitiDirect® Online Banking available?](#)
- [I am unable to connect to CitiDirect® Online Banking. What should I do?](#)
- [Internet Explorer Cannot Download Document Error](#)
- [What happens if I leave CitiDirect® Online Banking inactive for a period of time?](#)

[View All...](#)

Citigroup.com
Install CitiDirect...

[View Printable Format](#)
[Terms of Use](#) [Privacy](#)

Copyright © 2003 - 2013 Citigroup Inc.

Note: If your system does not meet the requirements, the Required Software page appears. You will need to have the necessary changes made to your computer so that it meets the requirements.

8. Click the Install CitiDirect button.




9. Select the Install CitiDirect directly from the Web site option.

Note: If you received a CD-ROM for CitiDirect installation, select the Install from the CitiDirect installation CD-ROM option, and click the “Continue...” button. On-screen instructions will guide you through the installation.

10. Click the “Continue...” button.

11. If you agree to the terms on the CitiDirect BE – Download Export Terms page and want to continue your installation, click the Proceed with Download button.

CitiDirect® Online Banking



[Home](#) | [About CitiDirect](#) | [Getting Started](#) | [Learning Center](#) | [Customer Support](#) | [Notifications](#) | [Trade Advisor](#) | [Payment Advisor](#)

Getting Started
CitiDirect® Online Banking - Download Export Terms

Language Preference:

English ▼

The CitiDirect® Online Banking software you are about to download is subject to U.S. export controls. By downloading this software you (i) agree that you will adhere to the conditions set forth below, and (ii) are making the following representations and warranties:

- a. understand that software is subject to export controls under the Export Administration Regulations (EAR) administered by the U.S. Department of Commerce;
- b. are not located in an prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria);
- c. are not a Denied Party, Specially Designated National, or other person or entity prohibited from receiving exports / re-exports by U.S. law;
- d. will not export, re-export, or transfer the software to any prohibited destination entity or individual without the necessary export license(s) or authorization(s) from the U.S. Government;
- e. understand that countries other than the U.S. may restrict the import or use of strong encryption products, and agree that you shall be solely responsible for compliance with any such import or use restrictions and shall indemnify and hold us harmless with respect to any violations of such restrictions; and
- f. do not know of any additional facts that are inconsistent with the foregoing.


You also agree that it is your responsibility to refer to the Export Administration Regulations of the United States and comply with the most current version of same.

If you do not agree to the foregoing, please click the button labeled "Refuse Download" below and the software will not be downloaded onto your system.

If you agree to the foregoing, please click the button labeled "Proceed with Download" below and the software will be downloaded onto your system.

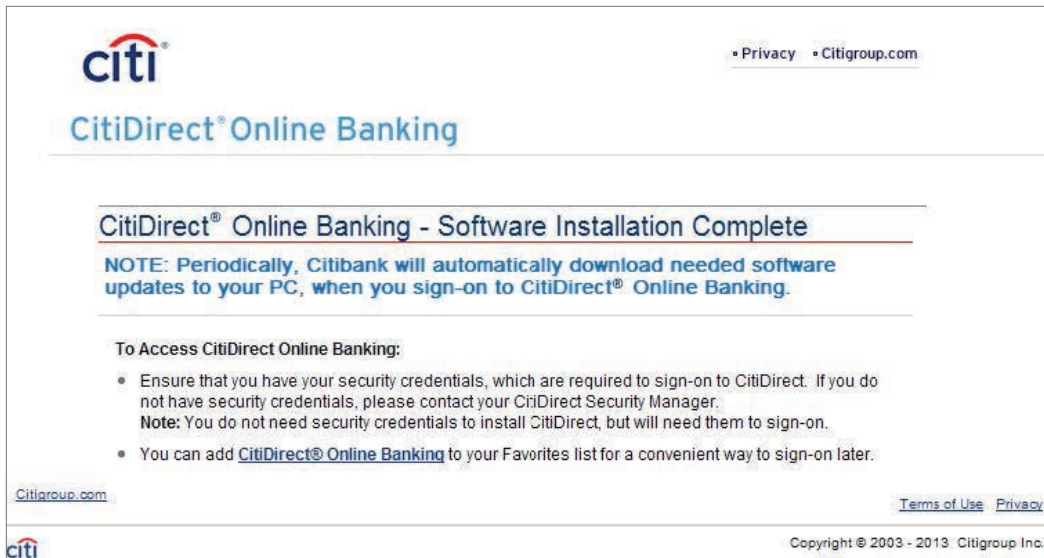
Proceed with Download
Refuse Download

[Citigroup.com](#)
[Terms of Use](#) | [Privacy](#)


Copyright © 2003 - 2013 Citigroup Inc.

Note: If you click the Refuse Download button, you will be returned to the home page and your website registration will remain intact. To install at another time, sign onto www.citidirect.com using the Personal ID you created during registration and go to the Getting Started tab to run Check My PC.

12. When the software download is complete, the CitiDirect BE – Software Installation Complete page appears.



The screenshot shows the CitiDirect Online Banking software installation completion page. At the top left is the Citi logo, and at the top right are links for Privacy and Citigroup.com. The main heading is "CitiDirect® Online Banking". Below this is a section titled "CitiDirect® Online Banking - Software Installation Complete". A note states: "NOTE: Periodically, Citibank will automatically download needed software updates to your PC, when you sign-on to CitiDirect® Online Banking." Underneath, a section titled "To Access CitiDirect Online Banking:" contains two bullet points: "Ensure that you have your security credentials, which are required to sign-on to CitiDirect. If you do not have security credentials, please contact your CitiDirect Security Manager. Note: You do not need security credentials to install CitiDirect, but will need them to sign-on." and "You can add CitiDirect® Online Banking to your Favorites list for a convenient way to sign-on later." At the bottom left is a link to Citigroup.com, and at the bottom right are links for Terms of Use and Privacy. The footer contains the Citi logo and the copyright notice "Copyright © 2003 - 2013 Citigroup Inc."

Note: Click the CitiDirect BE link and add the CitiDirect Sign-on page to your browser's bookmarks for a convenient way to sign on later.

13. Restart your browser. You can now proceed to the next section of this guide for step-by-step instructions on initial sign-on to CitiDirect Online Banking.

General Navigation

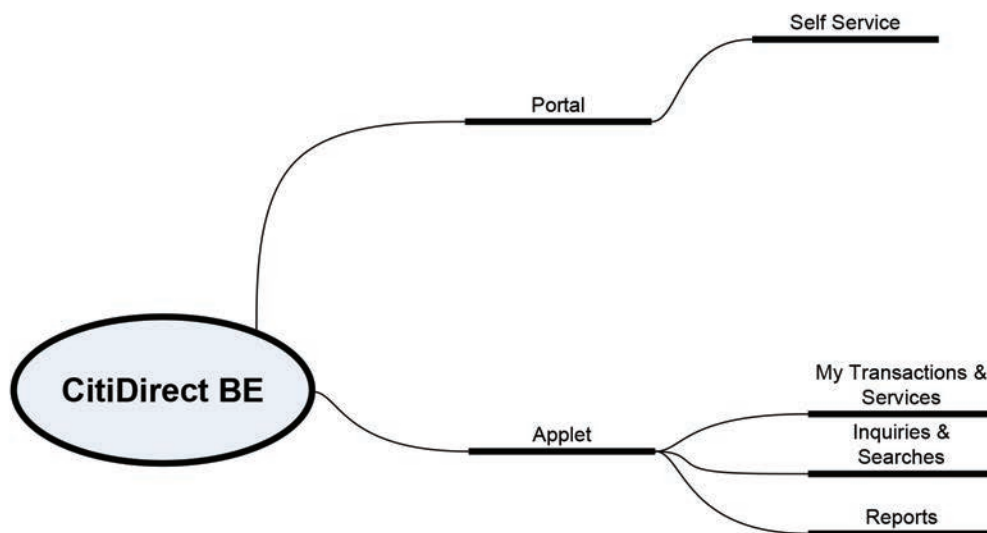
The CitiDirect Welcome Screen

The Welcome to CitiDirect BE screen is the first screen that appears each time you sign onto CitiDirect. This page is the Portal Home Page for CitiDirect BE. You will be able to access various features within the Portal page from here and also you can access the Applet page by clicking on CitiDirect Services.

Below are some of the primary components of the Portal and Applet pages.

Note: The above diagram is indicative in nature. Users may be able to see many other features based on their entitlement in both Applet and Portal.

Portal Page

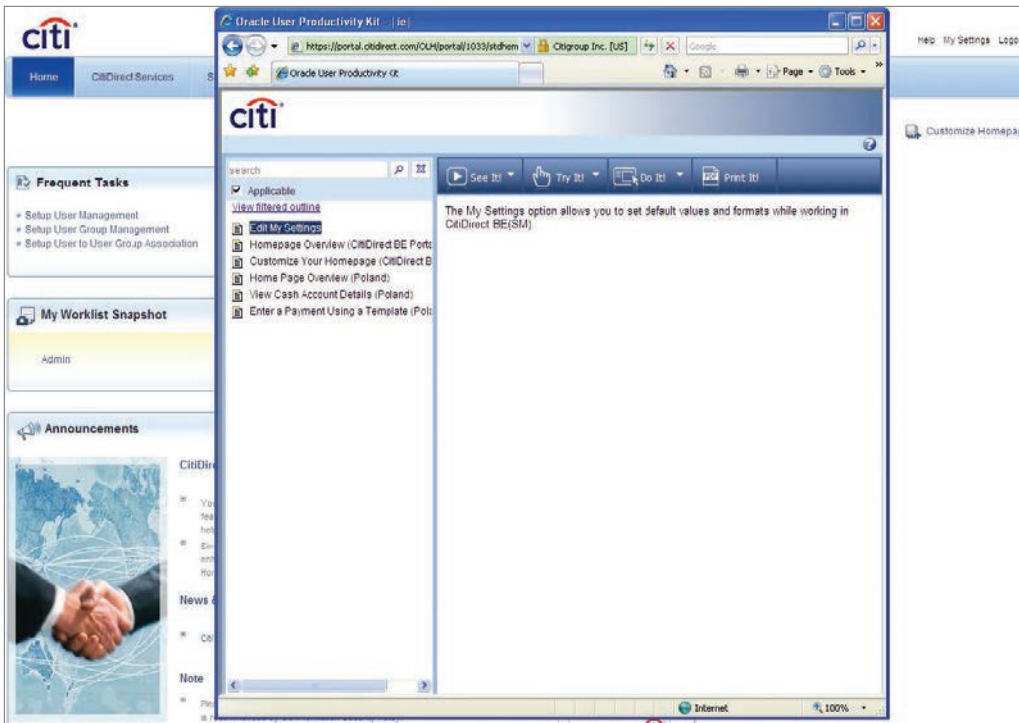


You will be able to access various features of CitiDirect from this page. The Client Administration Service through which the client, user setups can be done is accessible from this page. For accessing the services within CitiDirect, you need to click on the CitiDirect Services in the same blue panel which will open the Applet page in the popup window.



Help

You can see the help hyperlink on the right-hand corner of the screen. Clicking on that will open a separate window that will provide information on various features of the home page.



My Settings

If you click on My Settings on the top right-hand side of the home page, a new page will open as below. You can set the e-mail address, date format, amount format and default language in that. Clicking on submit will save and set the format for you. You can later click to set it back to default. If clicked on Cancel, you will lose all unsaved data and you will be reverted to the home page.

Home • My Settings

Global

Setting for Global

Email Address :


Date Format:
MM/DD/YYYY ▾

Amount Format:
English (No Thousand) ▾

Default Language:
English (United State) ▾


Submit Reset To Default Cancel

Citigroup.com Privacy Terms of Use

 Copyright © 2012 Citigroup

Applet Page

You will be able to see many of the services in a top blue panel in the Applet window based on your entitlement.



CitiDirect® Online Banking
UI UPGRADE DEMO 2
12/05/2012 14:27:42

Online Help | My Preferences | Inbox | Support Website | Close
[Privacy Statement](#)

Home My Transactions & Services Inquiries & Searches Reports Tools & Preferences User Administration

Home Favorite Reports

Welcome to CitiDirect Online Banking For UI UPGRADE DEMO 2

Need Assistance? First time using CitiDirect? The [CitiDirect Support Website](#) contains training, frequently asked questions and support contact information

Components of the Applet Page screen are described below.

Inbox

When you click the Inbox link in the upper-right corner of your CitiDirect Applet page, you have access to the tabs listed below.

1. To Do lists items in your workflow queue require action before Citi can process them. The source of each item is included, along with any associated comments, its priority and status.
2. News lists messages from Citi and other information sources. The screen is divided into summary and detail sections.
3. Status lists all of your current and open CitiDirect items and their related status. The items on this tab are listed for informational viewing purposes only.

CitiDirect Support Website

Click the CitiDirect Support Website link to go to the CitiDirect Support Website. The website offers information and news about CitiDirect, customer support and a learning center. The Learning Center contains user guides and quick reference materials organized by product/service for distribution within your organization.

Note: You can go directly to www.citidirect.com without signing onto the CitiDirect platform to download instructional guides and quick reference cards for end users. Contact your local Implementation Manager for more information and the access code.

Company Name/Client ID

Located in the upper middle portion of the screen is your Company Name or Client Definition name. After clicking any service class on the menu, place your cursor over the Company Name to reveal your CitiDirect Client ID.

Close Button

Log out and close your CitiDirect BE session by following the steps below:

1. Click the Close button on the right-hand side corner of the screen to log out and close all session browser windows. A confirmation dialogue box appears.
2. Click the Yes button to exit CitiDirect Online Banking.

Preferences

Use the Preferences feature in CitiDirect to personalize your experience and work more efficiently. You can select a customized main screen and other preferences based on your individual business needs and job function.

Found at the upper right-hand corner in the Applet page, the Preferences menu provides the following options: Again - my preferences are moved to the upper right-hand in the Applet.

1. **My Preferences:** Click this option to specify information that appears in fields on CitiDirect forms and the process tabs that appear when you access a service class. You can do any of the following:
 - Customize date and currency formats.
 - Select the screen you see once you have signed onto CitiDirect.
 - Customize the appearance of your menu.
 - Define the frequency of functions such as automatic report generation and auto-save.
2. **Customizer:** Customize the CitiDirect menu to your specifications.
3. **Favorite Reports:** Efficiently manage the reports you have designated as favorites and quickly access reports that you have run in the last 24 hours and reports scheduled to run.
4. **COB Contact Info:** Update your contact information for Continuity of Business notifications.

Note: For more information and instruction on fundamental user activities such as setting personal preferences, general CitiDirect navigation and reports, refer to the CitiDirect Basics section in the Learning Center at www.citidirect.com.

Online Help

CitiDirect Online Help is available to provide you with detailed information about using CitiDirect Online Banking, including step-by-step instructions that guide you through basic platform functionality.

To access Online Help, click anywhere in the form where you need assistance, click the question mark icon in the lower-left corner of the menu and then select the Online Help command. You can also press the F1 key on your keyboard.

Summary Forms

All CitiDirect processes are preformatted using a summary form, which displays key fields of information, or a detail form, which contains all of the information required for your current task. In the example below, the Library Summary is displayed. The breadcrumbs will display the navigation path in the Mega Menu.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance Last Login Date: 12/12/2012 17:10:17

Library Maintenance

(1) Service Class	(2) Description
Automated File and Report Delivery	Delivery Options
Export Profile	File Export BAI, ISO and SWIFT Code Library
Import Map Definition	File Import Map Definition Rule Set
Payments	Account Familiar Name
Payments	Account Grouping
Payments	Invoice Type
Payments	Ordering Party
Payments	Payment Description
Payments	Preformat
Payments	Preformat Group

<< Row 1 of 10 >> (1)(2) sorted columns More

OK Search Update Screen

Tabs

A user's access profile will determine the tabs and menu items available when working in CitiDirect. Click a tab to activate it. Once active, the tab label becomes orange.

- **Input Tab** – The starting point for most processes. Generally, all records with a status of Processed (fully authorized and active), Repair Required (records of items returned for repair during the authorization process) or Invalid (records that have failed CitiDirect server validation) are listed when you first access the Input tab.
Use this tab to access the forms needed to create new CitiDirect records and to search for, modify or delete existing records.
- **Authorization Required** – Lists all records with an Authorization Required status that you are entitled to authorize. If you submitted a record, you cannot authorize it. For Security Manager functions, records listed on the Authorization Required tab can be authorized, deleted or sent for repair. They cannot be modified.
- **View Tab** – Lists all records that you are entitled to view, along with their current status. You can select one or more records and click the Go to Details button to view all details.

This tab provides view-only access; therefore, records selected on this tab cannot be modified or deleted.

Action Buttons

Action buttons appear on the lower-right portion of CitiDirect summary forms. Click a button to perform an action. The action buttons that appear vary based on the actions that are available on the active tab within the CitiDirect summary form and the entitlements included in a user's access profile.

Detail Forms

The detail form displays all of the details of a record selected on a summary form, along with any corresponding actions that you may need to perform on that record. In this example, the User Profile Detail form is shown.

- Use the detail form to enter and submit the details of new records, and to manage and act on individual records.
- The detail form can only be accessed from a summary form. However, once in a detail form mode, you can move between multiple records by clicking the Next button.

Library Lookup Button

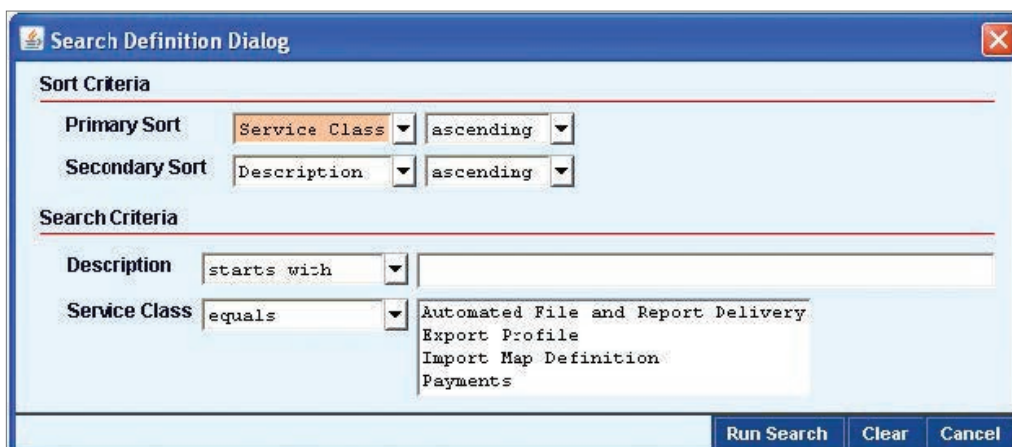
Libraries are CitiDirect database tables that make completing forms and data entry fast and easy. Click a Library Lookup button (which looks like a downward pointing triangle) to access a CitiDirect library. When information is selected from a Library Lookup list, the relevant information automatically populates the current field and any related fields.

Searching and Sorting Records

The Search Definition Dialogue window enables you to control the number of records that are displayed on a tab within a summary form and the order in which those records are displayed. The ability to search for and sort data is also available for certain Library Lookup lists, particularly those that might return a large amount of data.

Use the Search and Sort features by following the steps below:

1. On any summary form or library lookup dialogue list, right-click and select the Search command from the shortcut menu. A Search Definition Dialogue box appears.



Note: You can also access the search feature from any summary form or library lookup dialogue list by clicking the Other Options button and then clicking the Search command.

2. In the Sort Criteria section, select a primary sort field and optionally a secondary sort field and then specify the sort order, ascending (A to Z) or descending (Z to A). Sort is available for all fields presented on the active tab, and is applied against all records listed.
3. In the Search Criteria section, select an operator (starts with, equals, is not equal, etc.) and then enter criteria in one or more fields. If a field presents a dropdown list of possible items to search for, such as the Status field, you can select one or many. To select more than one, hold the shift key while clicking for adjacent items or the control key while clicking for non-adjacent items.
4. Click the Run Search button. Only those records that match your search criteria are listed on the active tab, and all records are sorted in the order you specified.

System Setup and Maintenance

Security Managers are responsible for setting up important processes within CitiDirect for their organization. This section describes the features and procedures that enable you, the Security Manager, to complete CitiDirect application setup and maintenance processes.

Security Managers can:

1. Maintain CitiDirect libraries.
2. Customize CitiDirect preferences.
3. Specify internal workflow processes.
4. Define and control user access to specific services and processes.

The Maintenance solution package allows you to work with Library Maintenance to populate and maintain any library to which you have access. The Access Management solution package allows you to work with Access Profiles, Flow Maintenance, User Profiles, Client Preference and User Entitlements. These service classes are discussed below. You need to access these through the Applet page under User Administration.



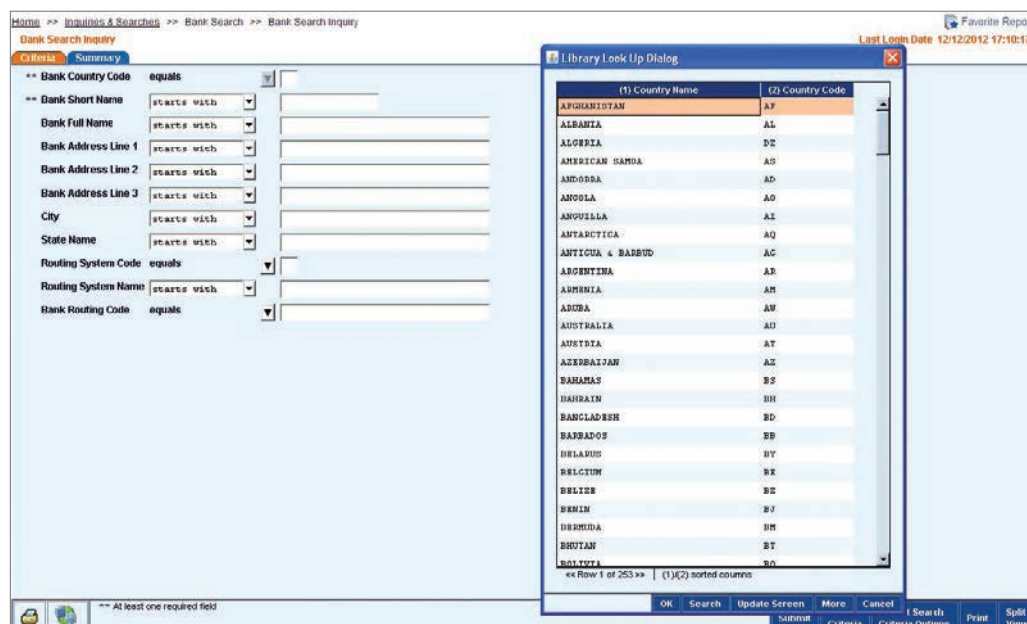
Library Maintenance

Use the Library Maintenance service class to perform the following:

1. View library records.
2. Modify or repair library records.
3. Create library records.
4. Authorize library records.
5. Delete library records.

Libraries provide a means for storing, using, maintaining and managing data. There are several ways that CitiDirect library data can be used. For example, Citi uses libraries to store information that clients can select for input within transactions and reports, and also to support data input, validation and processing rules.

Clients use libraries to store preformatted transaction templates, frequently used text, counterparties for Trade transactions, beneficiary information, payer information, account familiar names, etc. Information stored in libraries appears in library lookup dialogue boxes when the user clicks the library lookup button. This button appears next to all fields that offer a library lookup option.



Notes:

1. When a library contains a single record, the field is automatically populated with that data when the library lookup button is clicked.
2. When a library contains multiple records, a list of all available records appears when the dropdown button is clicked. When information is selected from a library list, all associated relevant information automatically populates the current field and any related fields.
3. Right-click on any summary form or library lookup dialogue list to access the search feature. For more information, refer to the "Searching and Sorting Records" section of this guide.

Benefits of Using Libraries

Use libraries to take advantage of many benefits in CitiDirect:

1. Libraries provide a standardized user experience.
2. Citi and your organization have greater flexibility and more control of data.
3. Libraries reduce or eliminate repetitive typing.
4. Libraries reduce input errors to ensure straight-through processing.
5. Libraries expedite data validation and processing.

Types of Library Data

Library data falls into two categories:

Non-client-specific information: Country codes, currency codes and branch codes that are housed in the database fall into the general information category. Citi maintains these libraries and they provide data that clients can select for input on most CitiDirect forms.

Client-specific information: This includes information such as your organization's account numbers and payment preformats. Based on the type of library and your CitiDirect services, some libraries may be maintained by Citi, your organization or both organizations.

Access to Libraries

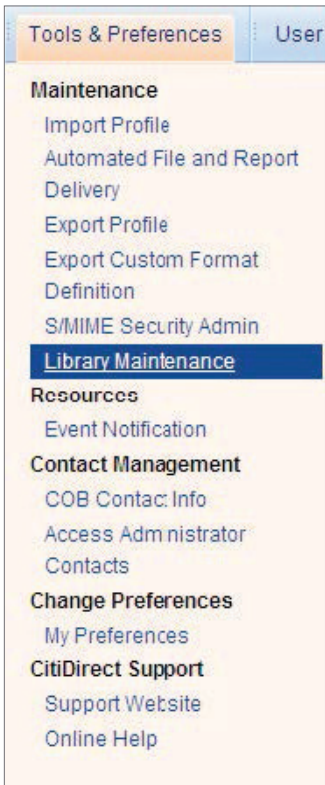
Visibility and access to library records vary depending on the data stored in the library. There are three possible categories that define library access.

Library Type	Description
Private	Ownership of information stored in libraries that are classified as private is restricted to specific high-level users in your organization, such as Security Managers or Treasurers.
Semi-private	Information stored in semi-private libraries is shared across a set of account numbers or client base numbers and branch code combinations that are applicable to your organization via Client Definition. These types of libraries are common for CitiDirect Trade clients. Although local Security Managers or other high-level users typically maintain semi-private libraries, based on the nature of the data in the library, Citi may also assume this responsibility.
Public	Most information is stored in public libraries and is commonly available for reference across clients, accounts, client base numbers and users without any restriction. Although Citi usually maintains public libraries, local Security Managers or other high-level users may be able to add or modify data in some libraries.

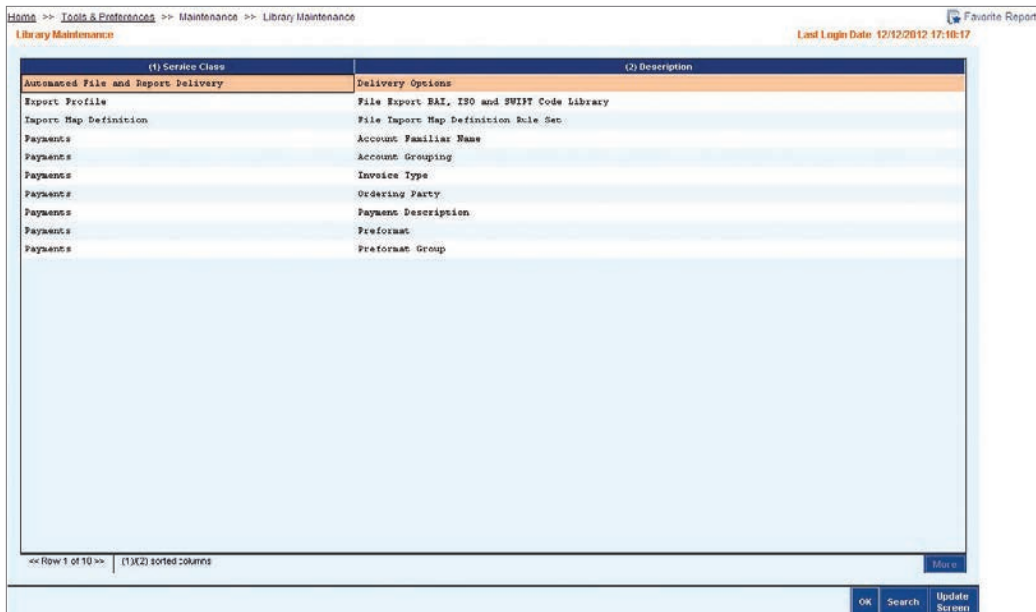
Viewing Library Records

View library records by following the steps below.

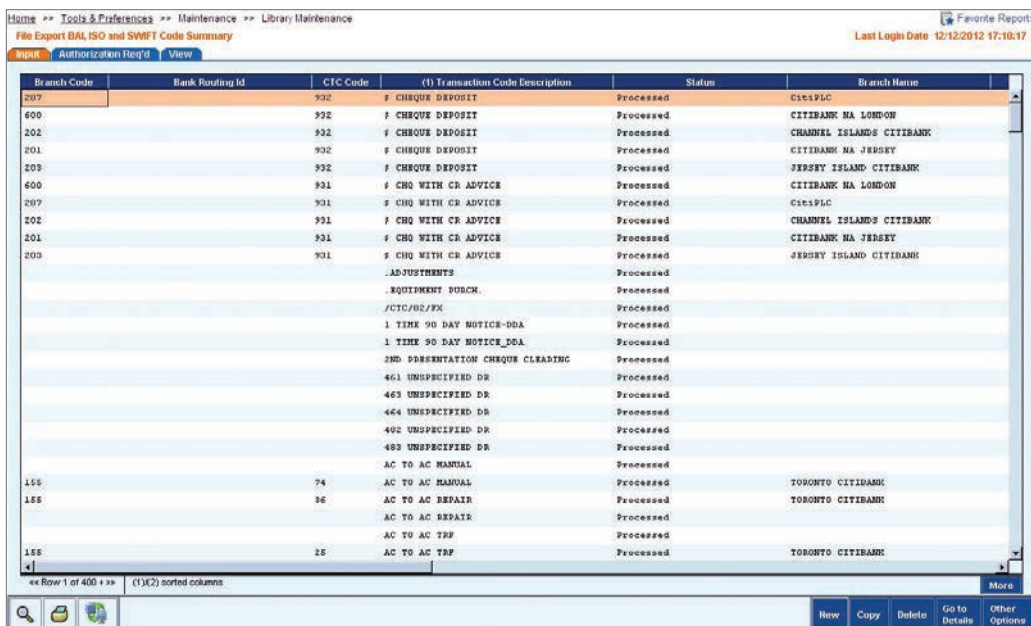
1. On the CitiDirect menu under Tools & Preferences, click on Library Maintenance as shown below.



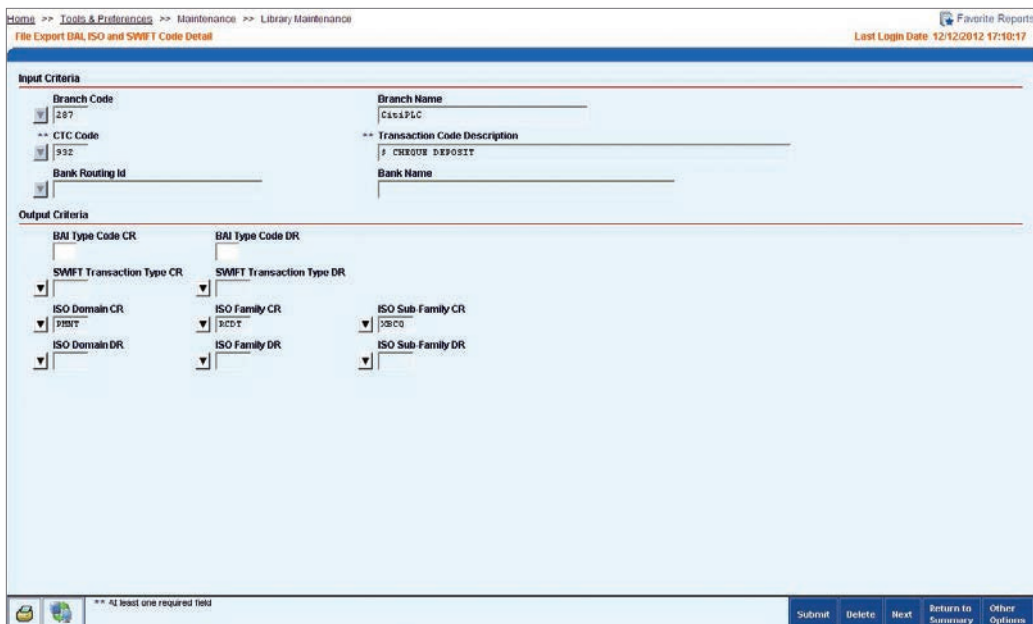
2. The Library Maintenance summary form appears.



3. Select a library and click the OK button. If necessary, use the search feature to find a specific library. The summary form for the select library appears.



4. Select a library record and click the Go to Details button. The library detail form appears. The details of the first selected record are displayed.



Adding Records to a Library

Add a new record to a library by following the steps below:

1. On the CitiDirect menu under Tools & Preferences, click on Library Maintenance as shown below.



2. The Library Maintenance summary form appears.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance Last Login Date: 12/12/2012 17:10:17

Library Maintenance

(1) Service Class	(2) Description
Automated File and Report Delivery	Delivery Options
Export Profile	File Export BAI, ISO and SWIFT Code Library
Export Map Definition	File Export Map Definition Rule Set
Payments	Account Familiar Name
Payments	Account Grouping
Payments	Invoice Type
Payments	Ordering Party
Payments	Payment Description
Payments	Preformat
Payments	Preformat Group

<< Row 1 of 10 >> (1)(2) sorted columns More

OK Search Update Screen

3. Select the appropriate library and then click the OK button. If necessary, use the search feature to find a specific library.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance

File Export BAL ISO and SWIFT Code Summary

Last Login Date 12/12/2012 17:10:17

Input: Authorization Req'd View

Branch Code	Bank Routing Id	CTC Code	(1) Transaction Code Description	Status	Branch Name
207		932	F CHEQUE DEPOSIT	Processed	CITISPLC
600		932	F CHEQUE DEPOSIT	Processed	CITIBANK NA LONDON
202		932	F CHEQUE DEPOSIT	Processed	CHANNEL ISLANDS CITIBANK
201		932	F CHEQUE DEPOSIT	Processed	CITIBANK NA JERSEY
203		932	F CHEQUE DEPOSIT	Processed	JERSEY ISLAND CITIBANK
600		931	F CHQ WITH CR ADVICE	Processed	CITIBANK NA LONDON
207		931	F CHQ WITH CR ADVICE	Processed	CITISPLC
202		931	F CHQ WITH CR ADVICE	Processed	CHANNEL ISLANDS CITIBANK
201		931	F CHQ WITH CR ADVICE	Processed	CITIBANK NA JERSEY
203		931	F CHQ WITH CR ADVICE	Processed	JERSEY ISLAND CITIBANK
			.ADJUSTMENTS	Processed	
			.EQUIPMENT PURCH.	Processed	
			/CTC/02/FX	Processed	
			1 TIME 90 DAY NOTICE-DDA	Processed	
			1 TIME 90 DAY NOTICE_DDA	Processed	
			2ND REPRESENTATION CHECKS CLEARING	Processed	
			461 UNSPECIFIED DR	Processed	
			463 UNSPECIFIED DR	Processed	
			464 UNSPECIFIED DR	Processed	
			492 UNSPECIFIED DR	Processed	
			493 UNSPECIFIED DR	Processed	
			AC TO AC MANUAL	Processed	
155		74	AC TO AC MANUAL	Processed	TORONTO CITIBANK
155		86	AC TO AC REPAIR	Processed	TORONTO CITIBANK
			AC TO AC REPAIR	Processed	
			AC TO AC TRF	Processed	
155		28	AC TO AC TRF	Processed	TORONTO CITIBANK

44 Row 1 of 400 >> (1)(2) sorted columns

More

New Copy Delete Go to Details Other Options

- On the Input tab, click the New button. A blank library detail form for the selected library appears. Some fields use a library lookup to select a predefined entry. Other fields allow free-form text entry.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance

File Export BAL ISO and SWIFT Code Detail

Last Login Date 12/12/2012 17:10:17

Favorite Reports

Input Criteria

Branch Code Branch Name

CTC Code Transaction Code Description

Bank Routing Id Bank Name

Output Criteria

RAI Type Code CR RAI Type Code DR

SWIFT Transaction Type CR SWIFT Transaction Type DR

ISO Domain CR ISO Family CR ISO Sub-Family CR

ISO Domain DR ISO Family DR ISO Sub-Family DR

** At least one required field

Submit Clear Next Return to Summary Other Options

- Complete the form for the library by entering the necessary data.

6. Click the Submit button. A blank detail form appears that enables you to continue entering additional new records into the library.

Modifying or Repairing Library Records

Modify library records by following the steps below:

1. On the CitiDirect menu under Tools & Preferences, click on Library Maintenance as shown below.



2. The Library Maintenance summary form appears.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance Favorite Reports

Library Maintenance Last Login Date 12/12/2012 17:10:17

(1) Service Class	(2) Description
Automated File and Report Delivery	Delivery Options
Export Profile	File Export BAL, ISO and SWIFT Code Library
Import Map Definition	File Import Map Definition Rule Set
Payments	Account Familiar Name
Payments	Account Grouping
Payments	Invoice Type
Payments	Ordering Party
Payments	Payment Description
Payments	Preformat
Payments	Preformat Group

<< Row 1 of 10 >> (1)(2) sorted columns More

OK Search Update Screen

3. Select the library to be modified, and then click the OK button. If necessary, use the search feature to find a specific library. The summary form for the selected library appears.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance Favorite Reports

File Export BAL, ISO and SWIFT Code Summary Last Login Date 12/12/2012 17:10:17

Most Authorization Req'd View

Branch Code	Bank Routing Id	CTC Code	(1) Transaction Code Description	Status	Branch Name
207		932	CHQUE DEPOSIT	Processed	CITIPLC
400		932	CHQUE DEPOSIT	Processed	CITIBANK NA LONDON
202		932	CHQUE DEPOSIT	Processed	CHANNEL ISLANDS CITIBANK
201		902	CHQUE DEPOSIT	Processed	CITIBANK NA JERSEY
203		932	CHQUE DEPOSIT	Processed	JERSEY ISLAND CITIBANK
400		931	CHQ WITH CR ADVICE	Processed	CITIBANK NA LONDON
207		931	CHQ WITH CR ADVICE	Processed	CITIPLC
202		931	CHQ WITH CR ADVICE	Processed	CHANNEL ISLANDS CITIBANK
201		931	CHQ WITH CR ADVICE	Processed	CITIBANK NA JERSEY
203		931	CHQ WITH CR ADVICE	Processed	JERSEY ISLAND CITIBANK
			.ADJUSTMENTS	Processed	
			.EQUIPMENT PURCH.	Processed	
			/CTC/BE/EX	Processed	
			1 TIME 90 DAY NOTICE-DDA	Processed	
			1 TIME 90 DAY NOTICE_DDA	Processed	
			2ND REPRESENTATION CHEQUE CLEARING	Processed	
			461 UNSPECIFIED DR	Processed	
			463 UNSPECIFIED DR	Processed	
			464 UNSPECIFIED DR	Processed	
			492 UNSPECIFIED DR	Processed	
			493 UNSPECIFIED DR	Processed	
			AC TO AC MANUAL	Processed	
155		74	AC TO AC MANUAL	Processed	TORONTO CITIBANK
155		86	AC TO AC REPAIR	Processed	TORONTO CITIBANK
			AC TO AC REPAIR	Processed	
			AC TO AC TRF	Processed	
155		28	AC TO AC TRF	Processed	TORONTO CITIBANK

<< Row 1 of 400 >> (1)(2) sorted columns More

New Copy Delete Go to Details Other Options

4. The Status column on the Input tab indicates the current status of each library, which assists you in which actions to take next.

Status	Description
Processed	The library entry has been authorized and is available for use in the application.
Input	The record has been auto-saved, but not submitted. Additional information is required before it can be submitted for processing.
Invalid	The record or library entry did not pass CitiDirect server validation and must be modified.
Repair Required	Another Security Manager (the authorizer) has determined that the library record contains incorrect information and requires correction.

5. Select the records you want to modify or repair, and then click the Go to Details button. The detail form for the selected library record appears.

Note: If the status of the library record is Invalid or Repair Required, click the Other Options button and then click the View Error Messages command. The Errors dialogue box appears and contains information on why repairs to the record are necessary.

6. Make the necessary modifications to the library record.
7. Click the Submit button. The library record is added to the authorization queue to be authorized by another Security Manager and the next selected record appears.

Notes:

When you modify a library record, another Security Manager must authorize it before it becomes effective. The CitiDirect preferred process for libraries is one level of authorization, requiring a maker-checker setup. You can define up to three levels of authorization for libraries by name. It is recommended that you establish a flow for libraries impacting payments, such as Preformat Group and Preformat (templates). Authorization levels are defined under Flow Maintenance.

Once the library record is modified, two records with the same name exist until the modified record is authorized. The record with the current status of Processed remains in effect until the modified library is authorized. The Service Inquiry Manager service class has only one level of authorization. CitiDirect users responsible for authorizing requests in the Service Inquiry Manager module must be able to authorize any amount.

Authorizing Library Records

Once records have been added to a CitiDirect library, a second Security Manager must authorize each new record to make it available for use in CitiDirect. The Security Manager who created the original record cannot authorize it.

Note: Although you can authorize library records from the Library Maintenance form, it is best to review and validate the records at the detail level as described below.

Authorize library records by following the steps below:

1. On the CitiDirect menu under Tools & Preferences, click on Library Maintenance as shown below.



2. The Library Maintenance summary form appears.



3. Select a library and then click the OK button. If necessary, use the search feature to find a specific library. The summary form for the selected library appears.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance

File Export BAL ISO and SWIFT Code Summary Last Login Date 12/12/2012 17:10:17

Input: Authorization Req'd View

Branch Code	Bank Routing Id	CTC Code	(1) Transaction Code Description	Status	Branch Name
207		932	F CHEQUE DEPOSIT	Processed	CITAPLC
600		932	F CHEQUE DEPOSIT	Processed	CITIBANK NA LONDON
202		932	F CHEQUE DEPOSIT	Processed	CHANNEL ISLANDS CITIBANK
201		932	F CHEQUE DEPOSIT	Processed	CITIBANK NA JERSEY
203		932	F CHEQUE DEPOSIT	Processed	JERSEY ISLAND CITIBANK
600		931	F CHQ WITH CR ADVICE	Processed	CITIBANK NA LONDON
207		931	F CHQ WITH CR ADVICE	Processed	CITAPLC
202		931	F CHQ WITH CR ADVICE	Processed	CHANNEL ISLANDS CITIBANK
201		931	F CHQ WITH CR ADVICE	Processed	CITIBANK NA JERSEY
203		931	F CHQ WITH CR ADVICE	Processed	JERSEY ISLAND CITIBANK
			.ADJUSTMENTS	Processed	
			.EQUIPMENT PURCH.	Processed	
			/CTC/02/FX	Processed	
			1 TIME 90 DAY NOTICE-DDA	Processed	
			1 TIME 90 DAY NOTICE_DDA	Processed	
			2ND REPRESENTATION CHEQUE CLEARING	Processed	
			461 UNSPECIFIED DR	Processed	
			463 UNSPECIFIED DR	Processed	
			464 UNSPECIFIED DR	Processed	
			492 UNSPECIFIED DR	Processed	
			493 UNSPECIFIED DR	Processed	
			AC TO AC MANUAL	Processed	
155		74	AC TO AC MANUAL	Processed	TORONTO CITIBANK
155		86	AC TO AC REPAIR	Processed	TORONTO CITIBANK
			AC TO AC REPAIR	Processed	
			AC TO AC TRF	Processed	
155		26	AC TO AC TRF	Processed	TORONTO CITIBANK

« Row 1 of 400 » (1)(2) sorted columns More

Home Copy Delete Go to Details Other Options

4. Click the Authorization Required tab. All library records awaiting authorization that you are entitled to authorize are listed.

Home >> Tools & Preferences >> Maintenance >> Library Maintenance

PrefORMAT Summary Last Login Date 12/12/2012 17:10:17

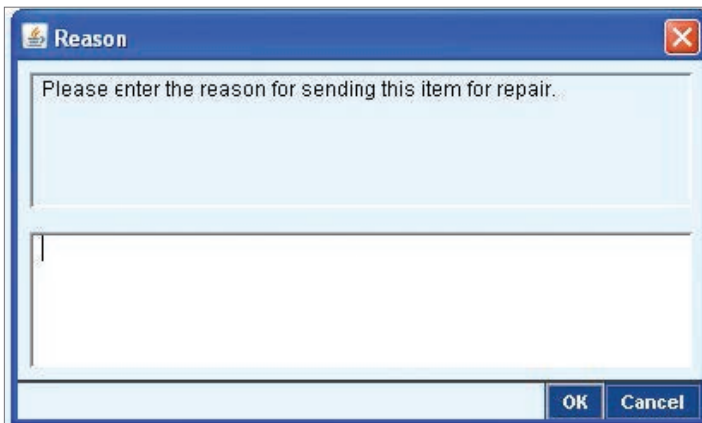
Input: Authorization Req'd View

Beneficiary Name	(1) Preformat Group Code	(2) Preformat Code	Post Method	Status	Last Used Date
PPT TEST	Default	NEW PREFORMAT ACH DEBIT 857 TO...	ACH Debit	Level 1 Authorization Required	
PPT 07/07/2012	Default	NEW PREFORMAT INT PPT 101 TO 057	Book Tran...	Level 1 Authorization Required	
PPT FT 181 TO 857	Default	PREFORMAT FT - 181 TO 857	Funds Tra...	Level 1 Authorization Required	12/08/2012
PPT FT 857 TO 181	Default	PREFORMAT FT - 857 TO 181	Funds Tra...	Level 1 Authorization Required	11/17/2012

« Row 1 of 4 » (1)(2) sorted columns More

Home Authorize Send to Repair Reject Go to Details Other Options

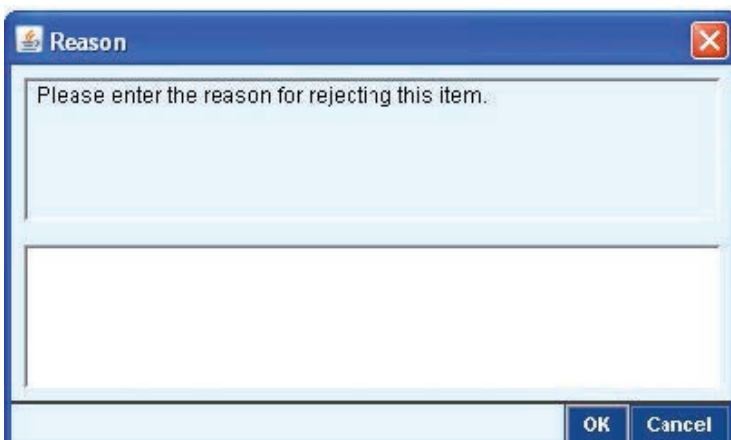
5. Select the record or records that you want to authorize and click the Go to Details button. The detail form for the selected library appears.
6. Review the details of the record and proceed with one of the following steps.
 - Click the Authorize button to authorize the library record. The next selected record appears.
 - Click the Send to Repair button to return the record to the creator for repairs. You can enter a enter reason dialogue box appears.



A screenshot of a Windows-style dialog box titled "Reason". The dialog has a blue title bar with a close button (X) in the top right corner. The main area contains a text input field with the prompt "Please enter the reason for sending this item for repair." Below the input field is a large empty rectangular area for text entry. At the bottom right of the dialog are two buttons: "OK" and "Cancel".

Enter a reason for the repair request, and then click the OK button. The library enters the repair queue. Its status is changed to Repair Required and it is sent to the Input tab for modification by the Security Manager who created it.

- Click the Reject button to delete the selected record. Please enter the reason dialogue box appears.



A screenshot of a Windows-style dialog box titled "Reason". The dialog has a blue title bar with a close button (X) in the top right corner. The main area contains a text input field with the prompt "Please enter the reason for rejecting this item." Below the input field is a large empty rectangular area for text entry. At the bottom right of the dialog are two buttons: "OK" and "Cancel".

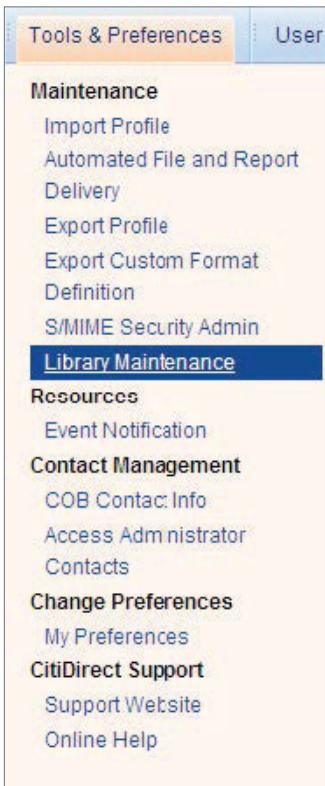
Enter a reason for the rejection, and then click the OK button. The library record is deleted from CitiDirect.

Deleting Library Records

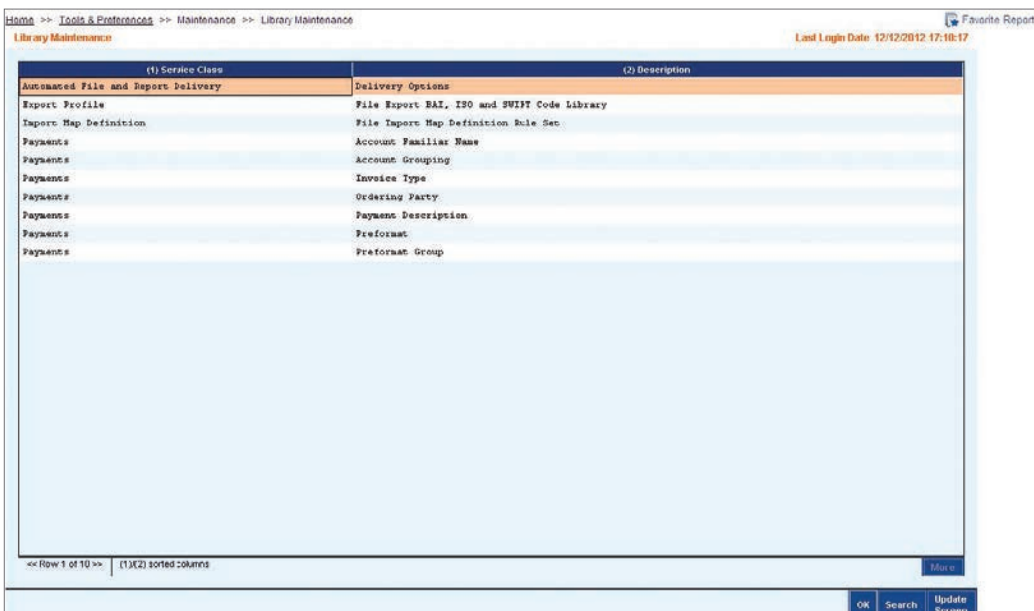
You can delete library records that you have added to libraries. You cannot delete records within Citi-maintained libraries.

Delete library records by following the steps below:

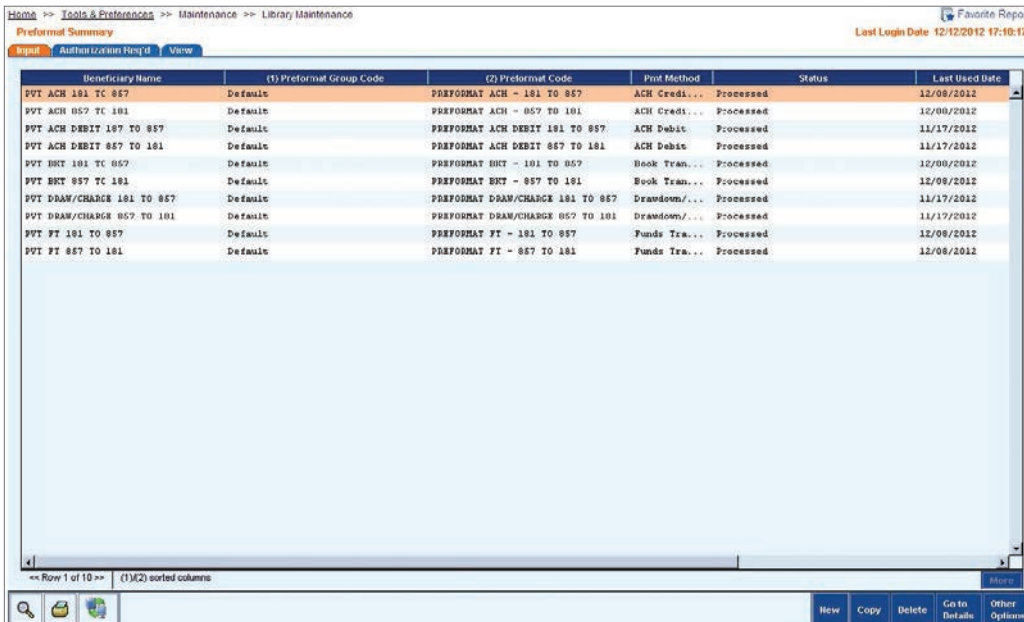
1. On the CitiDirect menu under Tools & Preferences, click on Library Maintenance as shown below.



2. The Library Maintenance form appears.

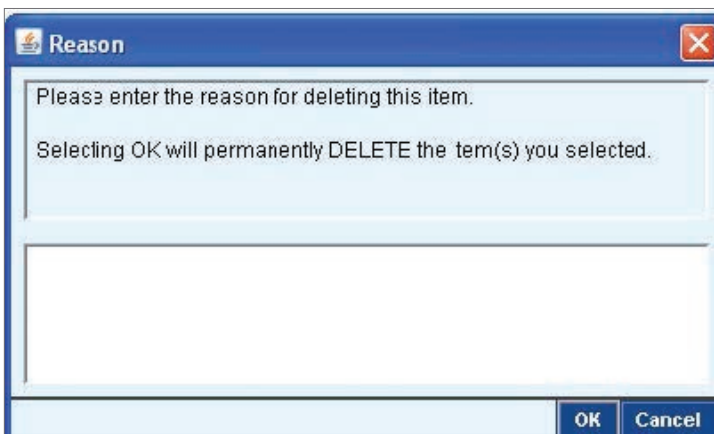


3. Select the library that contains the records you want to delete, and then click the OK button. If necessary, use the search feature to find the desired library. The summary form for the selected library appears.



Beneficiary Name	(1) Preformat Group Code	(2) Preformat Code	Prft Method	Status	Last Used Date
PVT ACH 181 TC 857	Default	PERFORMAT ACH - 181 TO 857	ACH Credi...	Processed	12/08/2012
PVT ACH 857 TC 181	Default	PERFORMAT ACH - 857 TO 181	ACH Credi...	Processed	12/08/2012
PVT ACH DEBIT 181 TO 857	Default	PERFORMAT ACH DEBIT 181 TO 857	ACH Debit...	Processed	11/17/2012
PVT ACH DEBIT 857 TO 181	Default	PERFORMAT ACH DEBIT 857 TO 181	ACH Debit...	Processed	11/17/2012
PVT BKT 181 TC 857	Default	PERFORMAT BKT - 181 TO 857	Book Tran...	Processed	12/08/2012
PVT BKT 857 TC 181	Default	PERFORMAT BKT - 857 TO 181	Book Tran...	Processed	12/08/2012
PVT DRAW/CHARGE 181 TO 857	Default	PERFORMAT DRAW/CHARGE 181 TO 857	Drawdown/...	Processed	11/17/2012
PVT DRAW/CHARGE 857 TO 181	Default	PERFORMAT DRAW/CHARGE 857 TO 181	Drawdown/...	Processed	11/17/2012
PVT FT 181 TO 857	Default	PERFORMAT FT - 181 TO 857	Funds Tra...	Processed	12/08/2012
PVT FT 857 TO 181	Default	PERFORMAT FT - 857 TO 181	Funds Tra...	Processed	12/08/2012

4. On the Input tab, select the library record you want to delete, and then click the Delete button. A dialogue box appears.



Reason

Please enter the reason for deleting this item.

Selecting OK will permanently DELETE the term(s) you selected.

OK Cancel

5. Enter a reason for the deletion, and then click the OK button. A dialogue box appears confirming the deletion.
6. Click the OK button to close the dialogue box. The status of the library record changes to Authorization Required for Delete. Library deletions require authorization by another Security Manager before they take effect.

Client Preferences

Use the Client Preference service class to perform the following:

- View client preference settings.
- Modify or repair client preference settings.
- Authorize client preference settings.

Client preferences are CitiDirect-defined or customized settings for CitiDirect forms, such as transaction Prefix ID, auto-save frequency and base currency. Use the Client Preference service class to maintain and modify client preference settings to suit the needs of your organization.

As Security Manager, you should first view your CitiDirect predefined (default) client preference settings to determine whether or not they should be changed to best meet your organization's needs. You should only modify settings if required.

The table below lists some examples of Payments client preferences.

Available Criteria	Preferences Options	
Transaction Reference	Full Auto	Prefix Auto
	Manual	Prefix ID
Edit	Transaction Charges	Company
	Debit Account	Base Currency
	Credit Account	Priority Mode
	Ordering Party	Delivery Mode
Auto Save	Auto-Save Frequency	Auto-Save Type
Field Level Verification	Debit Party Name	Value Date Beneficiary
	Name	Account Number
	Payment Currency	Beneficiary Account
	Payment Account	Other ID

Viewing Client Preferences

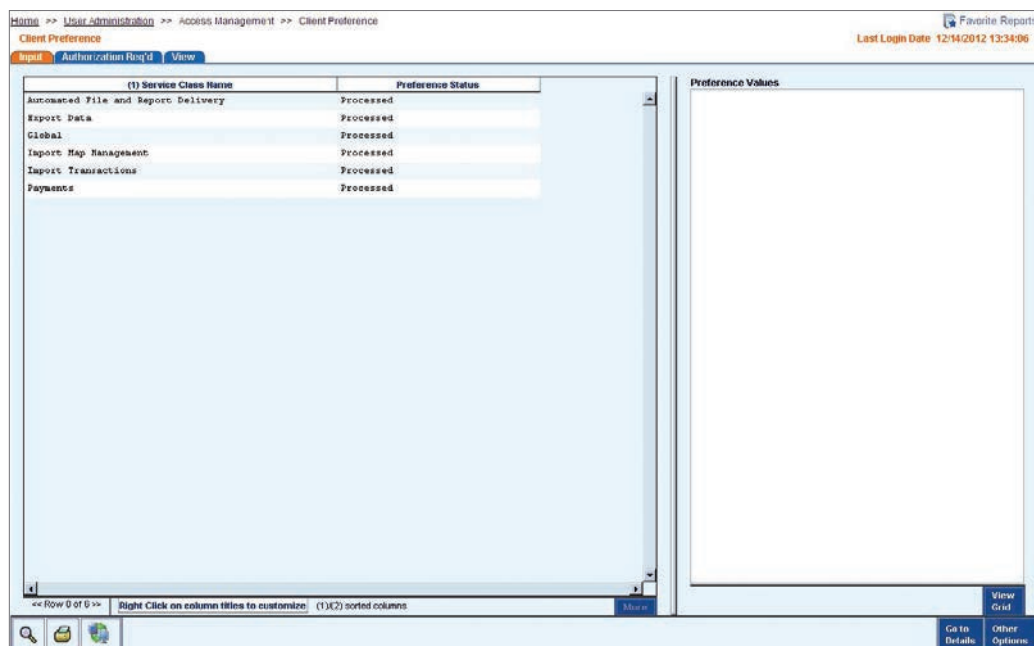
When CitiDirect is installed, some client preferences are predefined (set as default). Review these CitiDirect-defined settings with your local Implementation Manager to determine which, if any, need modification for your business needs.

View client preference settings by following the steps below.

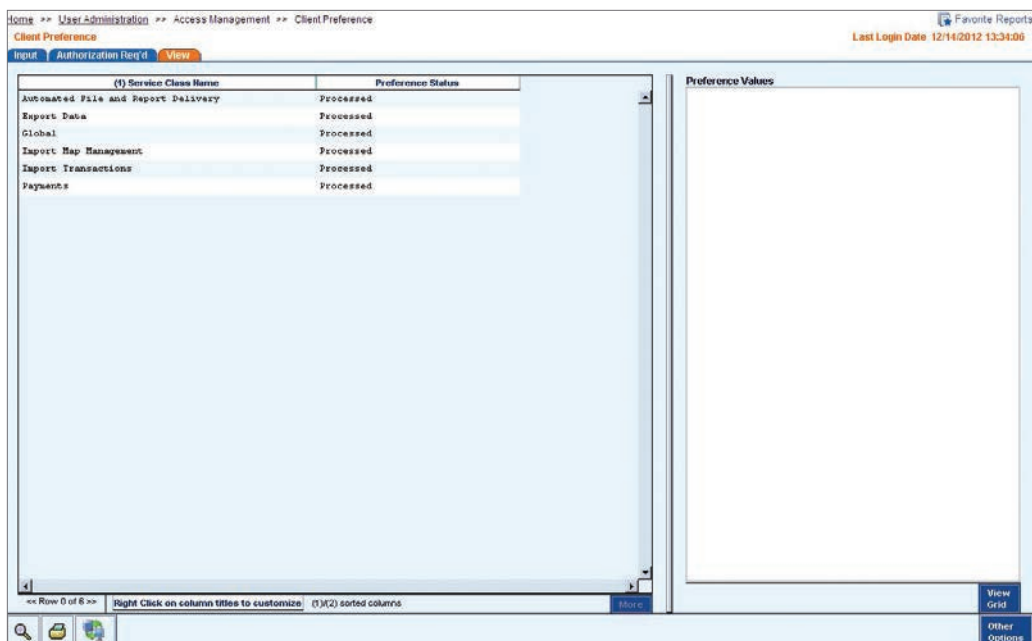
1. On the CitiDirect menu under User Administration, click on Client Preference as shown below.



2. The Client Preference form appears.



3. Click the View tab.
4. Select the service class you want to view. The current client preference settings for the selected service class appear in the Preference Values list box.



Notes:

In the Preference Values list, a value of None Specified indicates that there are no preferences (defaults) for the value listed.

If a value is listed as See Grid for Details, select it, and then click the View Grid button to see all details. This message appears if there are more preferences for a value than can be displayed on the screen.

Modifying or Repairing Client Preferences

Citibank has defined common application defaults that you need to modify only if other selections (values) better meet your organization's business needs. If you modify client preferences, another Security Manager must authorize them.

The Status column on the Input tab indicates the current status of each client preference and assists you in determining what action, if any, is needed.

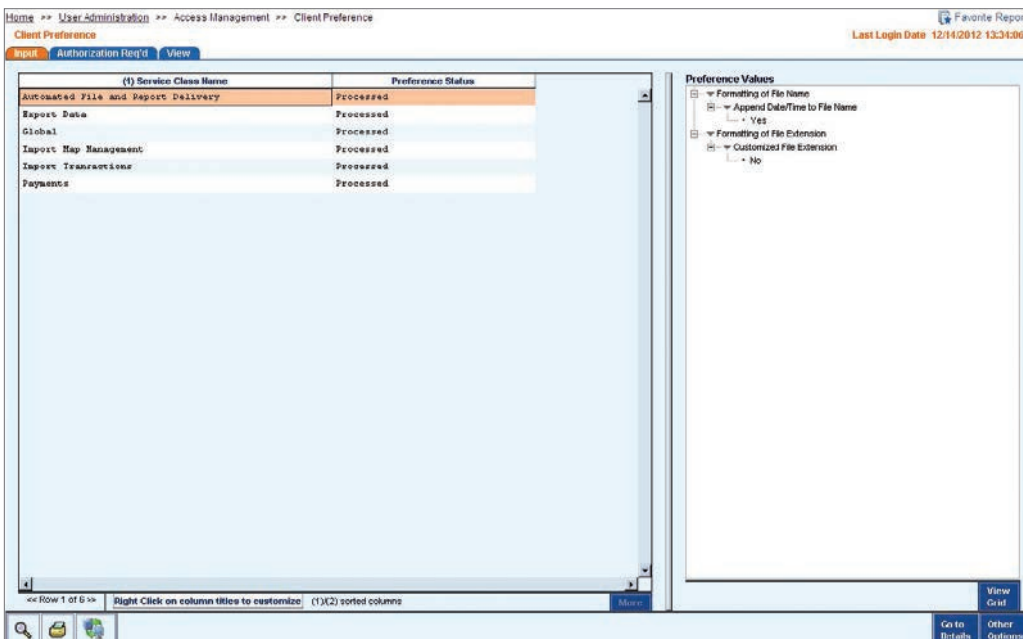
Status	Description
Processed	The client preference setting has been authorized and is available for use in the application.
Input	The record has been auto-saved, but not submitted. Additional information is required before it can be submitted for processing.
Invalid	The profile did not pass CitiDirect server validation and must be modified.
Repair Required	Another Security Manager (the authorizer) has determined that the client preference setting contains incorrect information or requires correction.

Modify or repair client preference settings by following the steps below:

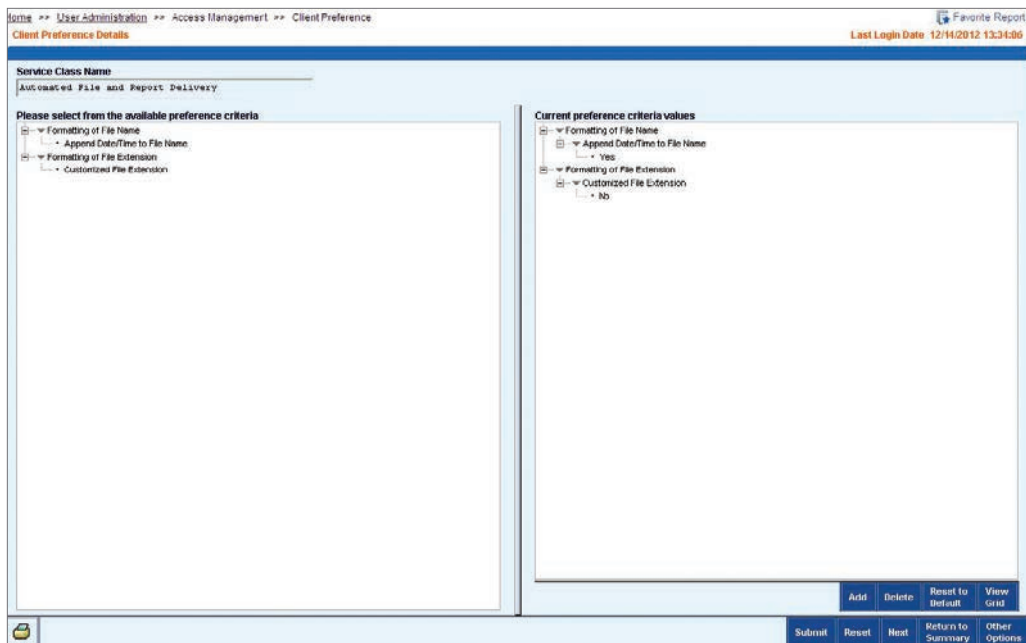
1. On the CitiDirect menu under User Administration, click on Client Preference as shown below.



2. The Client Preference form appears.

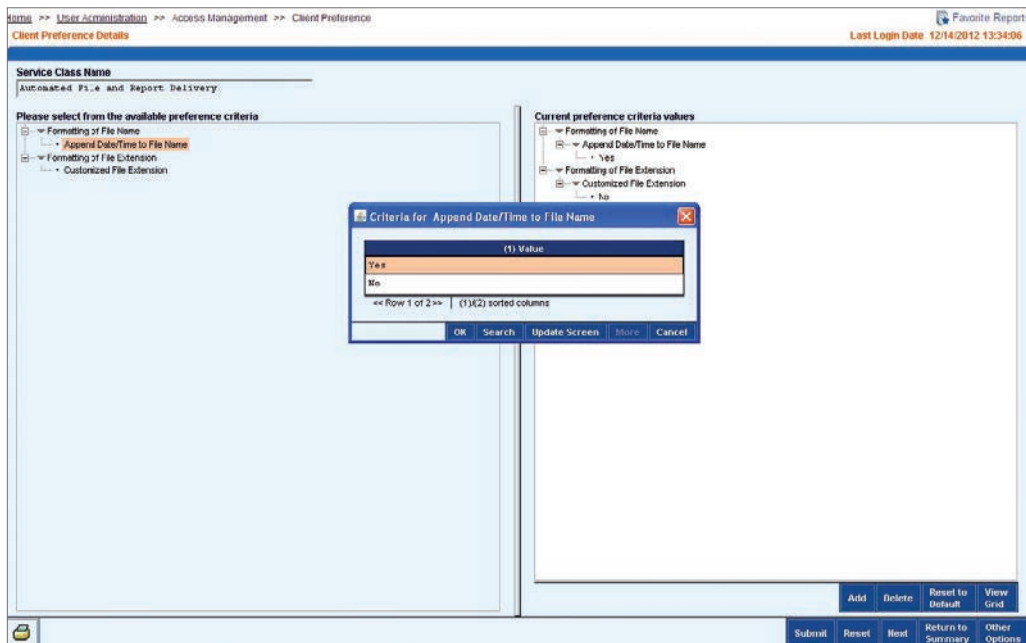


3. On the Input tab, select the service class you want to modify or repair, and click the Go to Details button. The Client Preference Details form for the selected service class appears.



4. Proceed with one of the following steps.

- To define criteria, select a criterion from the Please select from the available preference criteria list box on the left. A Criterion dialogue box appears. The choices in the dialogue box vary based on the criterion selected.



Select the preference value you want and click the OK button. The new value appears in the Current preference criteria values list box on the right.

- To reset the values to previously saved criteria, click the Reset button.
 - To reset criteria values to the CitiDirect-defined preferences, if any, select the criteria values and click the Reset to Default button.
5. Review the Preference Values list box for accuracy and click the Submit button. The original client preference settings status is Processed and it remains active until the modified settings are authorized.

Notes:

For client preferences with a Repair Required or Invalid status, click the Other Options button, and then click the View Error Messages command to see the reason for the necessary modifications.

A client preference record with the status of Processed is active.

Two client preference records for the selected service class exist until another Security Manager authorizes the modified settings: the original with a Processed status and the modified record with an Authorization Required status. Once the modified client preference record is authorized, the original, previous preference is removed.

Authorizing Client Preferences

Once client preferences have been modified and submitted, they need to be authorized. Before authorization, the original processed preference is active and will remain active until authorization is complete. Once authorization is complete, changes to the client preference settings are active.

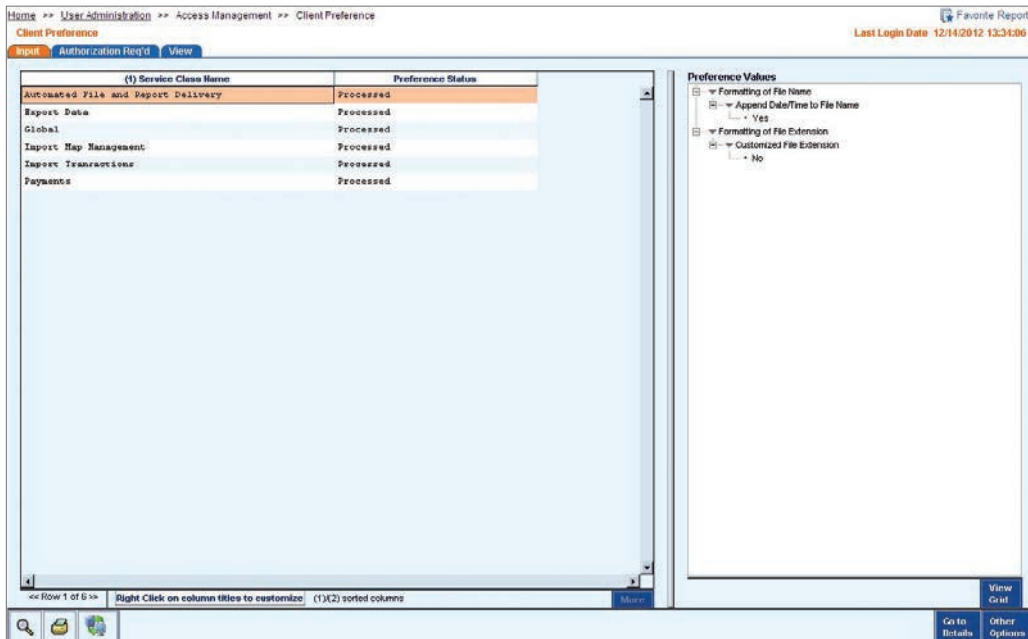
If you modified the client preference setting, you cannot authorize it. During the authorization process, client preferences can be authorized, rejected (deleted) or returned for repair.

Authorize a client preference setting record by following the steps below:

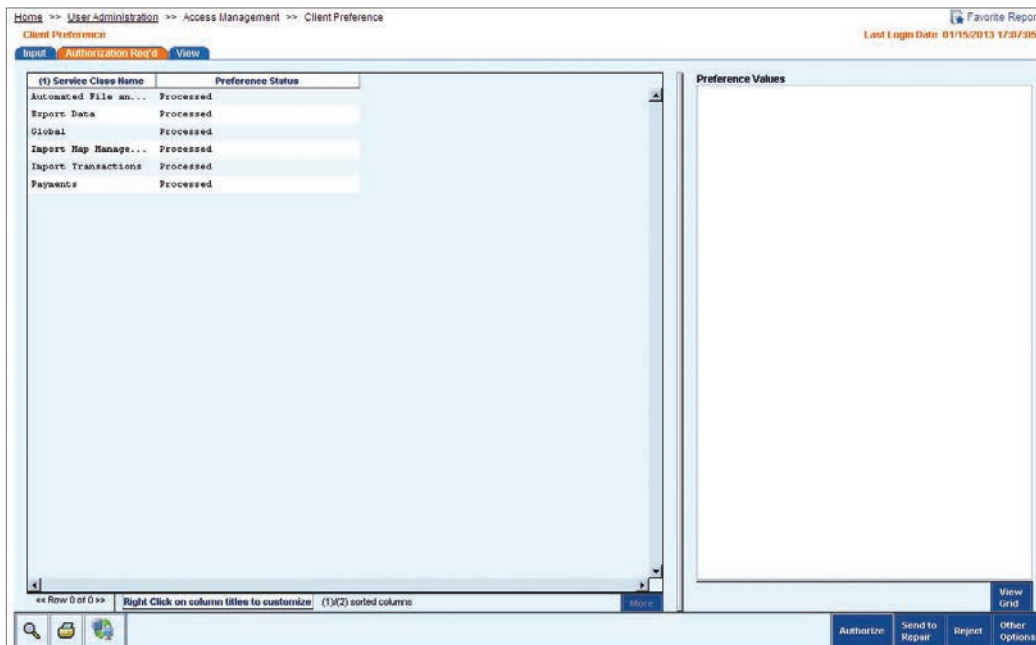
1. On the CitiDirect menu under User Administration, click on Client Preference as shown below.



2. The Client Preference form appears.

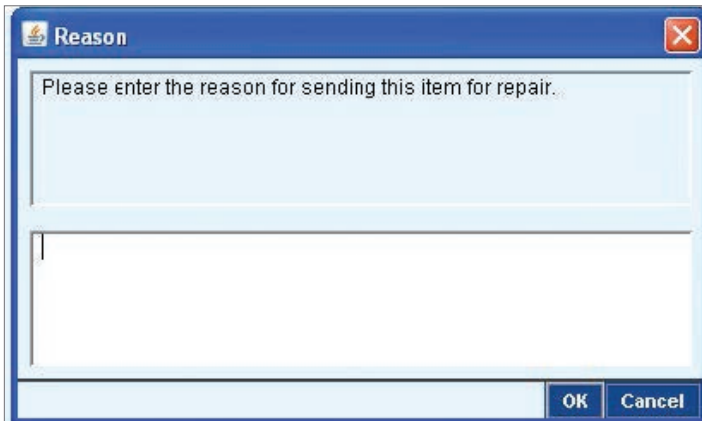


3. Click the Authorization Required tab. All client preference records with an Authorization Required status that you are entitled to authorize are listed.
4. Click a service class to select the client preference record you want to authorize. The client preference settings for the selected service class appear in the Preference Values list box.



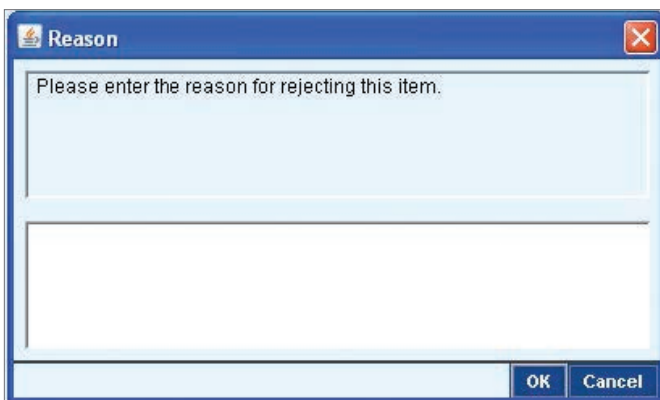
5. Proceed with one of the following steps.

- Click the Authorize button. A dialogue box appears indicating that the preference has been processed. Click the OK button to close the dialogue box.
- Click the Send to Repair button. A dialogue box entitled Reason appears.



Enter a reason for the repair and click the OK button. The preference record is sent to the Input tab and its status is changed to Repair Required. The initiator of the record must make the necessary changes and resubmit it.

- Click the Reject button to delete the client preference record if it is invalid or violates your organization's business rules. A dialogue box appears.



Enter a reason for the rejection and click the OK button. The client preference record is deleted from the application.

Flow Maintenance

Use the Flow Maintenance service class to perform the following:

1. View current flow controls.
2. Modify or repair flow controls.
3. Create new flow controls.
4. Authorize flow controls.
5. Delete flow controls.

Through the Flow Maintenance service class, you can control the flow of your organization's processes within CitiDirect. Flow maintenance enables you to quickly and efficiently specify the workflow that transactions, service requests and libraries must follow before they can be processed. For example, your organization may require more stringent controls for an outgoing payment of \$1,000,000 than for a payment of \$1,000.

As a Security Manager, you should first view your CitiDirect-default flow controls, and determine whether or not they should be changed to best meet your organization's needs. You should modify the predefined flow controls only if required.

Notes:

Flow controls are implemented at the client definition level and apply to all CitiDirect users within your organization.

For any criteria that are not defined, CitiDirect defaults to All.

It is recommended that any changes to flow maintenance be done after end-of-day processing is completed. All changes should be validated before the next processing date.

Flow controls can also apply to non-transactions such as libraries. For more information on libraries, refer to the "Library Maintenance" section of this guide.

Viewing Current Flow Controls

The View tab on the Flow Maintenance Summary form is best used to examine all flow controls and their current status. All flow controls are composed of input and output criteria. The input criteria allow you to define the limits of the data entered into the application. The output criteria define the levels of authorization required to release the item to a Citi back-end for processing.

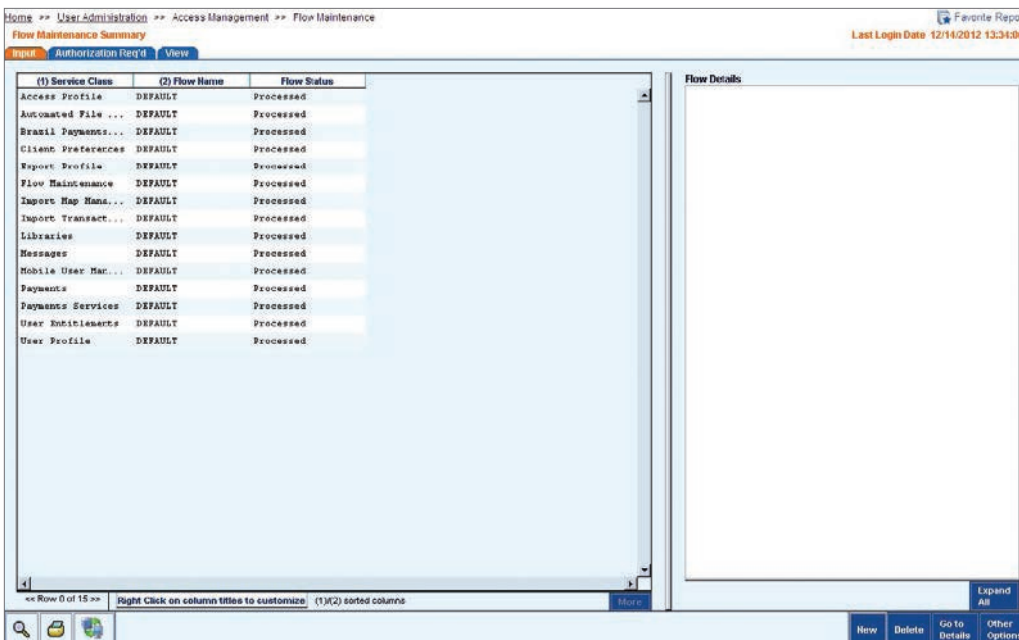
Status	Description
Criteria Type	Allows you to manage your workflow by specifying requirements for how transactions and library records are entered into CitiDirect. Available input criteria differ depending on service class. For example, account, amount, creation method, payment currency, payment method, payment type and processing location are some input criteria for Payments. Trade service types and amounts are examples of input criteria for Trade Services.
Input	The procedure, process or transaction flow that must happen before the data entered into CitiDirect by your users (input criteria) can be sent to Citibank for processing. For example, payments that fall within a specified amount range (input criteria) require authorization by another user before they can be processed. Examples of output criteria include verification required, level of authorization, number of authorizers and release.

View current flow controls by following the steps below:

1. On the CitiDirect menu under User Administration, click on Flow Maintenance as shown below.



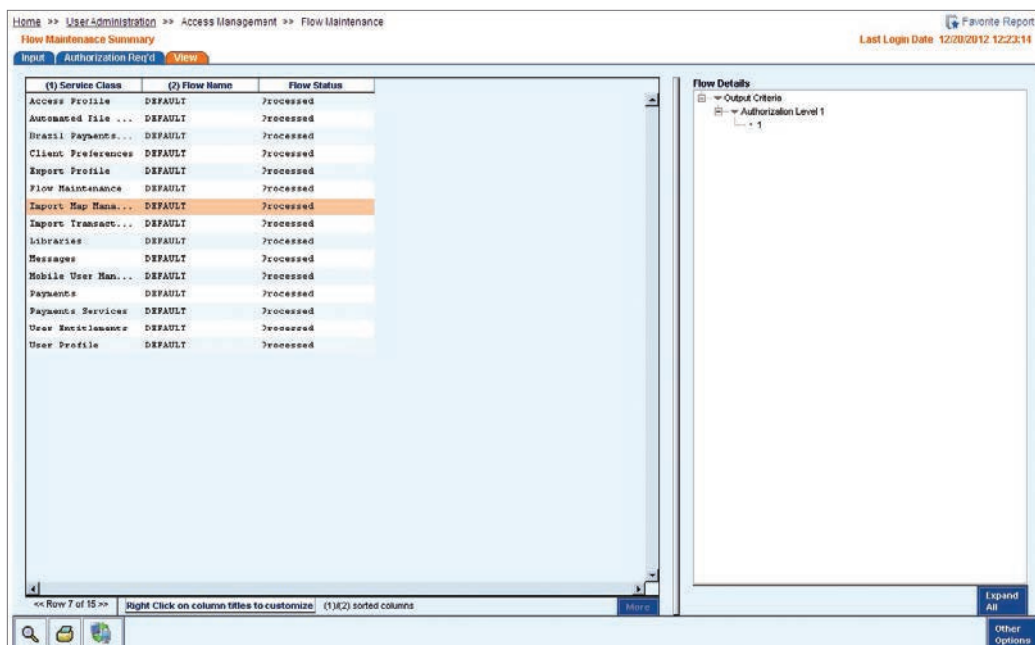
2. The Flow Maintenance Summary form appears. When you first access CitiDirect, only the CitiDirect defined flow controls appear.



3. Click the View tab. All flow controls appear regardless of their status.

Note: CitiDirect predefined flows appear within the Flow Name column as DEFAULT.

4. Select a flow control. The associated input and output criteria appear in the Flow Details box on the right. If you select more than one flow control, the Flow Details list box is empty.



(1) Service Class	(2) Flow Name	Flow Status
Access Profile	DEFAULT	Processed
Automated File ...	DEFAULT	Processed
Brasil Payments...	DEFAULT	Processed
Client Preferences	DEFAULT	Processed
Export Profile	DEFAULT	Processed
Flow Maintenance	DEFAULT	Processed
Import Map Mana...	DEFAULT	Processed
Import Transact...	DEFAULT	Processed
Libraries	DEFAULT	Processed
Messages	DEFAULT	Processed
Mobile User Man...	DEFAULT	Processed
Payments	DEFAULT	Processed
Payments Services	DEFAULT	Processed
User Maintenance	DEFAULT	Processed
User Profile	DEFAULT	Processed

In the flow control example above, the output criteria calls for all Payments to be authorized by a level 1 authorizer before they can be released for processing.

Modifying or Repairing Flow Controls

You can modify flow controls to better meet your business needs. All flow controls with an Input, Invalid or Repair Required status must be repaired before they can be authorized. The Status column on the Input tab indicates the current status of each flow and assists you in determining what action, if any, is needed.

Status	Description
Processed	The flow has been authorized, and is currently being used in the application.
Input	The record has been auto-saved, but not submitted. Additional information is required before it can be submitted for processing.
Invalid	The profile did not pass CitiDirect server validation and must be modified.
Repair Required	Another Security Manager (the authorizer) has determined that the flow contains incorrect information and/or requires correction.

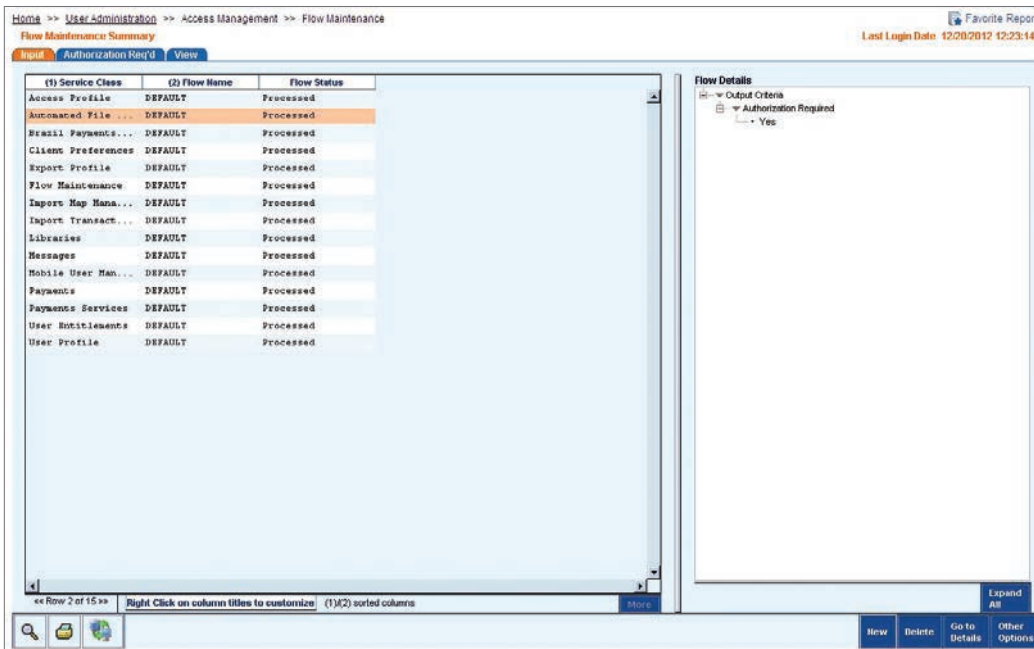
Note: For any criteria that are not defined, CitiDirect defaults to All. For example, if you do not specify a currency when you are specifying flow controls for Payments, the flow controls are applied to payments in all currencies.

Modify or repair flow controls by following the steps below:

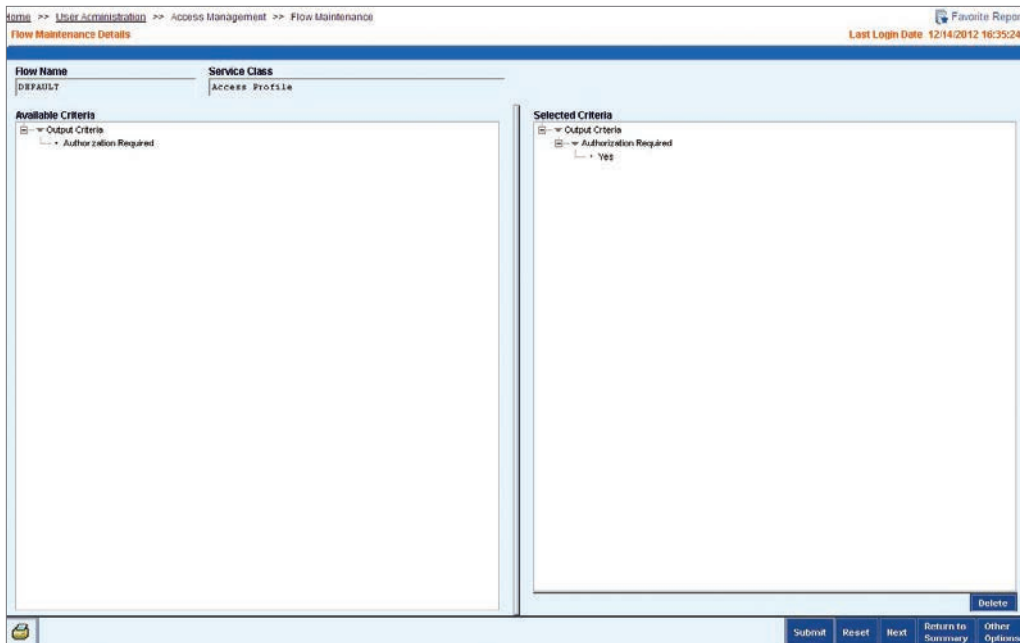
1. On the CitiDirect menu under User Administration, click on Flow Maintenance as shown below.



2. The Flow Maintenance Summary form appears. All flows with a status of Input, Invalid, Process or Repair Required are listed.

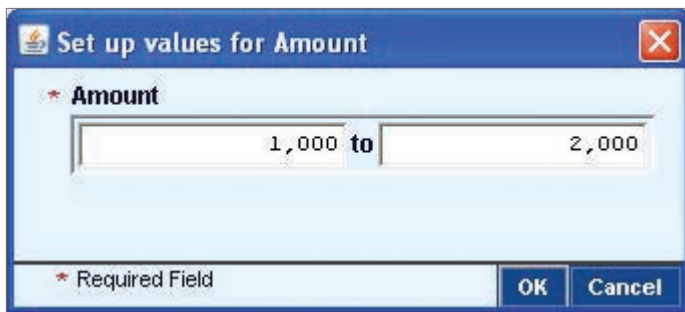


3. On the Input tab, select the flow you want to modify.
4. Click the Go to Details button. The Flow Maintenance Details form appears. The Available Criteria and the Selected Criteria for the first selected flow are displayed.



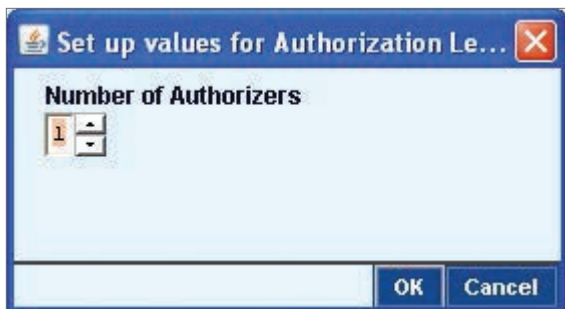
5. Proceed with one of the following steps:

- To add input criteria, select the criteria from the Available Criteria list as shown in the below screen. If you click on any of the Criteria, another dialogue box with different setup values will appear.



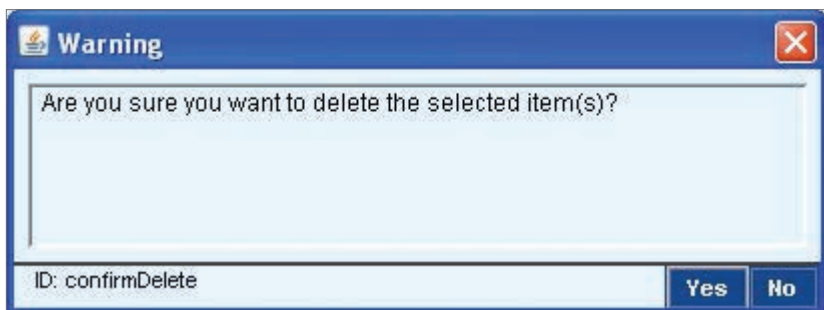
Select the value you want to add and then click the OK button.

- To add output criteria, select the criteria from the Available Criteria list box on the left. A Set up values for dialogue box appears.



Select the value you want to add and then click the OK button.

- To delete criteria, select the criteria that you want to delete from the Selected Criteria list box on the right, and click the Delete button. A warning message appears.



Click the Yes button to confirm the deletion.

- To reset criteria to their previously saved settings, click the Reset button. All of the criteria return to their previously saved settings.
6. Review the Selected Criteria list box for accuracy and click the Submit button. The Save As dialogue box appears.



7. Click the OK button to save the modified flow control with the same name.

Notes:

If you enter a new name, two flow controls will exist – the original and the modified/repared flow. The status of the modified flow control is changed to Authorization Required and it is added to the authorization queue. Another Security Manager must authorize the modification before it becomes active.

The current flow control remains active until the modified control is authorized.

Creating New Flow Controls

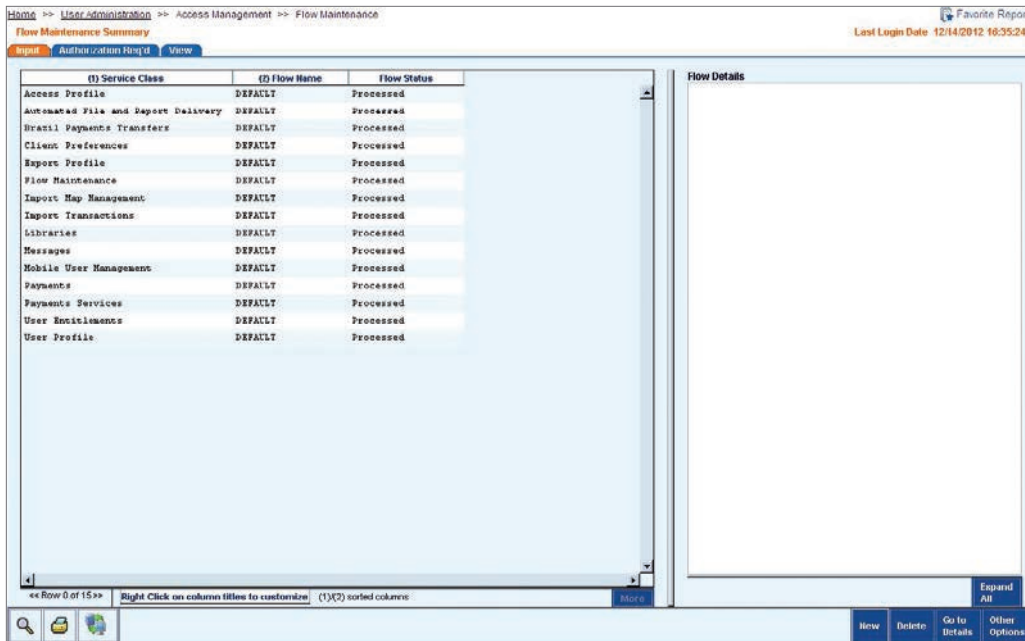
CitiDirect enables you to control the workflow processes in your organization. Flow controls are established by specifying a set of transactions, service requests and library records, and then assigning controls to them.

Create new flow controls by following the steps below.

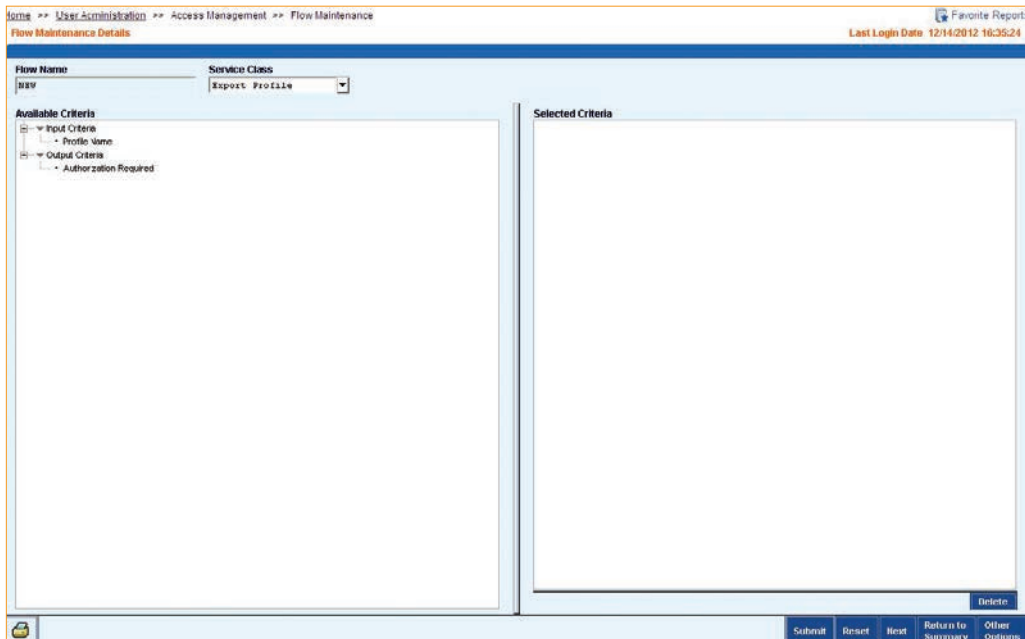
1. On the CitiDirect menu under User Administration, click on Flow Maintenance as shown below.



2. The Flow Maintenance Summary form appears. Select the Input tab, if necessary. The Input tab is the starting point for creating new flow control profiles.



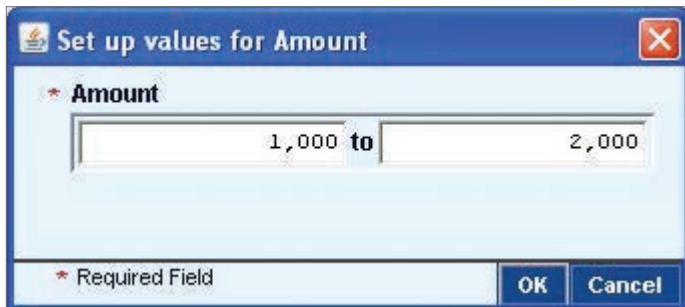
3. Click the New button. The Flow Maintenance Details form appears.



4. In the Service Class field, click the dropdown arrow and select the desired service class.

5. Proceed with one of the following steps:

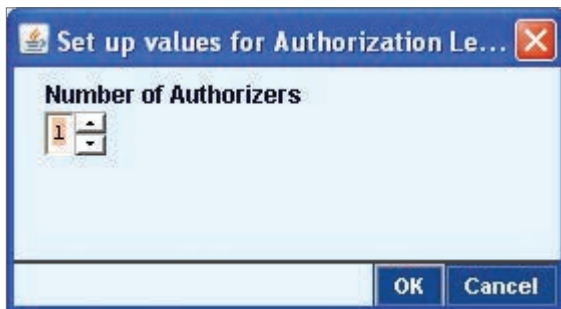
- In the Available Criteria list box, select an input criterion. A Set up values for dialogue box appears. The dialogue box varies based on the criterion selected.



The dialog box titled "Set up values for Amount" has a blue header with a close button. Below the header, the text "* Amount" is displayed. A text input field contains the value "1,000 to 2,000". At the bottom left, there is a label "* Required Field". At the bottom right, there are two buttons: "OK" and "Cancel".

Enter the values as required and click the OK button. The value appears under the Input criteria section in the Selected Criteria list box.

- In the Available Criteria list box, select an output criterion. A Set up values for dialogue box appears.



The dialog box titled "Set up values for Authorization Le..." has a blue header with a close button. Below the header, the text "Number of Authorizers" is displayed. A spinner control shows the value "1". At the bottom right, there are two buttons: "OK" and "Cancel".

Select the value and click the OK button. The value appears under the Output Criteria section in the Selected Criteria list box.

- To clear all criteria in the Selected Criteria list box, click the Reset button.
- To clear an individual criterion, select the criterion and click the Delete button.

6. Review the Selected Criteria list box for accuracy and click the Submit button. The Save As dialogue box appears.



The dialog box titled "Save As" has a blue header with a close button. Below the header, the text "* Flow Name" is displayed. A text input field contains the value "New Payment Flow". At the bottom left, there is a label "* Required Field". At the bottom right, there are two buttons: "OK" and "Cancel".

7. Enter the flow name and click the OK button. The status of the newly created flow control is changed to Authorization Required and is not applied until another Security Manager authorizes it.

Notes:

A flow status of Processed is an active flow control.

All flow controls that you define take precedence over the CitiDirect-defined flow controls.

If you specify that multiple levels of authorization are required before transactions can be processed, the access profiles assigned to the CitiDirect users responsible for authorizing those transactions must have authorization rights at the specified levels.

Applying Flow Controls: Base Currency

To determine the correct amount when applying transaction flow controls, the transaction amount is converted to your base currency. CitiDirect Online Banking uses the following currency conversion logic, which is commonly available across service classes:

1. If the base currency is USD and the transaction amount is not USD, the transaction amount is converted to USD.
2. If the base currency is not USD and the transaction amount is USD, the transaction amount (USD) is converted to the base currency.
3. If both the base currency and transaction amount are not USD, the amount is converted to USD, and then from USD to the base currency amount.
4. If the transaction currency is the same as the base currency, no currency conversion is required.

Authorizing Flow Controls

Any new or modified flow controls must be authorized before they take effect. If you created or modified a flow control, you cannot authorize it. During the authorization process, flow controls can be authorized or rejected.

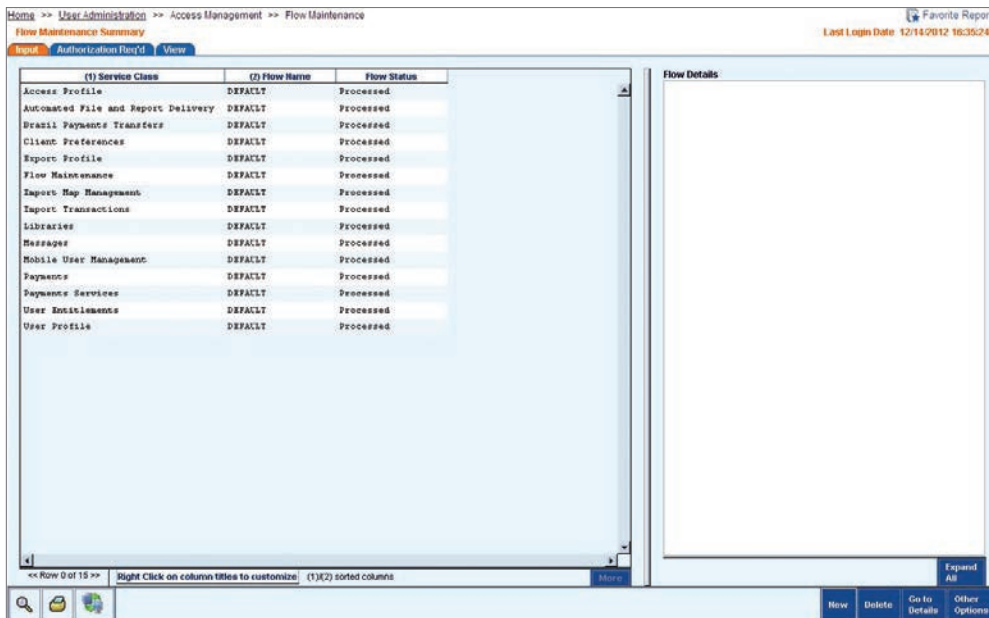
Note: It is recommended that any changes to flow maintenance be done after end-of-day processing is completed. All changes should be validated before the next process date.

Authorize flow controls by following the steps below:

1. On the CitiDirect menu under User Administration, click on Flow Maintenance as shown below.



2. The Flow Maintenance Summary form appears.



Home >> User Administration >> Access Management >> Flow Maintenance

Flow Maintenance Summary Favorite Reports

Last Login Date: 12/14/2012 16:35:24

Search: Authorization Flow ID View

(1) Service Class	(2) Flow Name	Flow Status
Access Profile	DEFAULT	Processed
Automated File and Report Delivery	DEFAULT	Processed
Brasil Payments Transfers	DEFAULT	Processed
Client Preferences	DEFAULT	Processed
Export Profile	DEFAULT	Processed
Flow Maintenance	DEFAULT	Processed
Import Map Management	DEFAULT	Processed
Import Transactions	DEFAULT	Processed
Libraries	DEFAULT	Processed
Messages	DEFAULT	Processed
Mobile User Management	DEFAULT	Processed
Payments	DEFAULT	Processed
Payments Services	DEFAULT	Processed
User Entitlements	DEFAULT	Processed
User Profile	DEFAULT	Processed

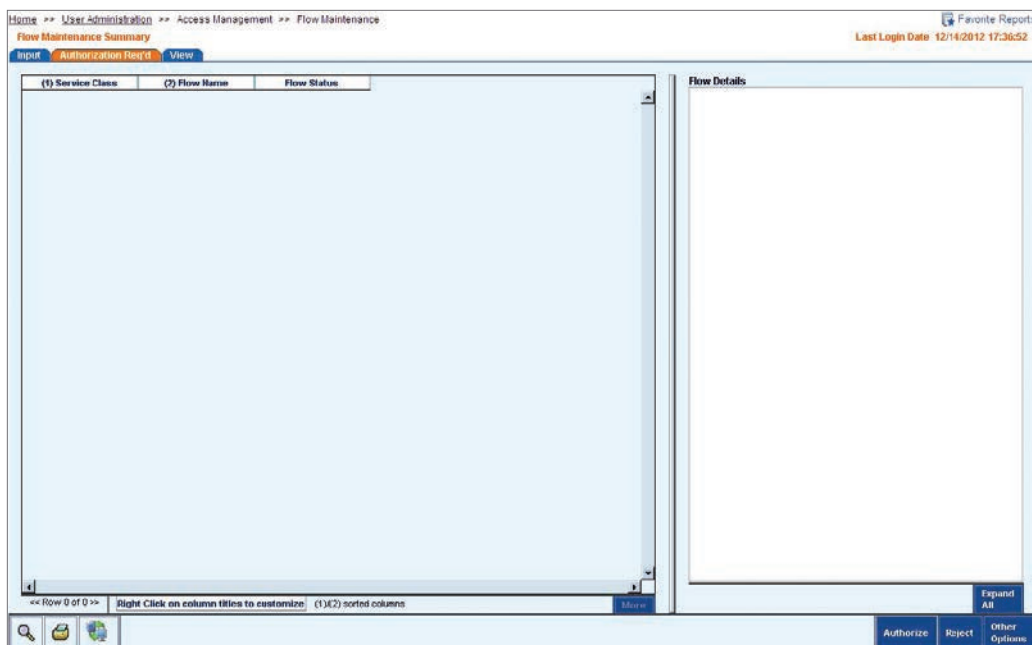
Flow Details

<< Row 0 of 15 >> Right Click on column titles to customize: (1)(2) sorted columns

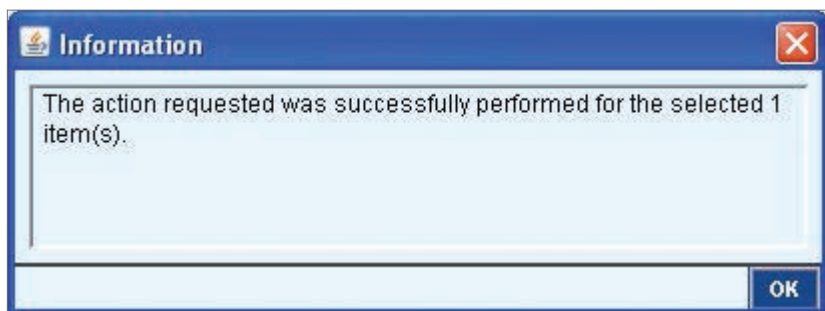
Expand All

New Delete Go to Details Other Options

3. Click the Authorization Required tab. The list of flow controls that you are entitled to authorize appears.



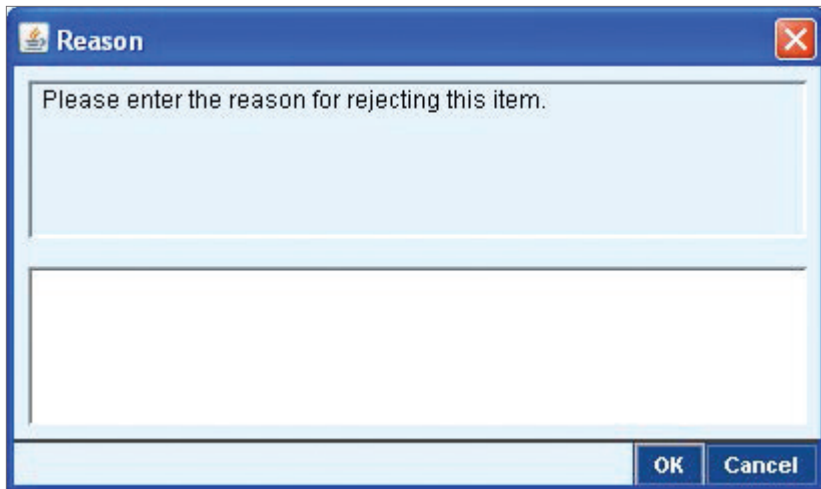
4. Select the flow control you want to authorize. For authorizing the flow controls, select each of them individually. The input and output criteria appear in the Flow Details list box.
5. Proceed with one of the following steps:
 - Click the Authorize button to authorize the selected flow. An information box appears.



Click the OK button to close the box. The flow control is active and its status is updated to Processed.

- Click the Reject button to delete the flow control. A dialogue box appears as "Are you sure you want to reject this flow?"

Click the Yes button. Another dialogue box appears.



Enter the reason for the rejection and click the OK button. The flow is deleted from CitiDirect and an information box confirms the deletion.

Notes:

For Payments and Trade transactions, CitiDirect Online Banking allows you to specify up to nine levels of authorization, with up to nine authorizations at each level. For example, a flow control can be set to require that all payments made over \$10,000 in any or all currencies be authorized by two people: one person at Authorization Level 1 and one person at Authorization Level 2.

If you are requiring multiple levels of authorization, make sure that the authorizers have that level of authorization in their access profiles. Authorization levels are required in ascending order. For example, Level 2 is a higher level of authorization than Level 1.

Payments that do not have at least one level of authorization will require the maker to approve the payment after it is submitted for processing.

Deleting Flow Controls

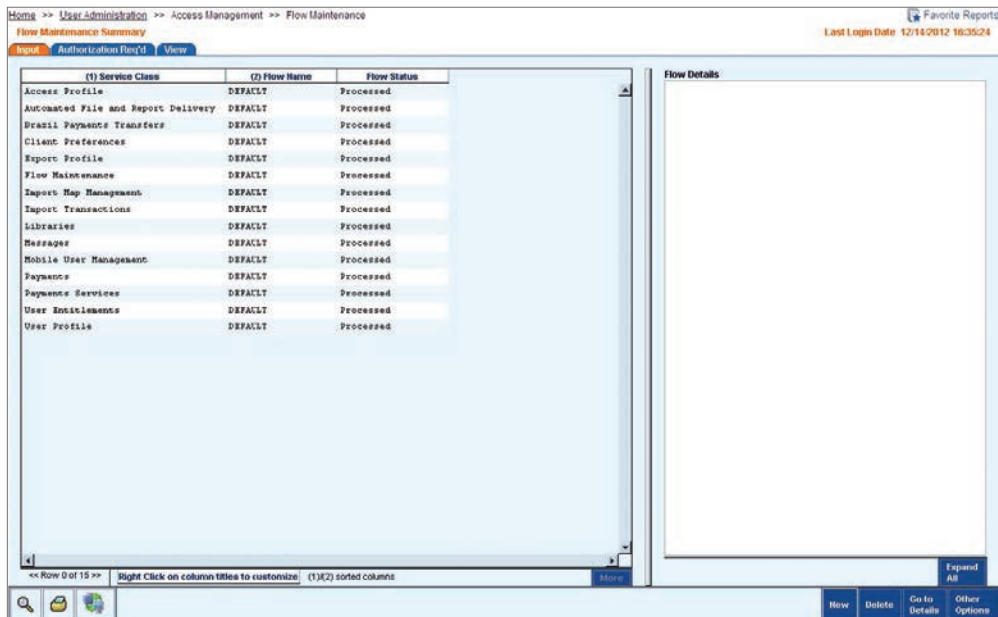
You can delete flow controls with the status Input, Repair Req'd, Authorization Req'd and Processed. However, you cannot delete CitiDirect predefined flow controls with the Flow Name DEFAULT.

Delete flow controls by following the steps below:

1. On the CitiDirect menu under User Administration, click on Flow Maintenance as shown below.



- The Flow Maintenance Summary form appears. All flows with a Processed status and their associated service classes are listed.



(1) Service Class	(2) Flow Name	Flow Status
Access Profile	DEFAULT	Processed
Automated File and Report Delivery	DEFAULT	Processed
Brasil Payments Transfers	DEFAULT	Processed
Client Preferences	DEFAULT	Processed
Export Profile	DEFAULT	Processed
Flow Maintenance	DEFAULT	Processed
Import Map Management	DEFAULT	Processed
Import Transactions	DEFAULT	Processed
Libraries	DEFAULT	Processed
Messages	DEFAULT	Processed
Mobile User Management	DEFAULT	Processed
Payments	DEFAULT	Processed
Payments Services	DEFAULT	Processed
User Entitlements	DEFAULT	Processed
User Profile	DEFAULT	Processed

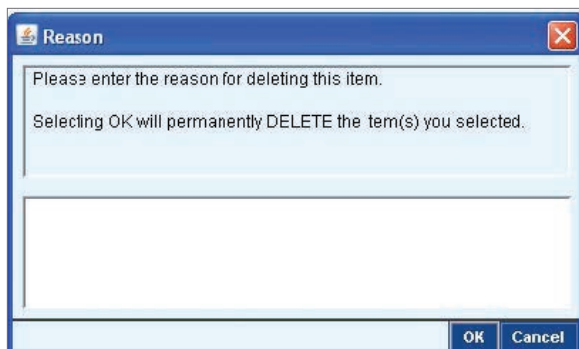
Flow Details

Expand All

Row 0 of 15 | Right Click on column titles to customize | (1)(2) sorted columns

How Delete Go to Details Other Options

- Select the flow you wish to delete and click the Delete button. A dialogue box appears.



4. Enter the reason for the deletion and click the OK button. An information box appears confirming the deletion. The status of the deleted flow is changed to Authorization Required for Delete. Two flows with the same name will exist until the deletion is authorized.

Access Profile

Use the Access Profiles service class to perform the following tasks:

View access profiles.

1. Modify or repair access profiles.
2. Create new access profiles.
3. Authorize access profiles.
4. Delete access profiles.

The Access Profiles service class enables you to define and control access to specific services and processes within CitiDirect. Access profiles can be created, modified or deleted. All of these functions require two Security Managers – one to create, modify or delete and another to authorize. Once one Security Manager creates an access profile and another Security Manager authorizes that profile, it is available to be assigned to a user.

Entitlement is the process of giving CitiDirect access rights or access profiles to a user or groups of users. Users are assigned one or more access profiles as part of the creation of their user entitlements. For more information on user entitlements, refer to the User Entitlements section of this guide.

CitiDirect Online Banking is provided to you with predefined access profiles by product. To meet your organization’s business needs, you can modify these predefined access profiles, or you can create new ones. It is important to note that for some services such as Payments, you may need to populate library information first in order to define items like preformat groups or account groups prior to adding them to an access profile.

Entitlement rights are added to access profiles on two levels:

Service Class Level: Entitlements assigned at the service class level grant access to all processes or activities within that service class. This is the highest form of entitlement. For example, if a user is given the Payments entitlement, then that user can perform all actions under the Payments service class for all accounts, amounts, etc.

Process or Activity Level: Entitlements assigned at the process or activity level limit users to a specific process or processes (Input/Modify only, for example) or to specific account numbers, payment methods, transaction types, etc.

Note: For the Inquiry and Report categories, you must select the specific accounts and base numbers under General Cash PI and General Trade PI to enable users to view related information.

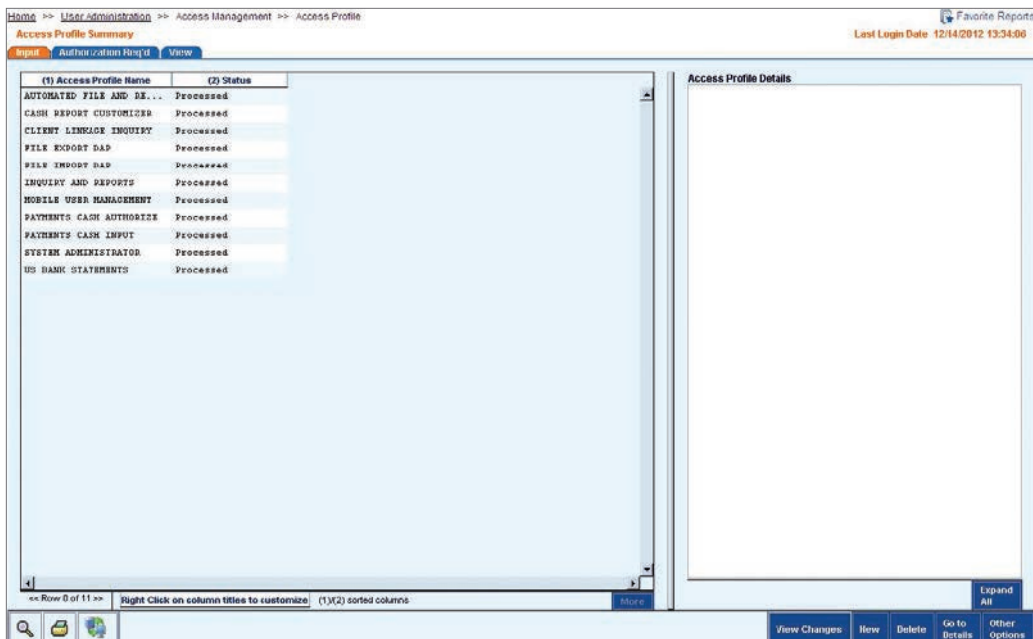
Viewing Access Profiles

View access profiles by following the steps below:

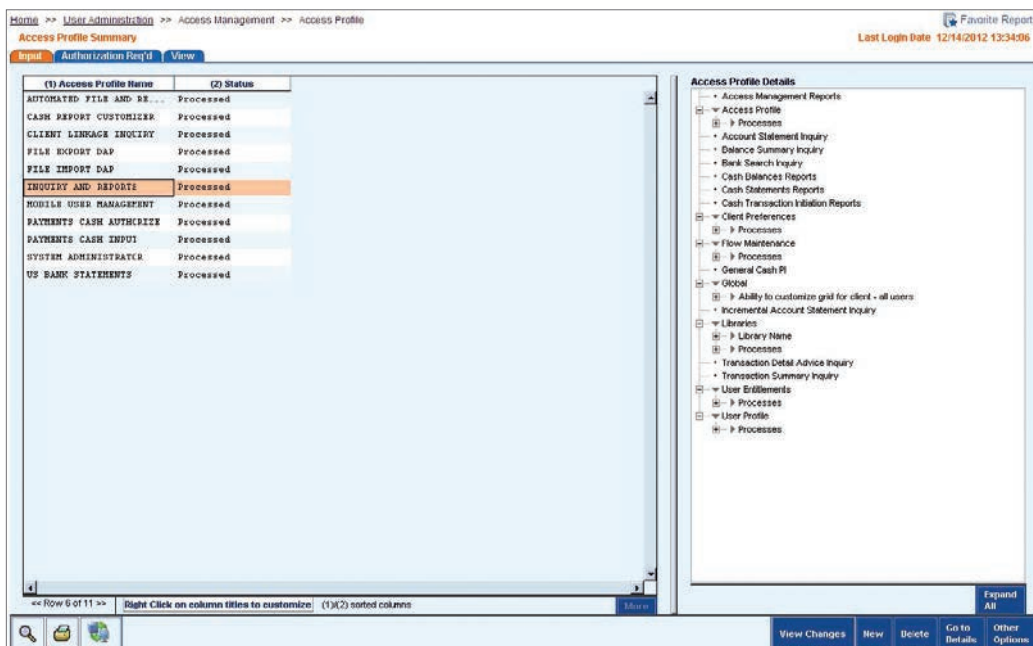
1. On the CitiDirect menu under User Administration, click on Access Profile as shown below.



2. The Access Profile Summary form appears.



3. Select an access profile and view its details in the Access Profiles Details list box.



4. Click the plus signs (+) to expand the list to view all entitlements.

Modifying or Repairing Access Profiles

As Security Manager, you can modify access profiles to better meet your organization’s business needs. The Status column on the Input tab indicates the current status of each access profile and assists you in determining what action, if any, is needed.

Status	Description
Processed	The profile has been authorized, and is currently being used in CitiDirect.
Input	The record has been auto-saved, but not submitted. Additional information is required before it can be submitted for processing.
Invalid	The profile did not pass CitiDirect server validation and must be modified.
Repair Required	Another Security Manager (the authorizer) has determined that the user profile contains incorrect information and/or requires correction.

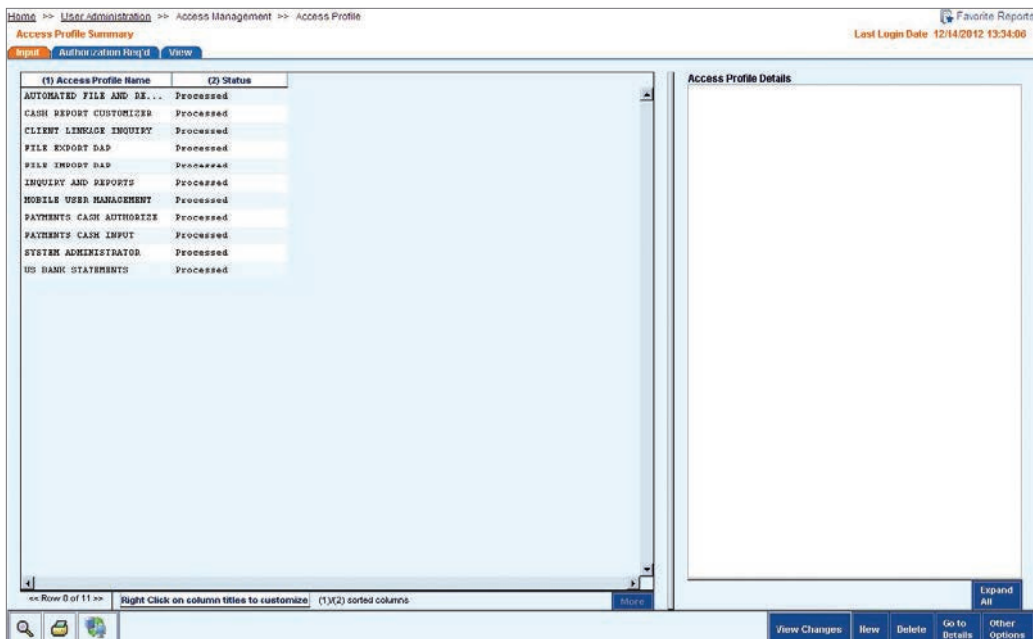
Note: If you modify an access profile, it is treated as new and you cannot authorize it. Access profile modification requires authorization by another Security Manager before the modifications take effect.

Modify or repair access profiles by following the steps below:

1. On the CitiDirect menu under User Administration, click on Access Profile as shown below.

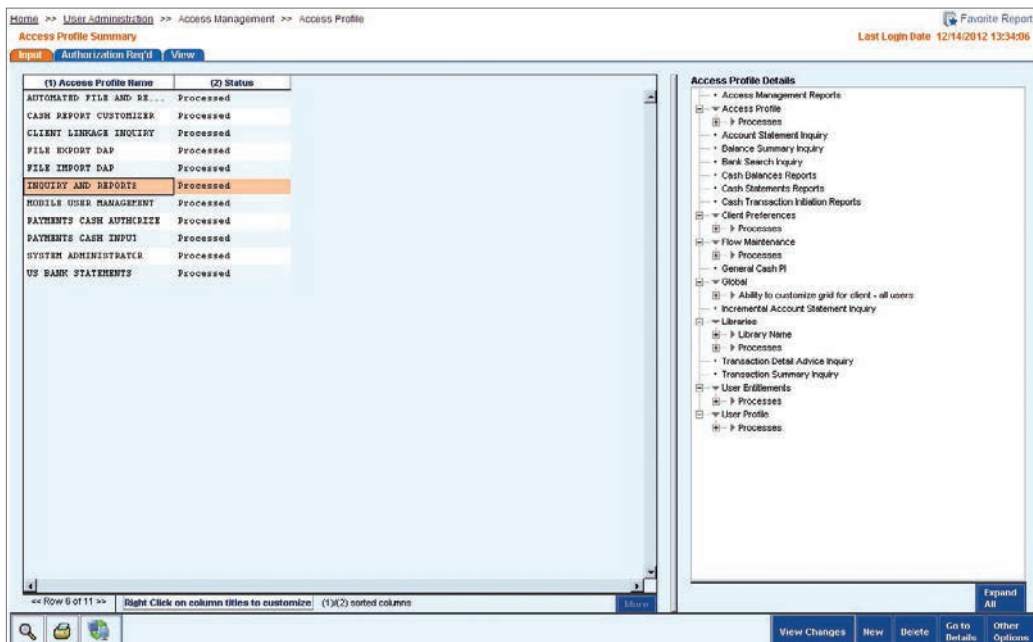


2. The Access Profile Summary form appears.



(1) Access Profile Name	(2) Status
AUTOMATED FILE AND DE...	Processed
CASH REPORT CUSTOMIZER	Processed
CLIENT LINKAGE INQUIRY	Processed
FILE EXPORT DAP	Processed
FILE IMPORT DAP	Processed
INQUIRY AND REPORTS	Processed
MOBILE USER MANAGEMENT	Processed
PAYMENTS CASH AUTHORIZE	Processed
PAYMENTS CASH INPUT	Processed
SYSTEM ADMINISTRATOR	Processed
US BANK STATEMENTS	Processed

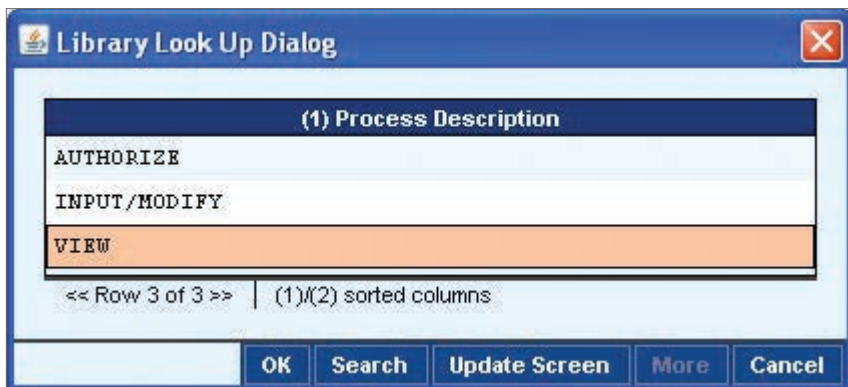
3. Select the access profile to be modified, and then click the Go to Details button. The Access Profile Detail form appears with the Entitlement Criteria and Access Profile Details for the selected profile displayed.



(1) Access Profile Name	(2) Status
AUTOMATED FILE AND DE...	Processed
CASH REPORT CUSTOMIZER	Processed
CLIENT LINKAGE INQUIRY	Processed
FILE EXPORT DAP	Processed
FILE IMPORT DAP	Processed
INQUIRY AND REPORTS	Processed
MOBILE USER MANAGEMENT	Processed
PAYMENTS CASH AUTHORIZE	Processed
PAYMENTS CASH INPUT	Processed
SYSTEM ADMINISTRATOR	Processed
US BANK STATEMENTS	Processed

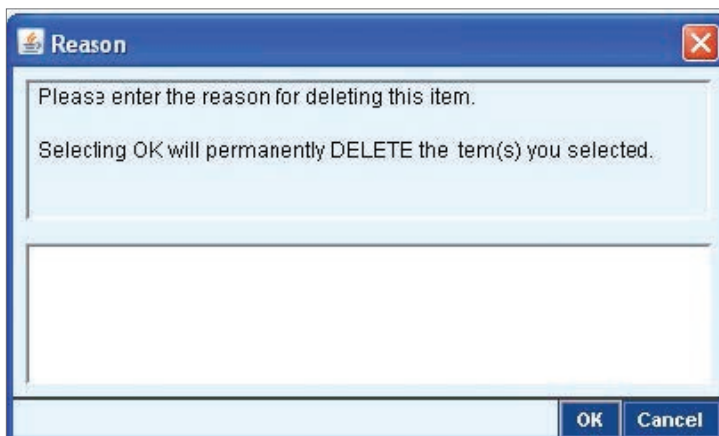
4. Proceed with one of the following steps.

- To add criteria, select the entitlement criteria that you want to add. A Library Look Up Dialogue box appears.



Select the values and click the OK button.

- To delete criteria, select the criteria that you want to delete from the Access Profile Details list box and click the Delete button. A warning message appears.



Click the Yes button to clear the message and delete the selected criteria.

- To reset the criteria to the most recently saved setting, click the Reset button. The access profile criteria return to their previously saved settings.

5. Click the Submit button. The Save As dialogue box appears.



- The Access Profile Name field contains the selected profile name. This name should not be changed. Click the OK button. The modified access profile is added to the authorization queue for approval. Another Security Manager must authorize the modification before it becomes active and can be assigned to a user.

Notes:

If you enter a new name for the modified profile, and then click the OK button, two profiles will exist. Do not change the Access Profile Name.

The assignment of a modified access profile will not take effect until the user closes CitiDirect Online Banking and signs on again.

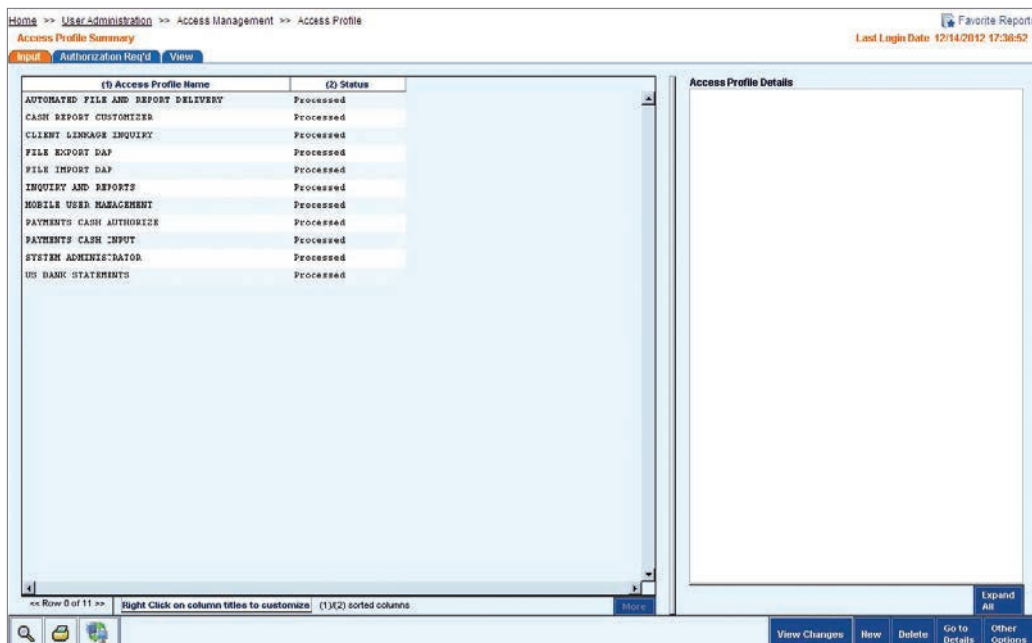
Creating New Access Profiles

Create new access profiles by following the steps below:

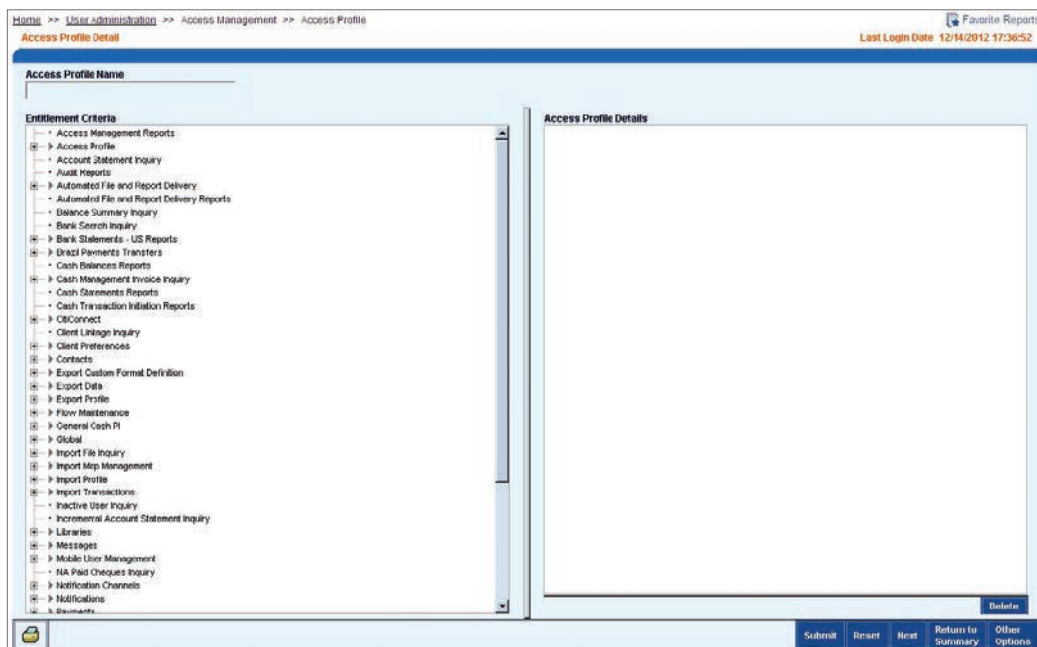
- On the CitiDirect menu under User Administration, click on Access Profile as shown below.



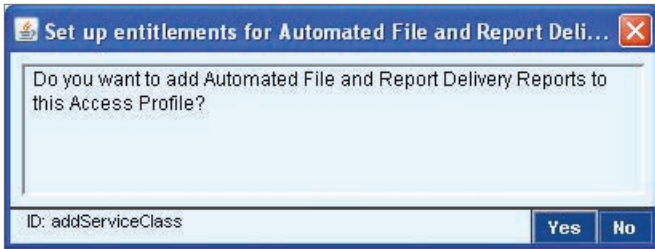
- The Access Profile Summary form appears.



3. Click the New button. The Access Profile Details form appears.



4. Select an entitlement to add to the new access profile. The Set up entitlements for dialogue box appears.



- Click the Yes button to add the entitlement to the access profile. As entitlements are added, they appear in the Access Profile Details list box on the right.

Note: Adding entitlements at the service class level will grant access rights to all processes, accounts, etc., associated with that service class.

- Click the Submit button to save the new access profile. The Save As dialogue box appears.



- Enter the Access Profile Name, and then click the OK button. The access profile enters the authorization queue. Another Security Manager must authorize the new access profile before it becomes active and can be assigned to a user.

Notes:

If specific entitlement criteria are not defined for a service class, the user has access rights to all entitlement values for that service.

A new access profile needs to be linked to a user via user entitlements before it takes effect.

If you submit an access profile, you cannot authorize it.

CitiDirect evaluates the entitlements submitted for processing. If error checking discovers a conflict between entitlements or that a required entitlement is not selected, an error message appears.

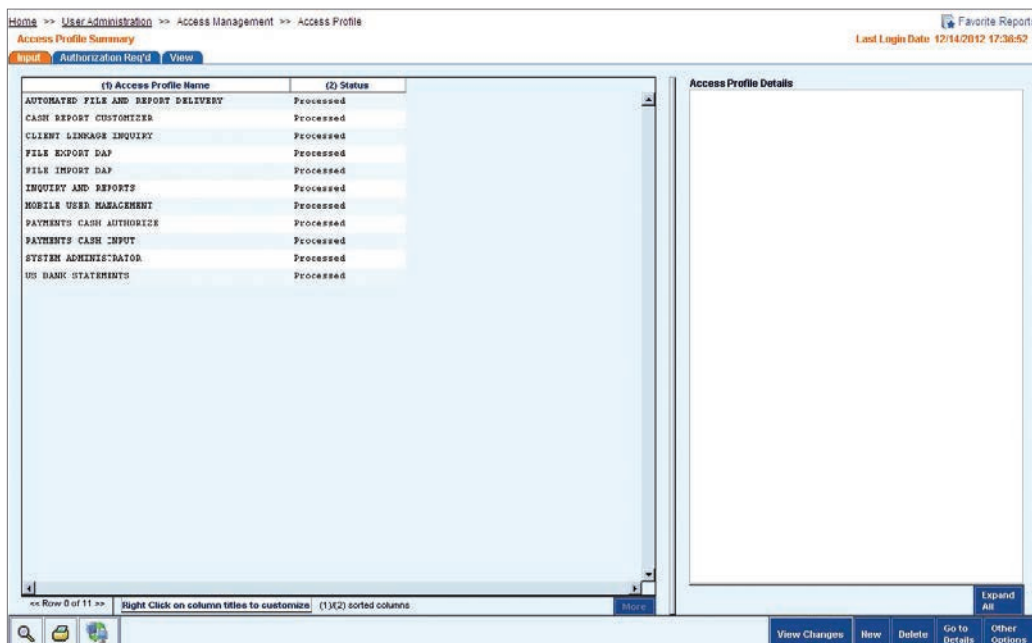
Authorizing Access Profiles

During the authorization process, access profiles can be authorized, rejected or sent to repair. Authorize access profiles by following the steps below:

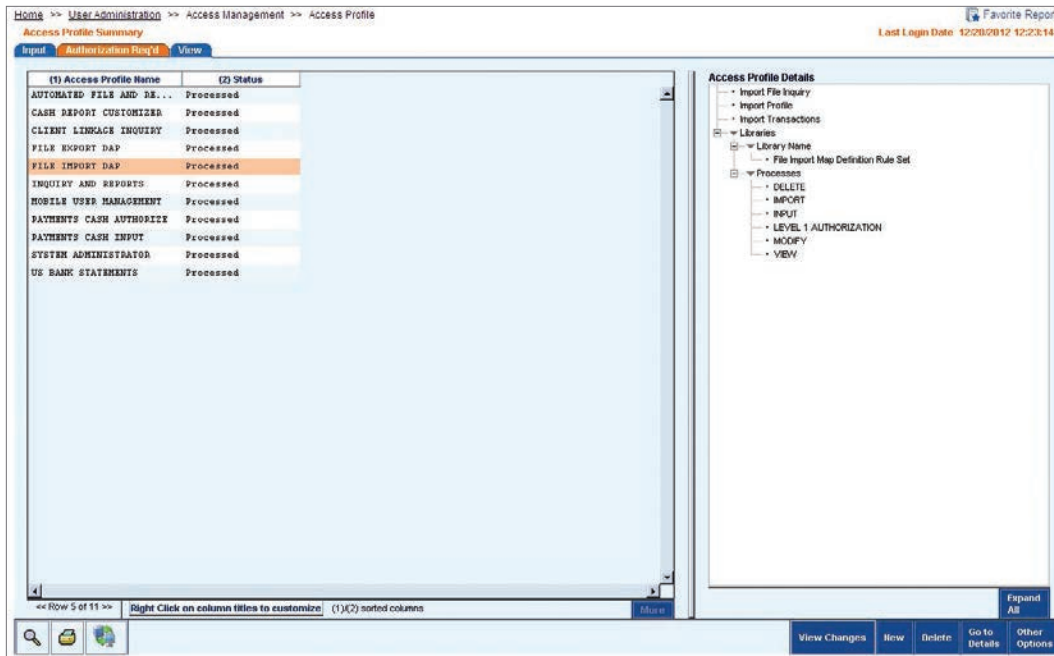
- On the CitiDirect menu under User Administration, click on Access Profile as shown below.



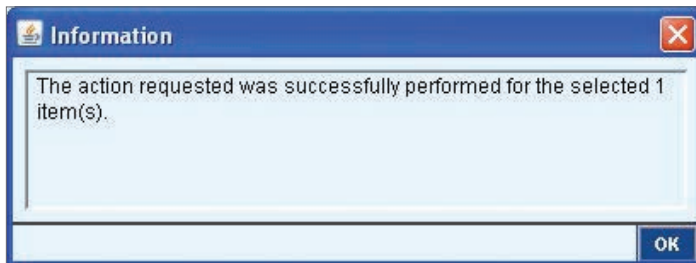
2. The Access Profile Summary form appears.



3. Click the Authorization Required tab to view all access profiles that you are entitled to authorize. If you submitted an access profile, it will not be listed.

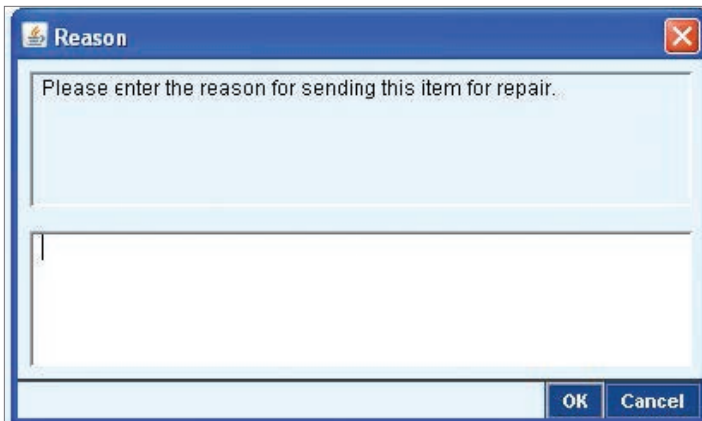


4. Select the access profile to be authorized. The details of the profile appear in the Access Profile Details list box.
5. Proceed with one of the following steps:
 - Click the Authorize button to authorize the selected access profile. A message appears.



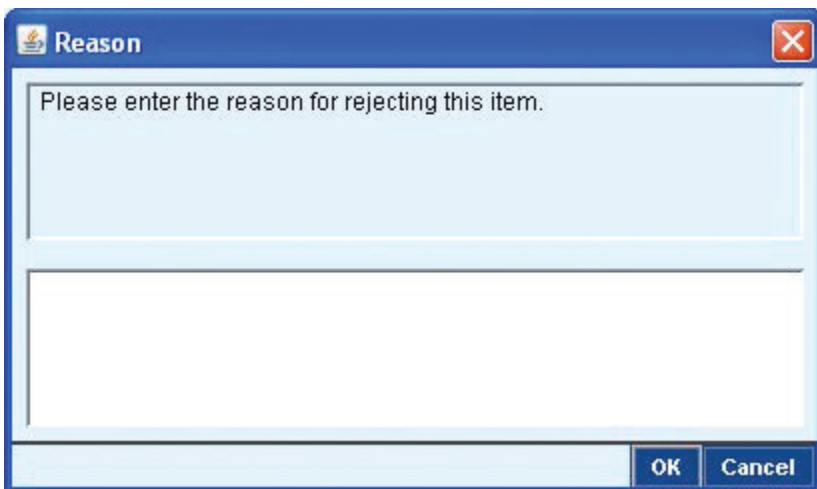
Click the OK button to close the message. The access profile status is changed to Processed and it is available to be assigned to users through the user entitlement process.

- Click the Send to Repair button to indicate that the access profile contains errors. A dialogue box appears.



Enter the reason for sending the profile to repair and click the OK button. A message appears confirming the action. The access profile is sent to the Repair Required queue.

- Click the Reject button to reject the access profile. A dialogue box appears.



Enter the reason for rejecting the profile and click the OK button. A message appears confirming the action and the access profile is deleted from CitiDirect.

Deleting Access Profiles

After viewing access profiles, you may find that some profiles no longer apply. As with new or modified profiles, deleted profiles must be authorized before the application recognizes the deletion.

Notes:

An access profile cannot be deleted if it is assigned to a user.

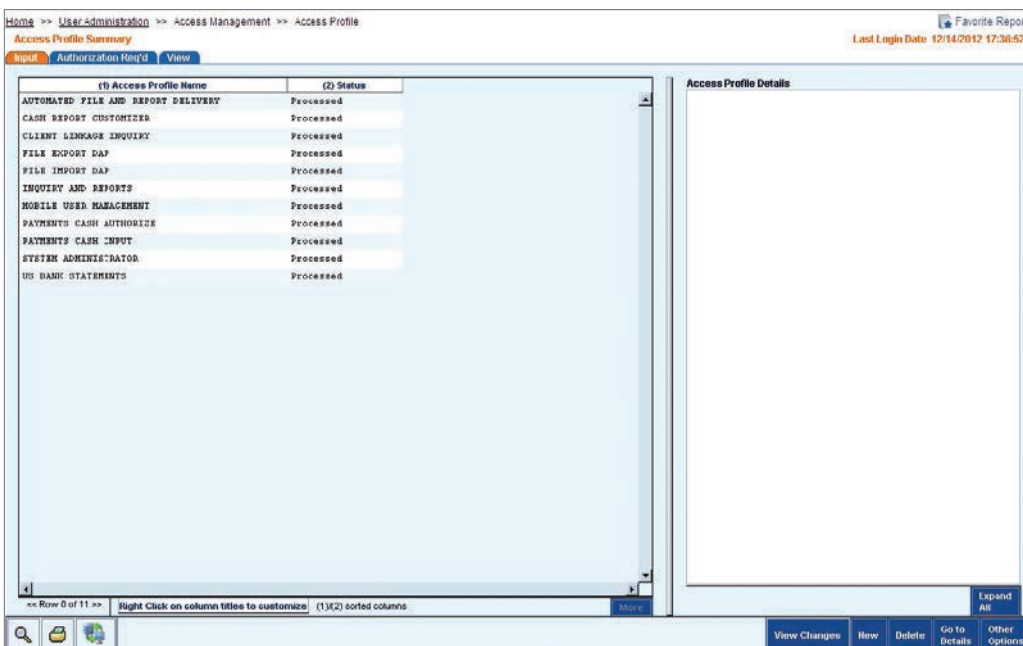
Once the access profile is deleted, two access profiles with the same name exist until another Security Manager authorizes the deletion. Once authorized, both access profiles are deleted.

Delete an access profile by following the steps below:

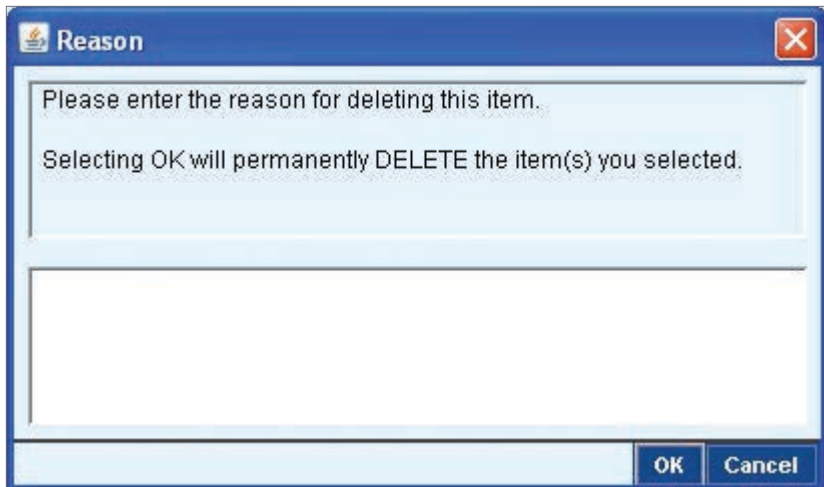
1. On the CitiDirect menu under User Administration, click on Access Profile as shown below.



2. The Access Profile Summary form appears.



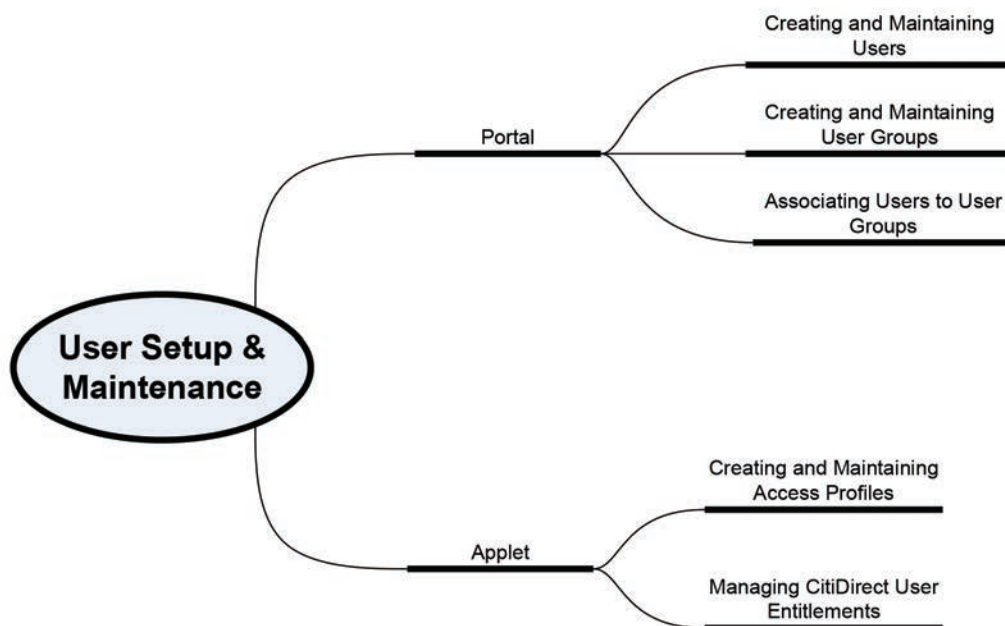
3. Select an individual access profile to be deleted. The details of the profile appear in the Access Profile Details list box.
4. Click the Delete button. A dialogue box appears.



5. Enter a reason for the deletion and click the OK button. The status of the deleted profile is updated to Authorization Required for Delete. The original access profile remains active until its deletion is authorized.

User Setup and Maintenance

In the present setup as a Security Manager, you are required to create and maintain the user and their entitlements. In this endeavor broadly there are two aspects of responsibilities to be handled, one at the level of Portal and another will be within Applet. Below diagram will illustrate the primary responsibilities:



At the level of the Portal you will manage the creation of the user for the first time. Then you will be creating user groups to associate services and manage the user entitlements. For example, the access to CitiDirect Services will be given to users here. Finally you will associate the users to the required user groups based on their job role to configure CitiDirect.

Thereafter in the Applet, you will create access profile to group the entitlement criteria comprising services and features within CitiDirect. This is required to create the right set of enablement based on the job performed by the users within CitiDirect. After this, through user entitlement, you will associate a user to various access profiles based on their role to play in your organization.

Hence, you can understand that through Portal you can provide subscription of CitiDirect to a user and access to features within CitiDirect (for example Check Status Inquiry or Asia Direct Debit Inquiry or Brazil Account Information) is to be given within.

After logging in Portal, the following tasks can be performed through Client Administration Service under **Self Service** in the top menu bar. Use the User Profile service class to perform the following tasks:

1. Create User
2. User Worklist
3. View All Users
4. Create User Group
5. User Group Worklist
6. View All User Group
7. Create User Group Association
8. User Group Association Worklist
9. View All User Group Association



After performing system setup and configuration for CitiDirect, the next step is to set up individual users and grant them access rights to services and account information in CitiDirect.

This section of the Security Manager guide describes the features and procedures that enable you to complete the above processes in the Client Administration Service under Self Service in the Portal page and in the User Entitlements service class, which are found under the Access Management category on the CitiDirect menu under User Administration through the Applet.

After user setup, periodic maintenance of user and security credential information is a critical part of your role as Security Manager.

Note: Users who have been inactive (i.e., not logged on for 24 months) will automatically be deleted by the system. Additionally, any users that have not logged into the application within 24 months from the date the user was initially added to the application will automatically be deleted by the system.

User Setup

Here it enables you to establish users on CitiDirect and to define how they will work with the application. Through the creation of the user you will capture the below information:

- The user's personal contact information, including name, address, telephone number and e-mail address.
- The times the user can access CitiDirect, including access time during the day, days of the week and the range of days for which access is granted and the type of security credentials currently assigned to the user.

Create User

Accurate information is essential when creating user for your organization as each user identifies the individual's unique personal and CitiDirect access information.

Ensure that you do not grant one individual more than one User ID. Doing so could result in unintended consequences. Search all user profiles to avoid creating a duplicate entry.

Create a new user by following the steps below:

1. On the portal menu, Create User can be accessed through Self Service under Client Administration Service.



2. Click on Create User to load the page.

Self Service > Client Administration Service > Create User

Client UI UPGRADE DEMO 2	Subscription 2 Products, 13 Services
------------------------------------	--

Create New User Print

* Required Field

User Details

Status:

General Information

User Alias: Employee ID: * First Name: * Last Name: Middle Name: Initials:

Building/Floor/Room: * Street Address 1: Street Address 2: Street Address 3: * Country:

State/Province/Territory: * City: Zip/Postal Code: * Time Zone: * Telephone:

* Email: User Manager:

CitiDirect Information

* SDR User Account Type: User ID:

* User Allow Access To Days: to * User Allow Access To Time: to * CitiDirect Time Zone:

Days of Week:
 SUNDAY
 MONDAY
 TUESDAY
 WEDNESDAY
 THURSDAY
 FRIDAY
 SATURDAY

0 - 0 of 0

<input checked="" type="checkbox"/> Credential Type	Credential ID
No Credentials	

New

Submit Save Cancel

Note: Based on your organization's preferences, some fields may be automatically populated, such as City, State/Province/Territory, Country, and Zip/Postal Code. The SDR User Account Type field will appear under CitiDirect Information for all Same Day Reconciliation (SDR) clients. The default value for this field is Omnibus Account, which specifies that the SDR user will have no account restrictions (access to all). You may elect to designate Sub-Account to specify that the user is restricted to Sub-Accounts only for SDR functionality in CitiDirect.

3. Select the status to be Active for this new user.
4. Enter the new user's contact information, including name, address, telephone and e-mail address, etc. Depending on your region, this information is used to create and mail CitiDirect BE security credentials once the user profile is authorized. Do not use P.O. Box numbers in the Street Address field. Security credentials must be mailed to a street address.

Note: ALL USERS ARE REQUIRED TO HAVE A VALID E-MAIL ADDRESS TO RECEIVE CITIDIRECT-RELATED COMMUNICATIONS.

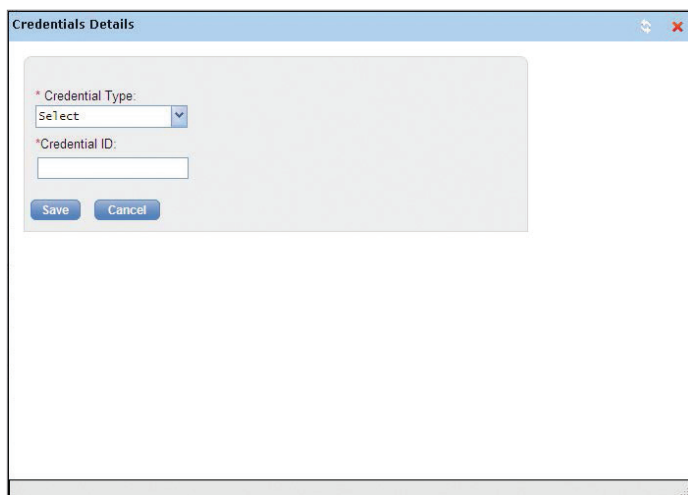
5. Select the user's Time Zone. The time zone can impact scheduled events and report time stamps (the date and time the report was generated). Selecting the incorrect Time Zone will affect a user's ability to access and work in CitiDirect. This can also impact users traveling on business.
6. Select a start and end date in the User Allow Access to Days field. This denotes the period of time in which the user can access CitiDirect.

Note: The Citibank-defined start date is the user profile creation date. The Citibank-defined end date is one year later. We recommend that you extend the date to comply with your internal regulation and compliance rules. To ensure that there is no interruption of access for users, Security Managers should validate user profiles on an annual basis, at a minimum.

- Specify the earliest and latest times the user can access CitiDirect using the 24-hour clock in the User Allow Access to Time fields. Times are relative to the selected time zone.

Note: For global travelers, the start and end times must allow access to CitiDirect Online Banking in both work and travel locations. For example, an employee based in Shanghai, traveling to Los Angeles, will require access beyond the normal Shanghai workday.

- Select the days on which the user can access CitiDirect in the Days of Week field. The predefined setting allows access every day of the week. You can hold the Control key on your keyboard and select individual days to select and assign non-consecutive days.
- In the Credentials section, click the New button. The Credentials Details dialogue box appears.



- Select the appropriate Credential Type for the user, and then enter the related Credential ID. Both fields are required.

Notes:

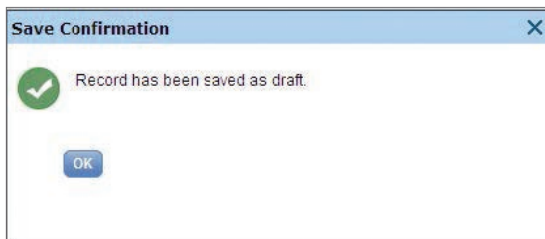
For SafeWord card users, distribution varies by region.

- If your organization distributes SafeWord security credentials, enter the SafeWord™ card number (found on the back of the card) into the Credentials ID field.
- If Citi distributes SafeWord security credentials, leave the Credentials ID field blank.
- For additional information please contact your local Implementation Manager

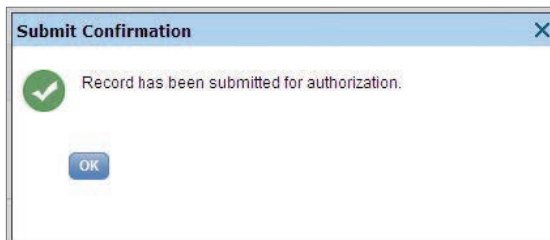
Information on how you should complete the Credential Details dialogue box:

- Depending on the user's job description, you may want a user to have the ability to use multiple types of security credentials.
- If the user has existing credentials, select the appropriate Credential Type and enter the related Credential ID.
- Click the Close button if you do not have the necessary information to define the user's security credentials.

11. Click the Save button on the Credentials Details dialogue box.
12. At this point, you may want to identify additional credentials for the user. Enter additional information as necessary, and then click the Close button.
13. Click on Save to save the user as a draft and it will move to the To Modify queue.



14. Click the Submit button to save the user and enter it into the authorization queue.



User Worklist

You can use this for the maintenance of the created users. Under this you can do the following:

1. To Authorize
 - a. Authorize
 - b. Send to Repair
 - c. Reject
2. To Modify
 - a. Recall Request
 - b. Save
 - c. Submit
 - d. Cancel
3. Processed
 - a. Save
 - b. Submit
 - c. Cancel
 - d. Delete User in CitiDirect

To Authorize

When created users are ready for authorization, they are listed on the To Authorize worklist where they can be selected and authorized by an entitled Security Manager.

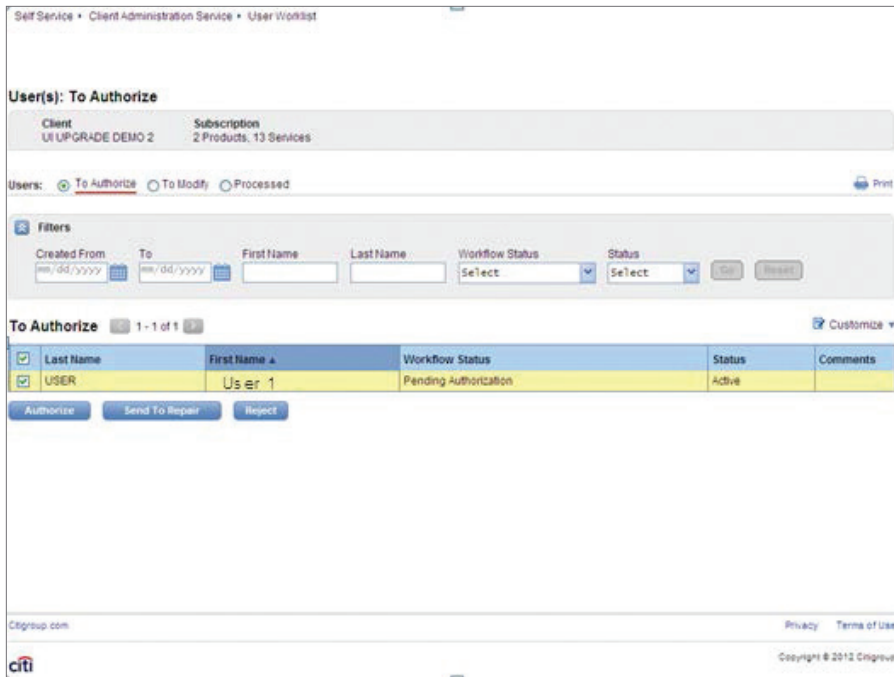
You will see only the records that you are entitled to authorize. If you created the user, you cannot authorize it. During the authorization process, user records can be authorized, sent to repair or rejected. The user profile remains inactive until it is authorized.

To Authorize you can follow the steps below:

1. On the portal menu, User Worklist can be accessed through Self Service under Client Administration Service.



2. Clicking on the User Worklist will take you to the To Authorize page.



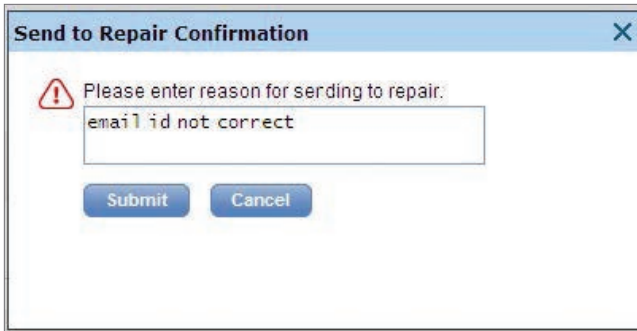
3. By default it will display all users pending to be authorized excepting the ones created by you. You can filter by entering created from and to, first name, last name, work flow status and status.
4. Once the users are displayed under To Authorize in multiple rows, they can be individually or group selected.
5. These selected users can be authorized, sent to repair or rejected.
6. Once authorized, it will be confirmed in a dialogue box.

Notes:

For most SafeWord card users, once a user profile is authorized a request is automatically generated in CitiDirect for Citi to distribute a SafeWord card to the address found in the profile.

Asia/Pacific Security Managers in some countries will directly distribute the SafeWord card and assign replacement cards to users.

7. If you click on Send to Repair on the To Authorize screen for any user, a dialogue box will prompt to enter the reason. Entering the reason will help others to understand why repair is required. Below is the screen for the Send to Repair Confirmation dialogue box.



8. On Submit, user record will move to the To Modify queue under User Worklist with workflow status as Repair Required. One of you can repair it and resubmit for authorization.
9. You can also reject a created user by clicking on the Reject on the To Authorize page.
10. A dialogue box will open to enter the reason for rejection and once submitted, the record will be rejected. None of the Security Managers will be able to see the record in the To Authorize queue again. Rejected records will be visible in View All Users under Client Administration Service in Rejected state.

Note: You can reject a profile because it is invalid and should not have been created. Rejecting a user profile deletes it from the application, but creates an audit trail of your action, along with your reason for the rejection.

To Modify you can follow the steps below:

1. You have to click To Modify on the User Worklist page. The page will be as below. You can recall a request from this page by selecting individual or all records.

Self Service > Client Administration Service > User Worklist

User(s): To Modify

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

Users: To Authorize To Modify Processed [Print](#)

Filters

Created From: To: First Name: Last Name: Workflow Status: Status:

To Modify 1 - 2 of 2 [Customize](#)

<input type="checkbox"/>	Last Name	First Name ▲	Workflow Status	Status	Comments
<input checked="" type="checkbox"/>	User	User 1	Repair Required	Active	
<input type="checkbox"/>	User	User 2	Repair Required	Active	

Citigroup.com Privacy Terms of Use

Copyright © 2012 Citigroup

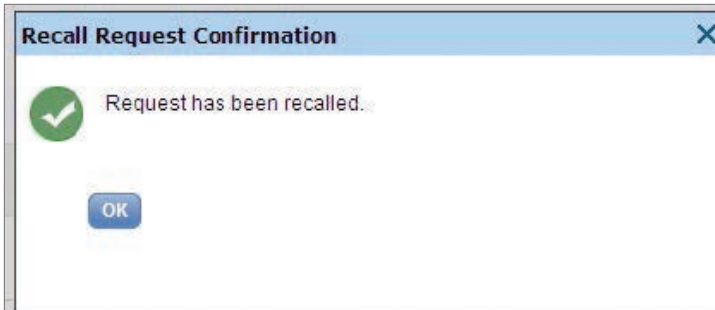
- The reasons can be inserted while rejecting, sending for repair, recalling etc. These reasons can be seen clicking the comments column in the To Authorize or View All Users page. It will display the user name, date, time and the comment.

Comments ✕

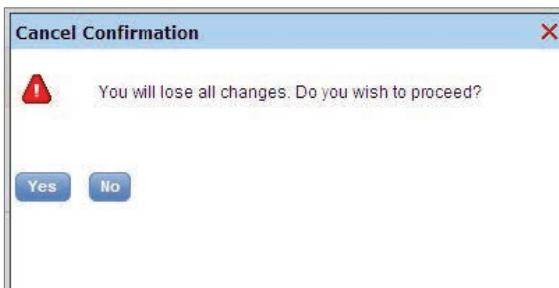
User 1 : 11/29/2012, 14:50 EST

test user not needed

- Once recall is requested it will open the Recall Request Confirmation dialogue box. The reason can be entered and it can be confirmed. The Confirmed dialogue box will be as below and the record will be logically deleted.



4. If you click on the first name of any record, the detail editable page for that user record will open.
5. You can modify or repair same fields entered during the creation of that user.
6. After modification if you click on Submit, the record is validated against all processing logic. If the validation is successful, you will see a confirmation message and move the record to Pending Authorization status. Records in Pending Authorization state will be visible under To Authorize queue under User Worklist.
7. If you click on Save, the record is validated against all processing logic. If the validation is successful, system will save the record and move it to Saved status. Records in Saved state will be visible under To Modify queue under User Worklist.
8. If you click on Cancel, you will lose all edited data and you will be navigated back to To Modify queue. A dialogue box will open for your confirmation of the cancel.



You can do the following steps with the Processed data:

1. You have to click Processed on the User Worklist page. The page will be as below.

Self Service » Client Administration Service » User Worklist

User(s): Processed

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

Users: To Authorize To Modify Processed [Print](#)


Filters

Created From: To: First Name: Last Name: Status: [Go](#) [Reset](#)

Filtered By - First Name

Processed 1 - 1 of 1 [Customize](#)

Last Name	First Name ▲	Status	Comments
User	User 1	Active	

Citigroup.com [Privacy](#) [Terms of Use](#)
 Copyright © 2012 Citigroup

- If you click on the first name of any record, the detail editable page for that user record will open as below.

* Required Field


► **User Details**
 Workflow Status: Processed Status: Active ▼

General Information

User Alias: Employee ID: * First Name: * Last Name: Middle Name: Initials:

Building/Floor/Room: * Street Address 1: Street Address 2: Street Address 3: * Country: UNITED STATES ▼

* State/Province/Territory: DE ▼ * City: Zip/Postal Code: * Time Zone: Eastern Time (US & Ca) ▼ * Telephone:

* Email: User Manager: 

CitiDirect Information

* SDR User Account Type: OmniBus Account User ▼ User ID:

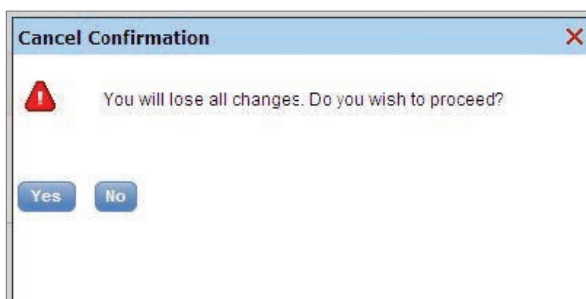
* User Allow Access To Days: 11/29/2012 to 11/29/2025 * User Allow Access To Time: 00:00:00 AM to 23:59:59 PM * CitiDirect Time Zone: Eastern Time (US & Ca) ▼

Days of Week
 SUNDAY
 MONDAY
 TUESDAY
 WEDNESDAY
 THURSDAY
 FRIDAY
 SATURDAY

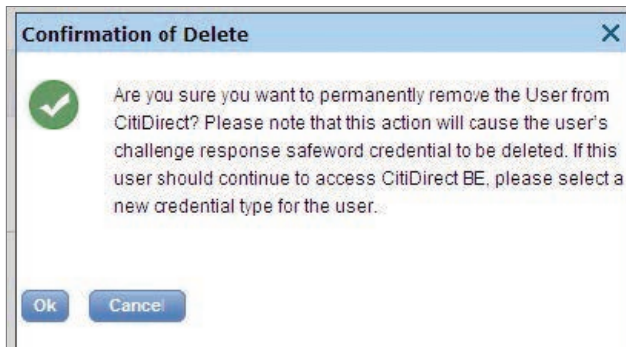
1 - 1 of 1

<input type="checkbox"/> Credential Type	Credential ID
<input type="checkbox"/> Sefaword ID	Dummy

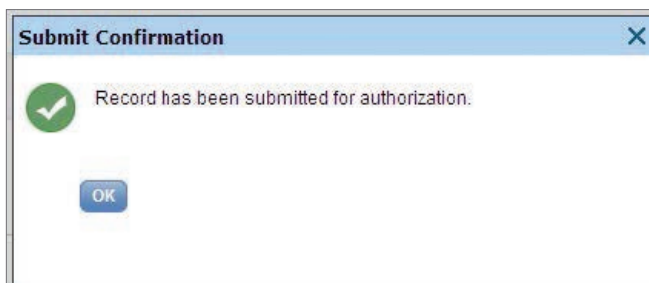
3. You can save, submit, cancel or delete user in CitiDirect in this page.
4. After modification if you click on Submit, the record is validated against all processing logic. If the validation is successful, you will see a confirmation message and move the record to Pending Authorization status. Records in Pending Authorization state will be visible under To Authorize queue under User Worklist.
5. If you click on Save, the record is validated against all processing logic. If the validation is successful, system will save the record and move it to Saved status. Records in Saved state will be visible under To Modify queue under User Worklist.
6. If you click on Cancel, you will lose all edited data and you will be navigated back to To Modify queue. A dialogue box will open for your confirmation of the cancel.



7. Delete will allow you to delete records. Every delete of Every Record will prompt the user to input reasons for deletion.



8. Deleted records will move to Pending Authorization for Delete state and will be visible under To Authorize queue under User Worklist. After Authorization the record will be logically deleted.



Note: If you have selected multiple records to delete, this reason must apply to all user profiles selected. If each user profile has a different reason for deletion, you must select and delete each profile individually.

9. A user should be disabled when you want to temporarily suspend a user's access to CitiDirect. You can disable a user by changing the status from active to inactive in the details page of a record.

Note: If an employee is terminated, you should immediately delete his or her user profile. It is the responsibility of client Security Managers to manage user profiles to ensure timely modification, disabling and deletion based on client business needs and employee access needs.

* Required Field


► User Details
 Workflow Status: Processed Status: Active

General Information

User Alias: Employee ID: * First Name: * Last Name: Middle Name: Initials:

Building/Floor/Room: * Street Address 1: Street Address 2: Street Address 3: * Country:

* State/Province/Territory: * City: Zip/Postal Code: * Time Zone: * Telephone:

* Email: User Manager: 

CitiDirect Information

* SDR User Account Type: User ID:

* User Allow Access To Days: to * User Allow Access To Time: to * CitiDirect Time Zone:

Days of Week:
 SUNDAY
 MONDAY
 TUESDAY
 WEDNESDAY
 THURSDAY
 FRIDAY
 SATURDAY

1 - 1 of 1

Credential Type	Credential ID
<input type="checkbox"/> Safeword ID	Dummy

New Delete

Submit Save Cancel Delete User in CitiDirect

10. You can also modify the status of the user from Inactive to Active when the user requires to work again in CitiDirect. On Submit this user will move to authorization queue.

* Required Field


► **User Details**
 Workflow Status: Processed Status: Active

General Information

User Alias: Employee ID: * First Name: * Last Name: Middle Name: Initials:

Building/Floor/Room: * Street Address 1: Street Address 2: Street Address 3: * Country:

* State/Province/Territory: * City: Zip/Postal Code: * Time Zone: * Telephone:

* Email: User Manager: 

CitiDirect Information

* SDR User Account Type: "/>

* User Allow Access To Days: to * User Allow Access To Time: to * CitiDirect Time Zone:

Days of Week:
 SUNDAY
 MONDAY
 TUESDAY
 WEDNESDAY
 THURSDAY
 FRIDAY
 SATURDAY

1 - 1 of 1

Credential Type	Credential ID
<input type="checkbox"/> Safeword ID	Dummy

New Delete

Submit Save Cancel Delete User in CitiDirect

Note: User will be able to work in CitiDirect once the change of status from Inactive to Active is being authorized.

View All Users

View All Users contains a comprehensive list of all user profiles, including processed profiles and those awaiting authorization or repair. This information is useful because it provides a snapshot of the current state of all user profiles, letting you know which steps to take next and prevents the creation of duplicate profiles.

Under this you can do the following:

1. On the portal menu, View All Users can be accessed through Self Service under Client Administration Service.



2. The list can be filtered as in To Authorize.

Self Service > Client Administration Service > View All Users

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

View All Users Print

Filters


Created From: To: First Name: Last Name: Workflow Status: Status: Go Reset

Filtered By - First Name

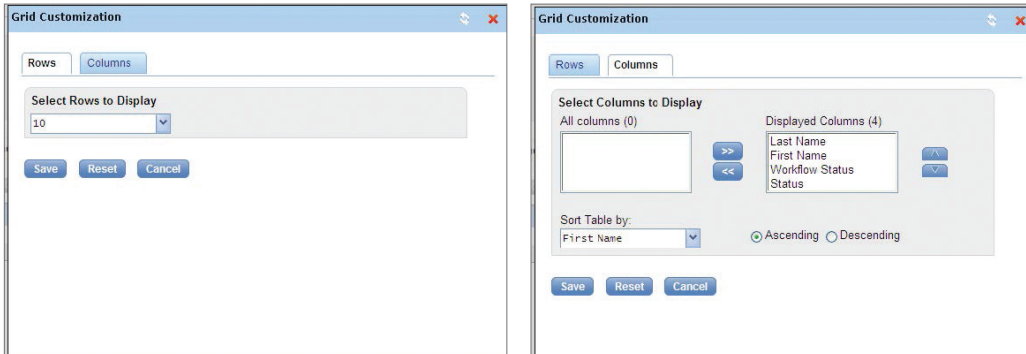
View All Users 1 - 2 of 2 Customize

Last Name	First Name ▲	Workflow Status	Status	Comments
User	User 1		Active	
User	User 1		Active	

Citigroup.com Privacy Terms of Use

 Copyright © 2012 Citigroup

- You can customize this page by clicking on Customize. A dialogue box will open where you can configure to see more numbers of rows, rearrange the columns for display and sort the table.



- Clicking on the first name of a record will take you to the detailed page where you can see the information for that user.

Self Service > Client Administration Service > View All Users

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

View All Users > View Details

View All Users Print

Workflow Status: Rejected Status: Active

General Information

User Alias:	Employee ID: 12345	First Name: User 1	Last Name: User	Middle Name:	Initials:
Building/Floor/Room:	Street Address 1: 1234	Street Address 2:	Street Address 3:	Country: US	
State/Province/Territory: DE	City: jersey city	Zip/Postal Code: 07310	Time Zone: Eastern Time (US & Canada)	Telephone: 12017633798	

Email: User1@citi.com User Manager

CitiDirect Information (Action being Authorized is "Delete User in CitiDirect")

SDR User Account Type: Omnibus Account User	User ID: 51040100		
CitiDirect Time Zone: Eastern Time (US & Canada)	User Allow Access To Days: 11/29/2012 to 11/29/2025	User Allow Access To Time: 12:00 AM to 11:59 PM	Days of Week: SUN,MON,TUE,WED,THU,FRI,SAT

0 - 0 of 0

Credential Type	Credential ID
No Credentials	

Cancel

- Clicking on cancel will take you back to the list of all users.

User Group Maintenance

Here as a Security Manager, you need to create groups based on the requirement of the jobs to be handled by your users. This feature will enable you to create user group, maintaining it and also to view all user groups.

Under this you can do the following:

1. Create User Group
 - a. Preview
 - b. Reset
 - c. Submit
 - d. Save
 - e. Cancel
2. User Group Worklist
 - a. To Authorize
 - b. To Modify
 - c. Processed
3. View All User Group

Create User Group

Accurate planning is essential when creating user group for your organization as each group identifies the Admin privileges and CitiDirect access information.

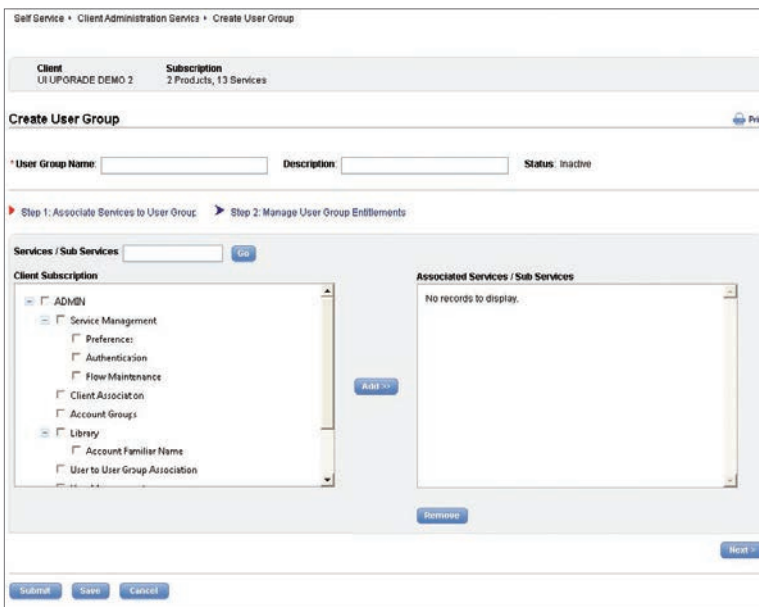
Ensure you create unique User Groups and search all user groups to avoid creating a duplicate entry.

Create new user group by following the steps below:

1. On the portal menu, Create User Group can be accessed through Self Service under Client Administration Service.

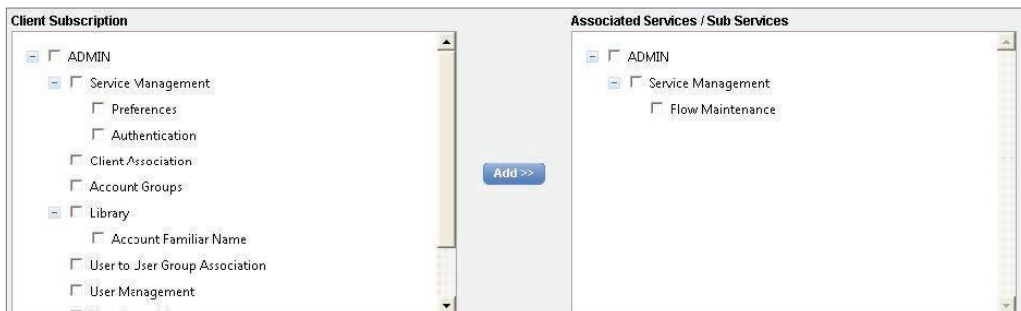


2. Click on Create User Group to load the page.



Note: Based on your organization's preferences, associated services and sub-services are to be selected for the user group.

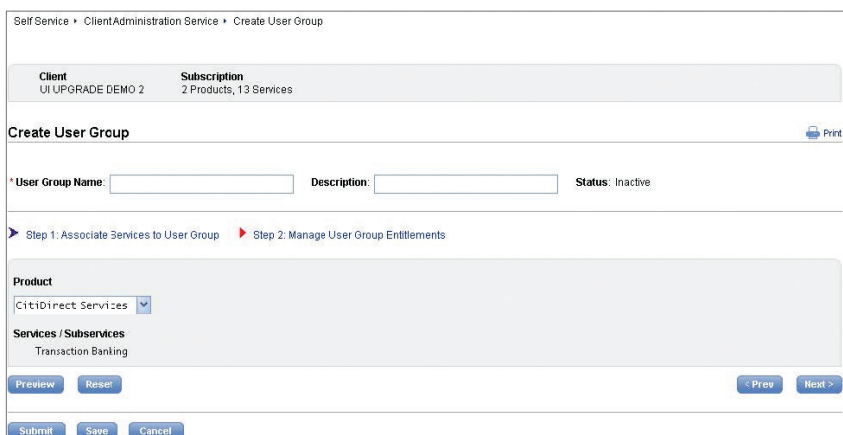
3. Enter the User Group name and Description as appropriate.
4. Select the services and sub-services from the subscription list of your organization on the left-hand side and click on Add to see it under Associated Services/Sub Services list. In this page you associate services to the user group.



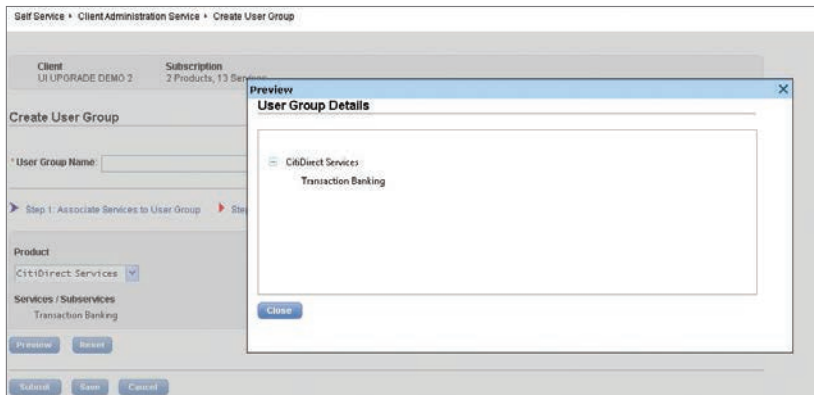
5. To remove, select the Associated Services/Sub Services and click on Remove. A dialogue box will open to confirm the removal.



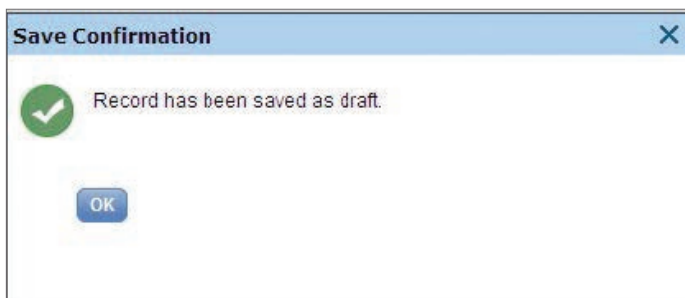
6. In the following step, by clicking next, you will be taken to the Manage User Group Entitlement page. The subscription to the products can be selected from here. This list will display the list of products based on the selection of the services in the previous page.



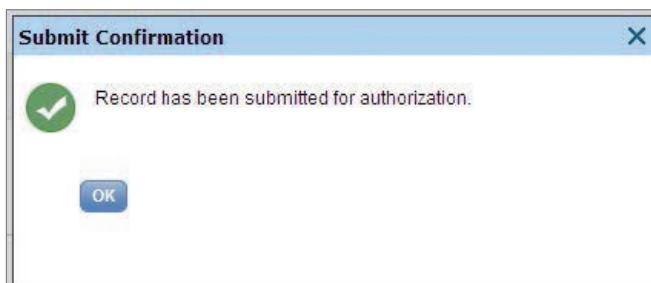
- If you click on Preview, you will be able to see a summary of all the products and the services in a dialogue box.



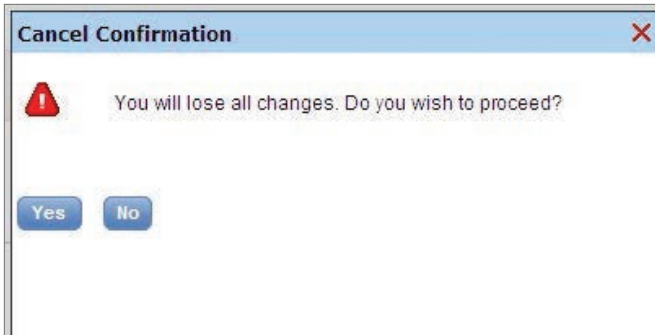
- On clicking Reset, all filter criteria will be removed and all records immaterial of the filter parameters will be displayed.
- Clicking on Save will save the user group and move it to To Modify queue.



- If you click Submit, the record will be saved and will be submitted for authorization. Another user will find it in the To Authorize queue.



- Cancel will not save any of the entered data in the page. A dialogue box will open for your confirmation of the cancel.



User Group Worklist

You can use this for the maintenance of the created user groups. Under this you can do the following:

1. To Authorize
 - a. Authorize
 - b. Send to Repair
 - c. Reject
2. To Modify
 - a. Recall Request
 - b. Save
 - c. Submit
 - d. Cancel
3. Processed
 - a. Save
 - b. Submit
 - c. Cancel
 - d. Delete

To Authorize

When created user groups are ready for authorization, they are listed on the To Authorize worklist where they can be selected and authorized by an entitled Security Manager.

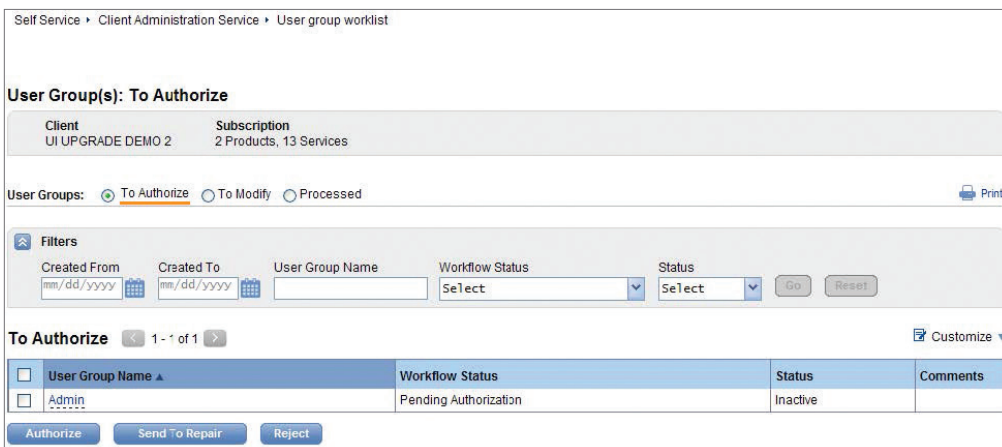
You will see only the records that you are entitled to authorize. If you created the user group, you cannot authorize it. During the authorization process, user group records can be authorized, sent to repair or rejected. The user group remains inactive until it is authorized.

To Authorize you can follow the steps below:

1. On the portal menu, User Group Worklist can be accessed through Self Service under Client Administration Service.

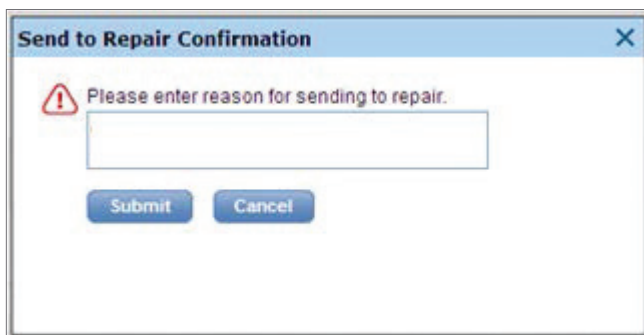


2. Clicking on the User Group Worklist will take you to the To Authorize page.



- By default it will display all User Groups pending to be authorized except the ones created by you. You can filter by entering created from and to, first name, last name, work flow status and status.
- Once the User Groups are displayed under To Authorize in multiple rows, they can be individually or group selected.
- These selected User Groups can be authorized, sent to repair or rejected.
- Once authorized, it will be confirmed in a dialogue box.

- If you click on Send to Repair on the To Authorize screen for any User Group, a dialogue box will prompt to enter the reason. Entering the reason will help others to understand why repair is required. The below is the screen for the Send to Repair Confirmation dialogue box.

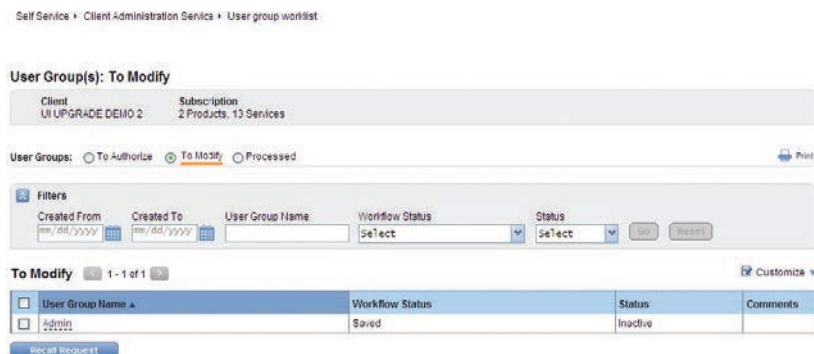


- On Submit User Group, record will move to the To Modify queue under User Group Worklist with workflow status as Repair Required. One of you can repair it and resubmit for authorization.
- You can also reject a created User Group by clicking on Reject on the To Authorize page.
- A dialogue box will open to enter the reason for rejection and once submitted, the record will be rejected. None of the Security Managers will be able to see the record in the To Authorize queue again. Rejected records will be visible in View All User Groups under Client Administration Service in Rejected state.

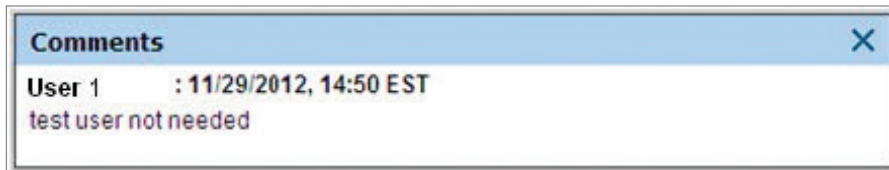
Note: You can reject a User Group because it is invalid and should not have been created. Rejecting a User Group deletes it from the application, but creates an audit train of your action, along with your reason for the rejection.

To Modify you can follow the steps below:

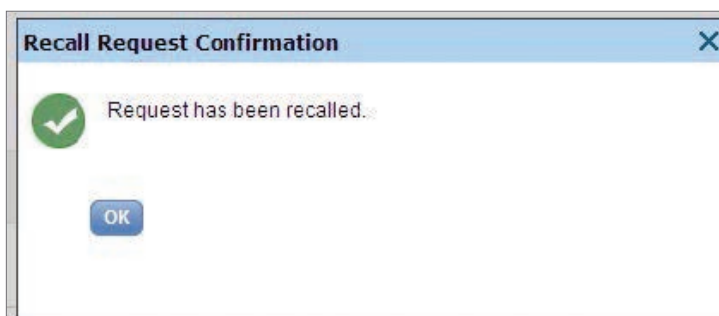
- You have to click To Modify on the User Group Worklist page. The page will be as below. You can recall a request from this page by selecting individual or all records.



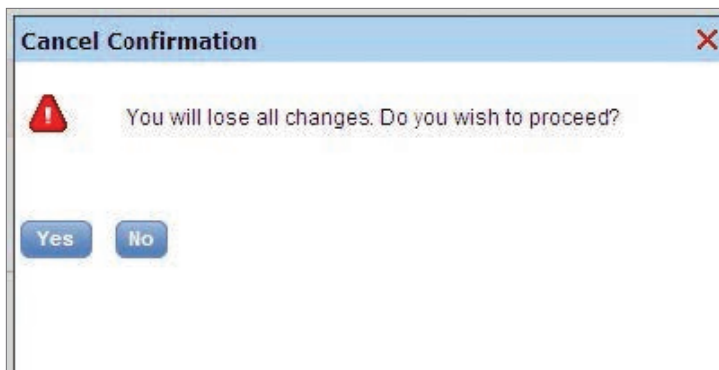
2. The reasons can be inserted while rejecting, sending for repair, recalling, etc. These reasons can be seen clicking the comments column in the To Authorize or View All User Groups page. It will display the user name, date, time and the comment.



3. Once recall is requested it will open the Recall Request Confirmation dialogue box. The reason can be entered and it can be confirmed. The Confirmed dialogue box will be as below and the record will be logically deleted.

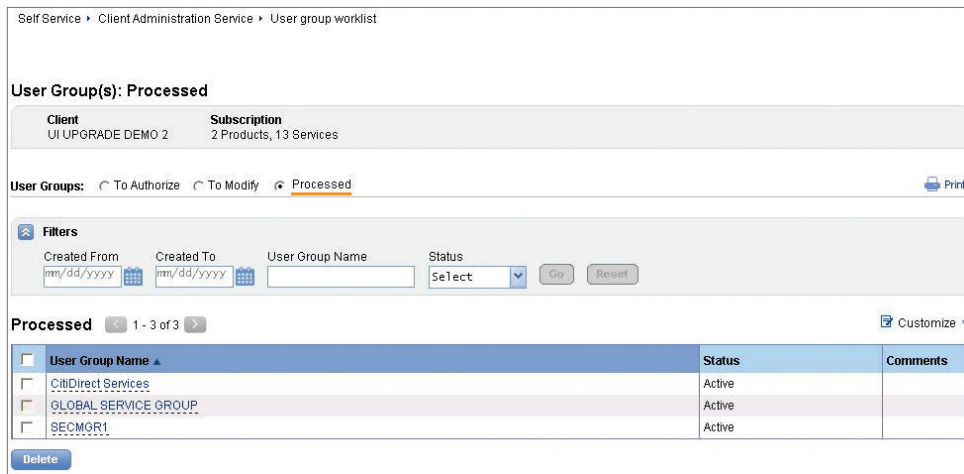


4. If you click on the User Group name of any record, the detail editable page for that User Group record will open which is similar to the Create User Group page.
5. You can modify or repair same fields entered during the creation of that User Group.
6. After modification if you click on Submit, the record is validated against all processing logic. If the validation is successful, you will see a confirmation message and move the record to Pending Authorization status. Records in Pending Authorization state will be visible under To Authorize queue under User Group Worklist.
7. If you click on Save, The record is validated against all processing logic. If the validation is successful, system will save the record and move it to Saved status. Records in Saved state will be visible under To Modify queue under User Group Worklist.
8. If you click on Cancel, you will lose all edited data and you will be navigated back to To Modify queue. A dialogue box will open for your confirmation of the cancel.



You can do the following steps with the **Processed** data:

9. You have to click Processed on the User Group Worklist page. The page will be as below.



Self Service > Client Administration Service > User group worklist

User Group(s): Processed

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

User Groups: [To Authorize](#) [To Modify](#) [Processed](#) [Print](#)

Filters

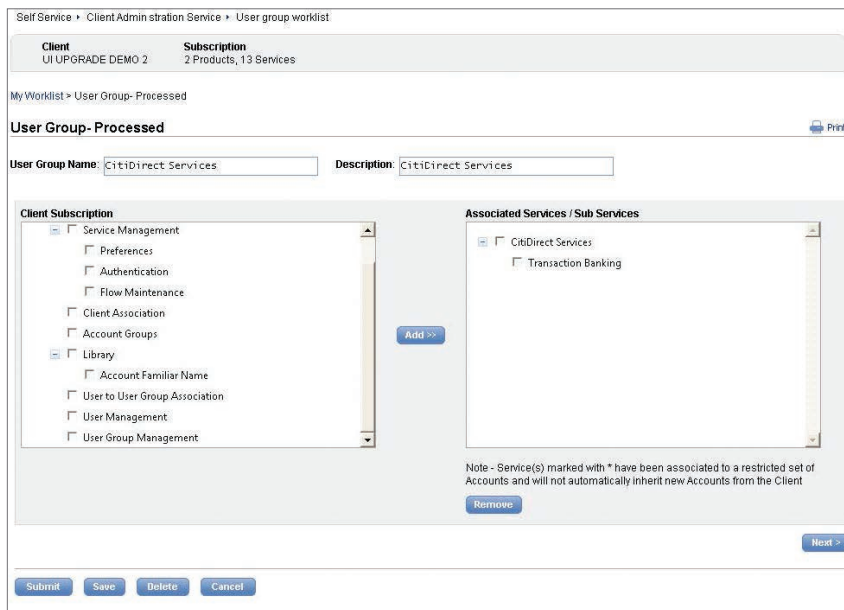
Created From: Created To: User Group Name: Status: [Go](#) [Reset](#)

Processed 1 - 3 of 3 [Customize](#)

<input type="checkbox"/>	User Group Name	Status	Comments
<input type="checkbox"/>	CitiDirect Services	Active	
<input type="checkbox"/>	GLOBAL SERVICE GROUP	Active	
<input type="checkbox"/>	SECUMGR1	Active	

[Delete](#)

10. If you click on the User Group name of any record, the detail editable page for that User Group record will open as User Group Processed. The Work flow status for this record will also display as Processed.



Self Service > Client Administration Service > User group worklist

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

My Worklist > User Group - Processed [Print](#)

User Group - Processed

User Group Name: Description:

Client Subscription

- Service Management
 - Preferences
 - Authentication
 - Flow Maintenance
 - Client Association
 - Account Groups
- Library
 - Account Familiar Name
 - User to User Group Association
 - User Management
 - User Group Management

[Add >>](#)

Associated Services / Sub Services

- CitiDirect Services
 - Transaction Banking

[Remove](#)

Note - Service(s) marked with * have been associated to a restricted set of Accounts and will not automatically inherit new Accounts from the Client

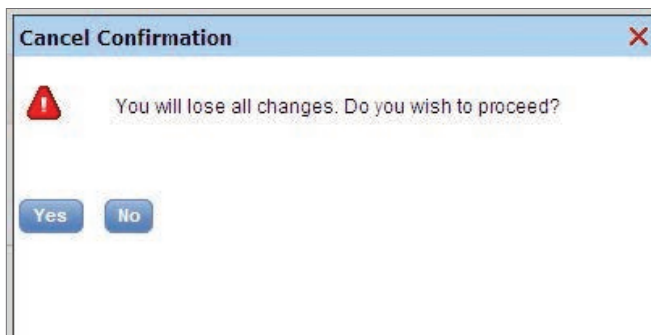
[Next >](#)

[Submit](#) [Save](#) [Delete](#) [Cancel](#)

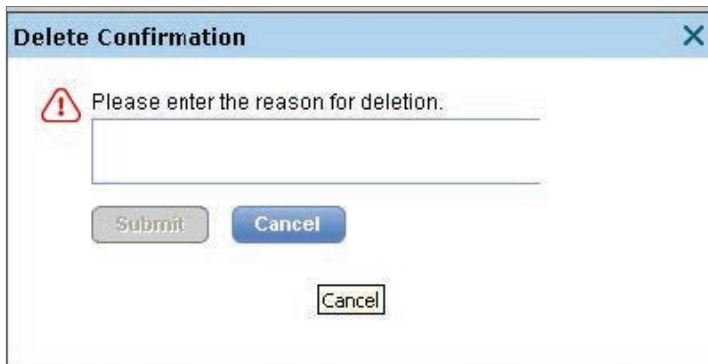
11. You can save, submit, cancel or delete User Group in CitiDirect in this page.

12. After modification if you click on Submit, the record is validated against all processing logic. If the validation is successful, you will see a confirmation message and move the record to Pending Authorization status. Records in Pending Authorization state will be visible under To Authorize queue under User Group Worklist.

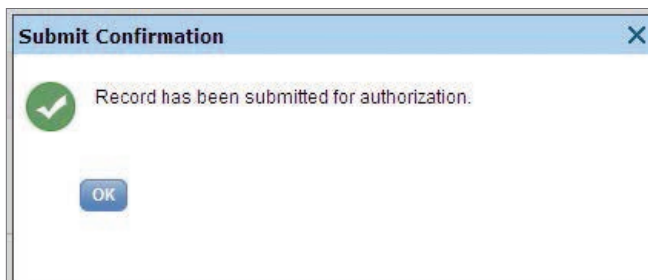
13. If you click on Save, The record is validated against all processing logic. If the validation is successful, system will save the record and move it to Saved status. Records in Saved state will be visible under To Modify queue under User Group Worklist.
14. If you click on Cancel, you will lose all edited data and you will be navigated back to To Modify queue. A dialogue box will open for your confirmation of the cancel.



15. Delete will allow you to delete records. Every delete of Every Record will prompt the User Group to input reason for deletion.



16. Deleted records will move to Pending Authorization for Delete state and will be visible under To Authorize queue under User Group Worklist. After Authorization the record will be logically deleted.



Note: If you have selected multiple records to delete, this reason must apply to all User Group profiles selected. If each User Group profile has a different reason for deletion, you must select and delete each one individually. Once deleted, the users associated to the group will lose the entitlement to those products and services instantaneously.

View All User Groups

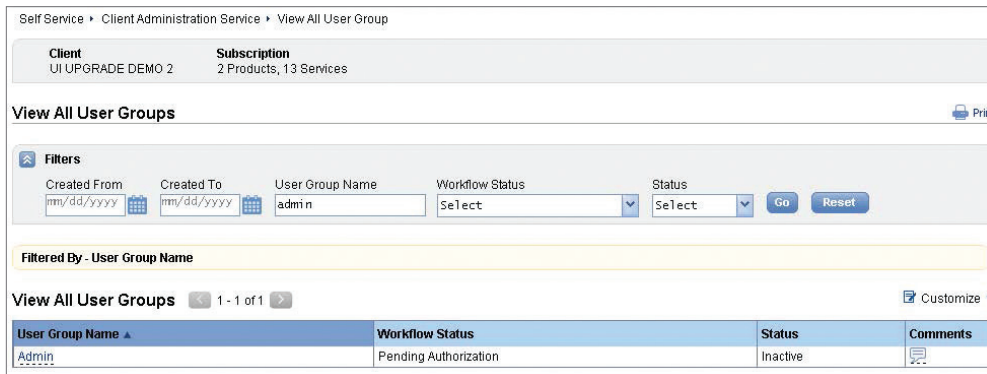
This View All User Groups contains a comprehensive list of all User Group profiles, including processed profiles and those awaiting authorization or repair. This information is useful because it provides a snapshot of the current state of all User Group profiles, letting you know which steps to take next and prevents the creation of duplicate profiles.

Under this you can do the following:

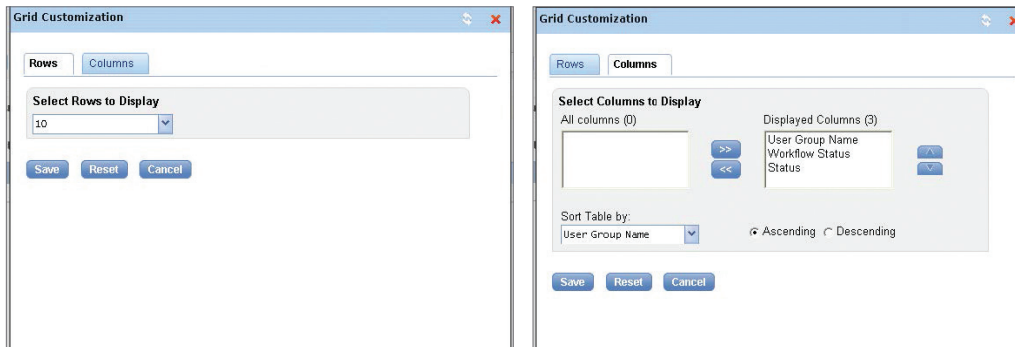
1. On the portal menu, View All User Groups can be accessed through Self Service under Client Administration Service.



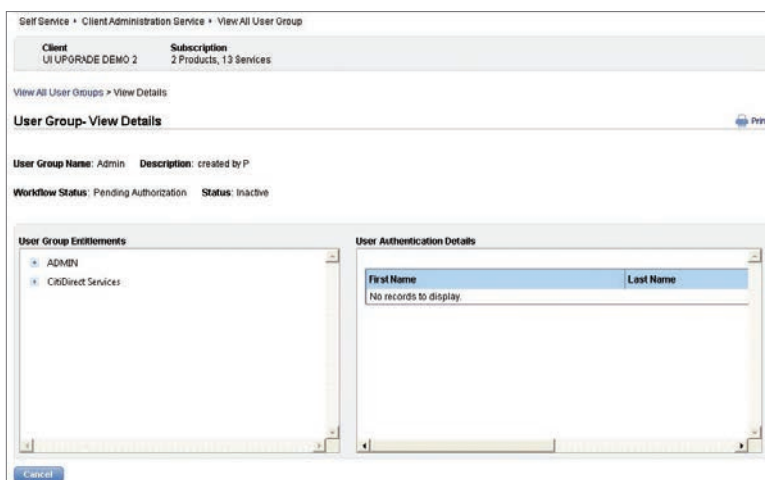
2. The list can be filtered as in To Authorize.



3. You can customize this page by clicking on Customize. A dialogue box will open where you can configure to see more numbers of rows, rearrange the columns for display and sort the table.



4. Clicking on the first name of a record will take you to the detailed page where you can see the information for that User Group.



5. Clicking on cancel will take you back to the list of all User Groups.

User Group Association Maintenance

After creating the user and user group, you will associate them through User Group Association. A user can be associated to multiple user groups based on the need of the job to be performed in your organization. Additionally, any new user created in the future in the system can be associated to user groups through this infrastructure. Also a user group can be required to be removed for a user because of the change of role in the organization or employment transition.

This association is to be reviewed periodically by Security Manager for all the users to check its relevance.

Under this you can do the following:

1. Create User Group Association
 - a. Submit
 - b. Save
 - c. Cancel
2. User Group Association Worklist
 - a. To Authorize
 - b. To Modify
 - c. Processed
3. View All User Group Association

Create User Group Association

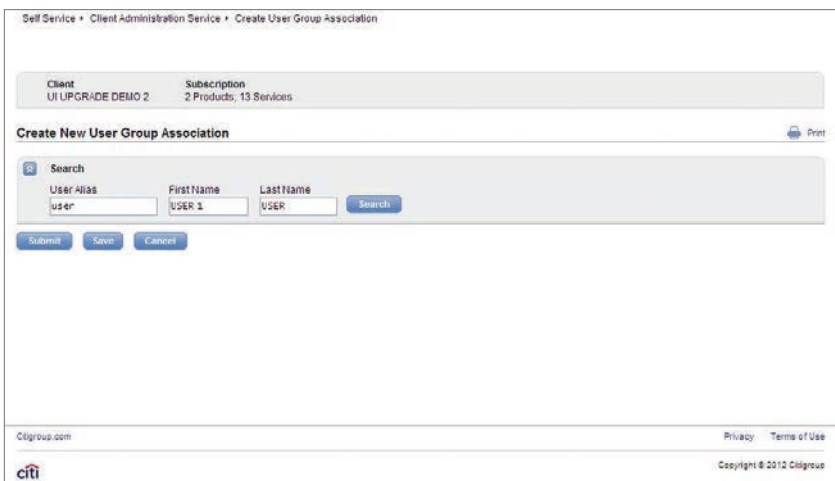
You will be using this feature to associate users with user groups. You can choose them to associate with multiple groups based on their job role in your organization.

Create new User Group Association by following the steps below:

1. On the portal menu, Create User Group Association can be accessed through Self Service under Client Administration Service.




- Click on Create User Group Association to load the page. You have to enter the user alias, first name of last name to find the user.



- Once the user is searched, you will see the client definition of the user under client name. You will also be able to search the User Group.

Self Service > Client Administration Service > Create User Group Association

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

Create New User Group Association  Print

Search

User Alias: First Name: Last Name:



Users Found 1 - 1 of 1

<input type="checkbox"/>	User Alias	First Name	Last Name	Email	Status
<input type="checkbox"/>	user1@citi.com	User 1	User		Active

Client Name: UI UPGRADE DEMO 2 User Group:

Citigroup.com Privacy Terms of Use Copyright © 2012 Citigroup

- Clicking on the search icon on the above screen will open a dialogue box to search the user group. You can enter the user group name or click on search to view all user groups.

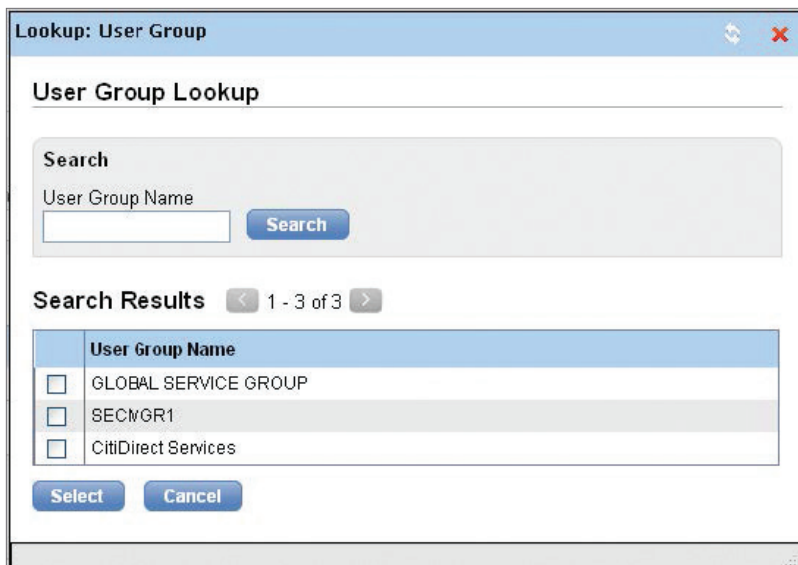
Lookup: User Group  

User Group Lookup

Search

User Group Name:

- The below is the dialogue box with the list of all user groups. The applicable user group for the user can be selected by checking the box.



Lookup: User Group

User Group Lookup

Search

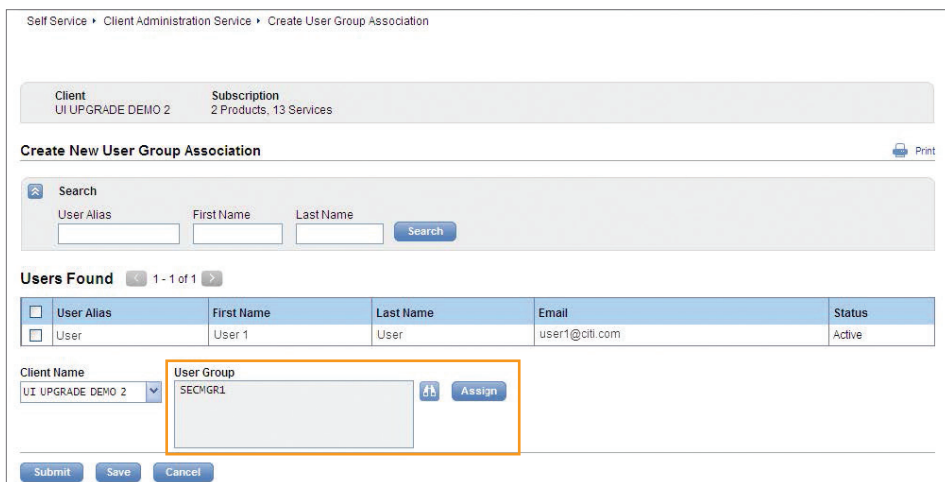
User Group Name **Search**

Search Results < 1 - 3 of 3 >

	User Group Name
<input type="checkbox"/>	GLOBAL SERVICE GROUP
<input type="checkbox"/>	SECNGR1
<input type="checkbox"/>	CitiDirect Services

Select **Cancel**

- In the following step, the selected user groups will be displayed in the screen in the user group text box.



Self Service > Client Administration Service > Create User Group Association

Client
UI UPGRADE DEMO 2

Subscription
2 Products, 13 Services

Create New User Group Association [Print](#)

Search

User Alias First Name Last Name **Search**

Users Found < 1 - 1 of 1 >

<input type="checkbox"/>	User Alias	First Name	Last Name	Email	Status
<input type="checkbox"/>	User	User 1	User	user1@citi.com	Active

Client Name
UI UPGRADE DEMO 2

User Group
SECNGR1 **Assign**

Submit **Save** **Cancel**

- The user name can be checked in the above screen for which these user groups are to be assigned. Once you click the assign, it will display the user groups that are being assigned to it. You have the option of un-assigning it.

Self Service > Client Administration Service > Create User Group Association

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

Create New User Group Association Print

Search

User Alias: First Name: Last Name:

Users Found 1 - 1 of 1

<input type="checkbox"/>	User Alias	First Name	Last Name	Email	Status
<input type="checkbox"/>	User	User 1	User	user1@cit.com	Active

Client Name: UI UPGRADE DEMO 2 User Group: SECMGR1

User Group Association 1 - 1 of 1

<input type="checkbox"/>	First Name	Last Name	Client Name	Group Name
<input type="checkbox"/>	User 1	User	UI UPGRADE DEMO 2	SECMGR1

- If you click on the Group Name, a dialogue box will open to display the details of entitlement criteria for that group.

User Group Details Refresh Close

User Group Details

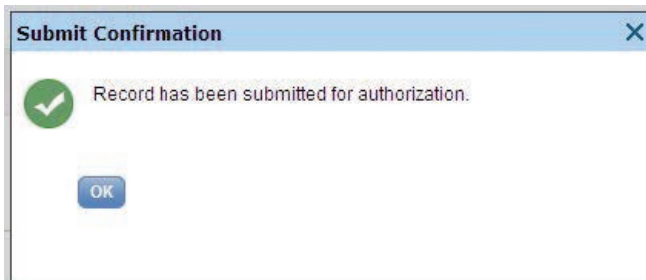
- ADMIN
 - + Service Management
 - + Client Association
 - + User to User Group Association
 - + User Management
 - + User Group Management

- Clicking on Save will save the User Group Association and move it to To Modify queue.

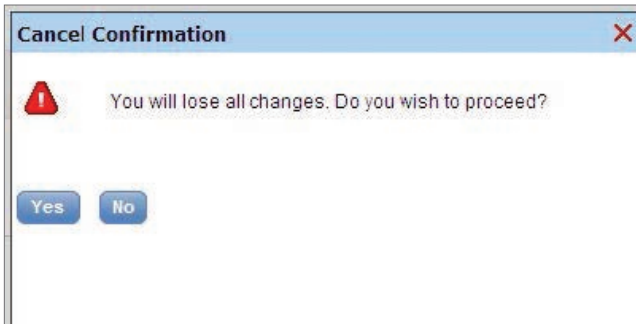
Save Confirmation Close

Record has been saved as draft.

10. If you click Submit, the record will be saved and will be submitted for authorization. Another user will find it in the To Authorize queue.



11. Cancel will not save any of the entered data in the page. A dialogue box will open for your confirmation of the cancel.



User Group Association Worklist

You can use this for the maintenance of the created User Group Associations. Under this you can do the following:

1. To Authorize
 - a. Authorize
 - b. Send to Repair
 - c. Reject
2. To Modify
 - a. Recall Request
 - b. Save
 - c. Submit
 - d. Cancel
3. Processed
 - a. Save
 - b. Submit
 - c. Cancel
 - d. Delete

To Authorize

When created User Group Associations are ready for authorization, they are listed on the To Authorize worklist where they can be selected and authorized by an entitled Security Manager.

You will see only the records that you are entitled to authorize. If you created the User Group Association, you cannot authorize it. During the authorization process, User Group Association records can be authorized, sent to repair or rejected. The User Group Association remains inactive until it is authorized.

To Authorize you can follow the steps below:

1. On the portal menu, User Group Association Worklist can be accessed through Self Service under Client Administration Service.



2. Click on the User Group Association Worklist will take you to the To Authorize page.

User Group Association(s): To Authorize

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

User Group Associations: To Authorize To Modify Processed [Print](#)

Filters

Created From: Created To: First Name: Last Name: User Group:


Workflow Status: Status:

To Authorize 1 - 1 of 1 [Customize](#)

<input type="checkbox"/>	Last Name	First Name	Assigned User Groups	Workflow Status	Status	Comments
<input type="checkbox"/>	User	User 1	3	Pending Authorization	Inactive	

- By default it will display all User Group Associations pending to be authorized except the ones created by you. You can filter by entering created from and to, first name, last name, work flow status and status.
- Once the User Group Associations are displayed under To Authorize in multiple rows, they can be individually or group selected.
- These selected User Group Associations can be authorized, sent to repair or rejected.
- Once authorized, it will be confirmed in a dialogue box.
- If you click on Send to Repair on the To Authorize screen for any User Group Association, a dialogue box will prompt to enter the reason. Entering the reason will help others to understand why repair is required. The below is the screen for the Send to Repair Confirmation dialogue box.

Send to Repair Confirmation

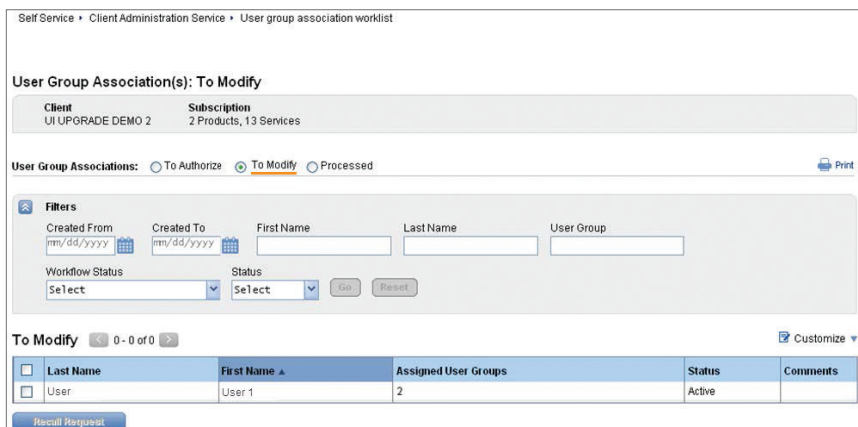
 Please enter reason for sending to repair.

- On Submit, User Group Association record will move to the To Modify queue under User Group Association Worklist with workflow status as Repair Required. One of you can repair it and resubmit for authorization.
- You can also reject a created User Group Association by clicking on the Reject on the To Authorize page.
- A dialogue box will open to enter the reason for rejection and once submitted, the record will be rejected. None of the Security Managers will be able to see the record in the To Authorize queue again. Rejected records will be visible in View All User Group Associations under Client Administration Service in Rejected state.

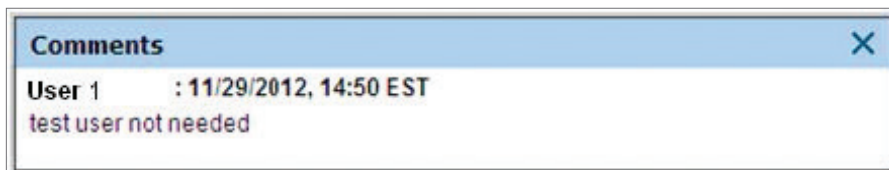
Note: You can reject a User Group Association because it is invalid and should not have been created. Rejecting a User Group Association deletes it from the application, but creates an audit trail of your action, along with your reason for the rejection.

To Modify you can follow the steps below:

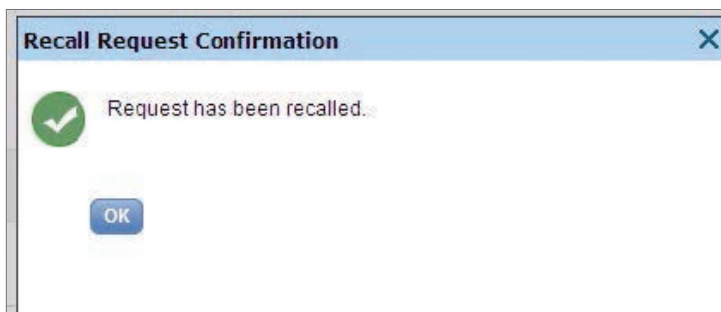
1. You have to click To Modify on the User Group Association Worklist page. The page will be as below. You can recall a request from this page by selecting single or all records.



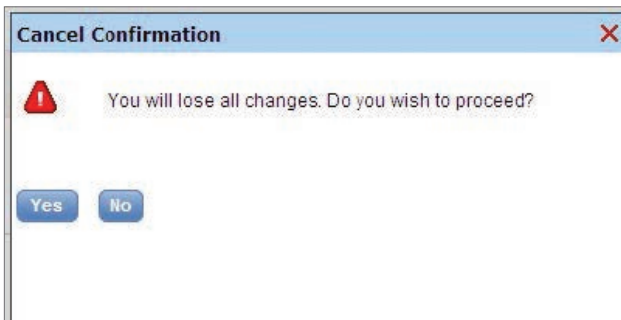
2. The reasons can be inserted while rejecting, sending for repair, recalling, etc. These reasons can be seen, but clicking the comments column in the To Authorize or View All User Group Associations page. It will display the user name, date, time and the comment.



3. Once recall is requested it will open the Recall Request Confirmation dialogue box. The reason can be entered and it can be confirmed. The Confirmed dialogue box will be as below and the record will be logically deleted.

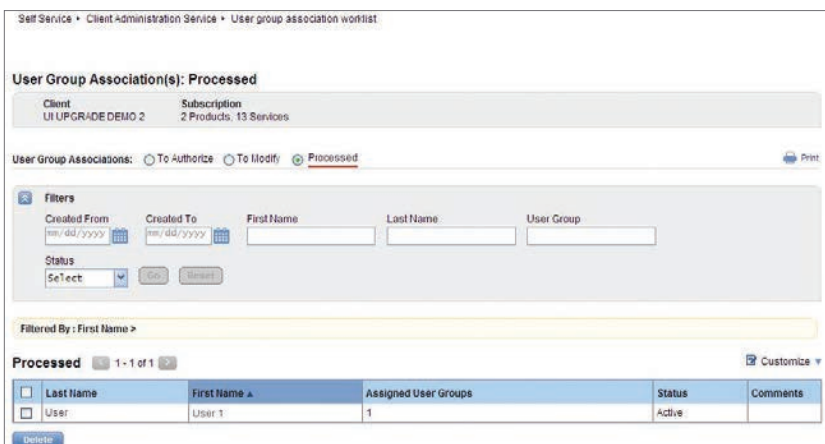


4. If you click on the User Group Association name of any record, the detail editable page for that User Group Association record will open which is similar to the Create User Group Association page.
5. You can modify or repair same fields entered during the creation of that User Group Association.
6. After modification if you click on Submit, the record is validated against all processing logic. If the validation is successful, you will see a confirmation message and move the record to Pending Authorization status. Records in Pending Authorization state will be visible under To Authorize queue under User Group Association Worklist.
7. If you click on Save, The record is validated against all processing logic. If the validation is successful, system will save the record and move it to Saved status. Records in Saved state will be visible under To Modify queue under User Group Association Worklist.
8. If you click on Cancel, you will lose all edited data and you will be navigated back to To Modify queue. A dialogue box will open for your confirmation of the cancel.



You can do the following steps with the Processed data:

9. You have to click Processed on the User Group Association Worklist page. The page will be as below.



10. If you click on the First Name column for any record, the editable detail page for that User Group Association record will open as User Group Association Processed. The Work flow status for this record will also display as Processed. Clicking on View Details will display the details for that user entered during creating the user. New user group can be assigned or existing user groups can be unassigned.

Self Service > Client Administration Service > User group association worklist

Client: UI UPGRADE DEMO 2 **Subscription:** 2 Products, 13 Services

My Worklist > User Group Association- Processed

User Group Association- Processed

Workflow Status: Processed User Status: Active

General Information

User Alias: dudu9005 First Name: DUBILLY Last Name: DUBILLY Middle Name: [View Details](#)

Safeword

Safeword ID Exists Get New Safeword ID Do not issue Safeword

User Group Association

Client Name: UI UPGRADE DEMO 2 User Group: [Assign](#)

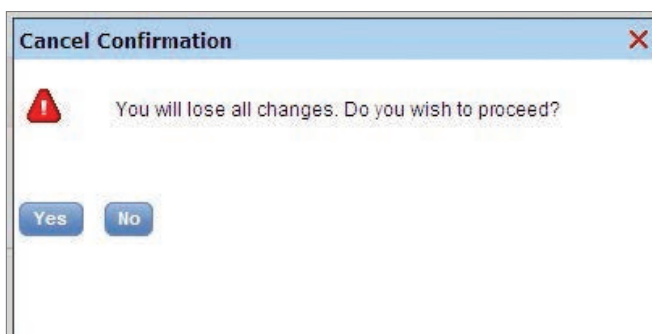
User Group Association 1 - 1 of 1

First Name	Last Name	Client Name	Group Name	Association Date
<input type="checkbox"/> User 1	User	UI UPGRADE DEMO 2	GLOBAL SERVICE GROUP	11/29/2012 12:00:00 AM

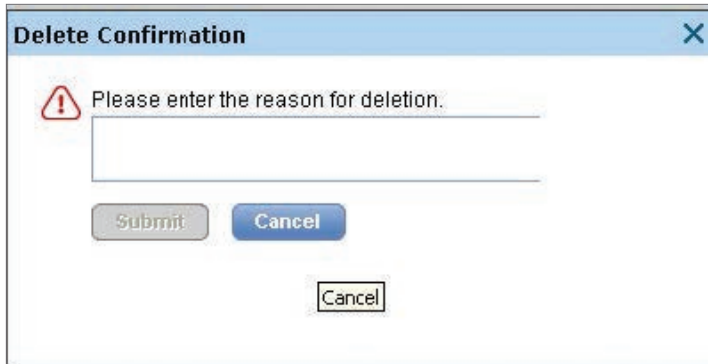
[Unassign](#)

[Submit](#) [Save](#) [Delete](#) [Cancel](#)

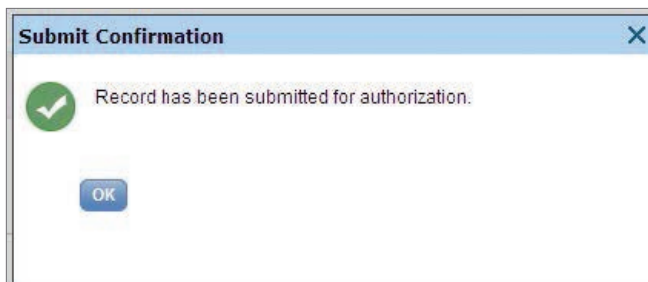
11. You can save, submit, cancel or delete User Group Association in CitiDirect in this page.
12. After modification if you click on Submit, the record is validated against all processing logic. If the validation is successful, you will see a confirmation message and move the record to Pending Authorization status. Records in Pending Authorization state will be visible under To Authorize queue under User Group Association Worklist.
13. If you click on Save, The record is validated against all processing logic. If the validation is successful, system will save the record and move it to Saved status. Records in Saved state will be visible under To Modify queue under User Group Association Worklist.
14. If you click on Cancel, you will lose all edited data and you will be navigated back to To Modify queue. A dialogue box will open for your confirmation of the cancel.



15. Delete will allow you to delete records. Every delete of Every Record will prompt the User Group Association to input reason for deletion.



16. Deleted records will move to Pending Authorization for Delete state and will be visible under To Authorize queue under User Group Association Worklist. After Authorization the record will be logically deleted.



Note: If you have selected multiple records to delete, this reason must apply to all User Group Association profiles selected. If each User Group Association profile has a different reason for deletion, you must select and delete each one individually. Once deleted, the users associated to the group will lose the entitlement to those products and services instantaneously.

View All User Group Association

View All User Group Associations contains a comprehensive list of all User Group Association profiles, including processed profiles and those awaiting authorization or repair. This information is useful because it provides a snapshot of the current state of all User Group Association profiles, letting you know which steps to take next and prevents the creation of duplicate profiles.

Under this you can do the following:

1. On the portal menu, View All User Group Associations can be accessed through Self Service under Client Administration Service.



2. The list can be filtered as in To Authorize.

Self Service > Client Administration Service > View All User Group Association

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

View All User Group Associations Print

Filters

Created From: Created To: First Name: Last Name: User Group:

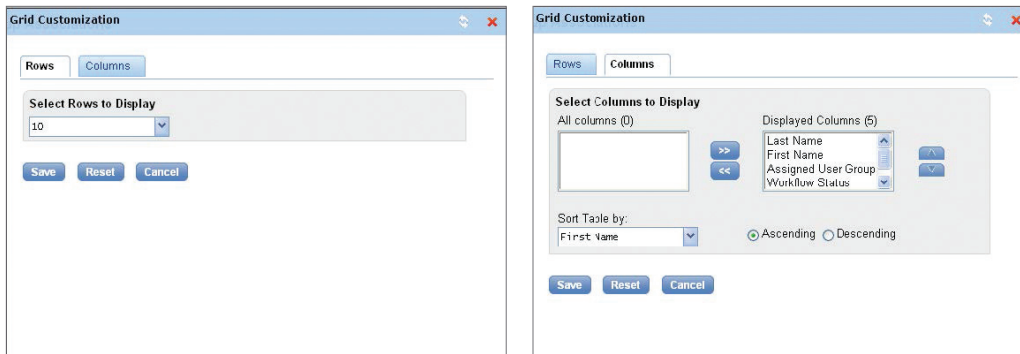
Workflow Status: Status:

Filtered By: First Name >

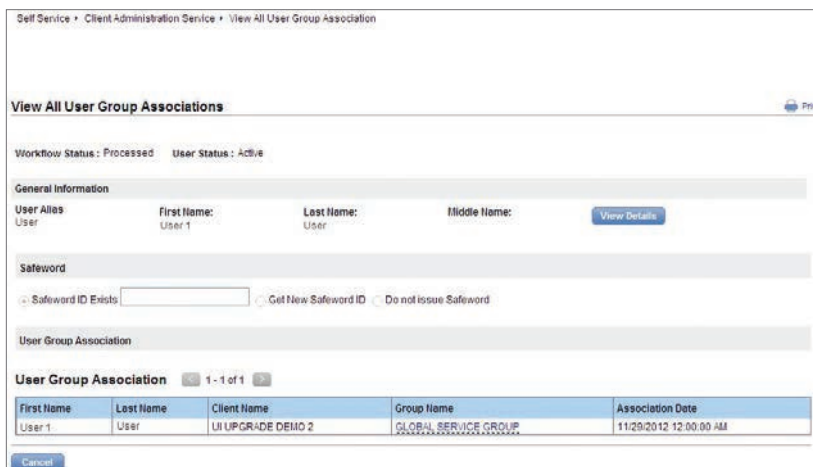
All User Group Associations 1 - 1 of 1 Customize

Last Name	First Name ▲	Assigned User Groups	Workflow Status	Status	Comments
User	User 1	1	Processed	Active	

3. You can customize this page by clicking on Customize. A dialogue box will open where you can configure to see more numbers of rows, rearrange the columns for display and sort the table.



- Clicking on the first name of a record will take you to the detailed page where you can see the information for that User Group Association.



- Clicking on cancel will take you back to the list of all User Group Associations.

User Entitlements

Use the User Entitlements service class to perform the following:

- Assign user entitlements.
- Authorize user entitlements.
- Modify or repair user entitlements.
- Delete user entitlements.
- View user entitlements.

The User Entitlements service class enables you to link, or assign, access profiles to individual user profiles. Access profiles define exactly what actions a user can perform when he or she is working in CitiDirect. For more information on access profiles, refer to the Access Profiles section of this guide. User Entitlement can be accessed from the Applet through User Administration.

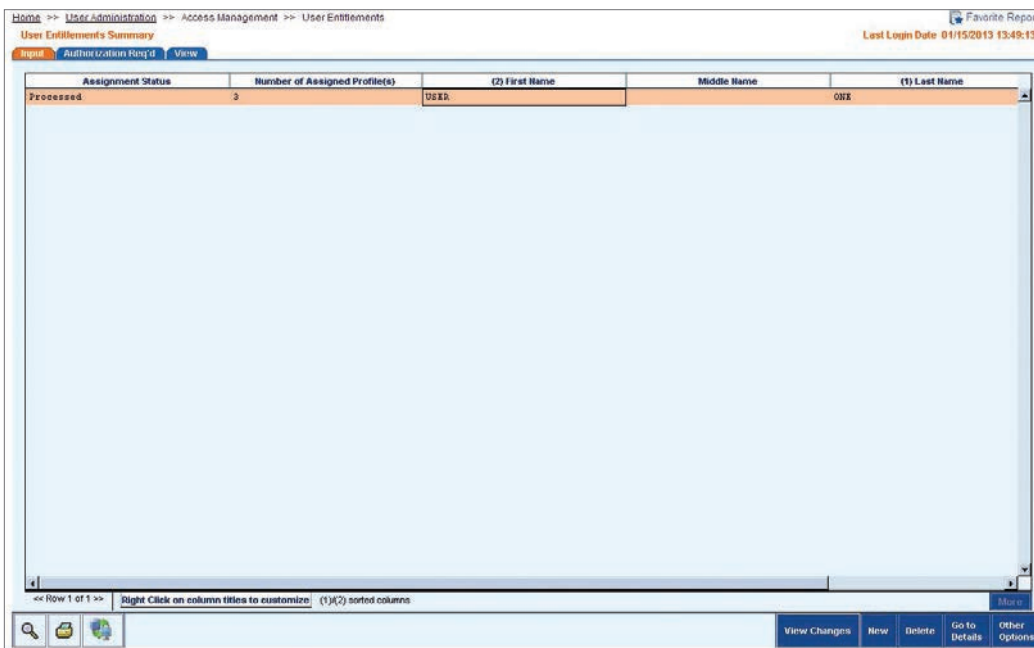
Assigning User Entitlements

Assigning access profiles to user profiles defines how the user will work in the CitiDirect application. Assign user entitlements by following the steps below:

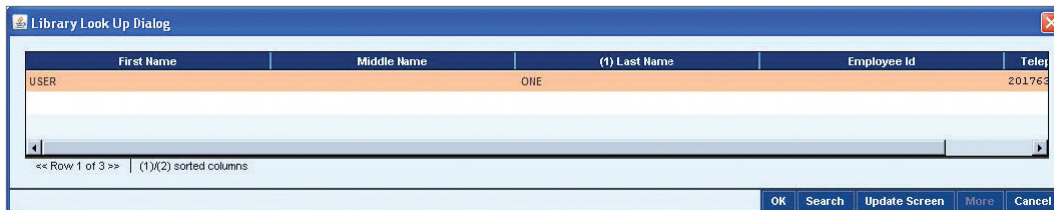
1. On the CitiDirect menu under User Administration, click on User Entitlements as shown below.



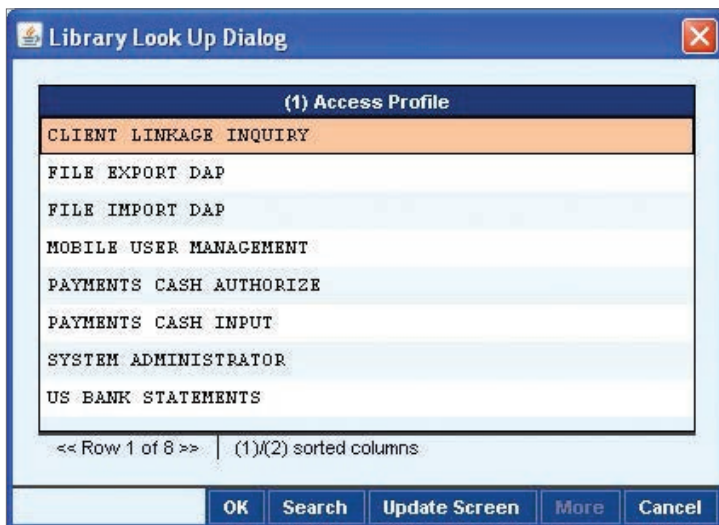
2. The User Entitlements Summary form appears.

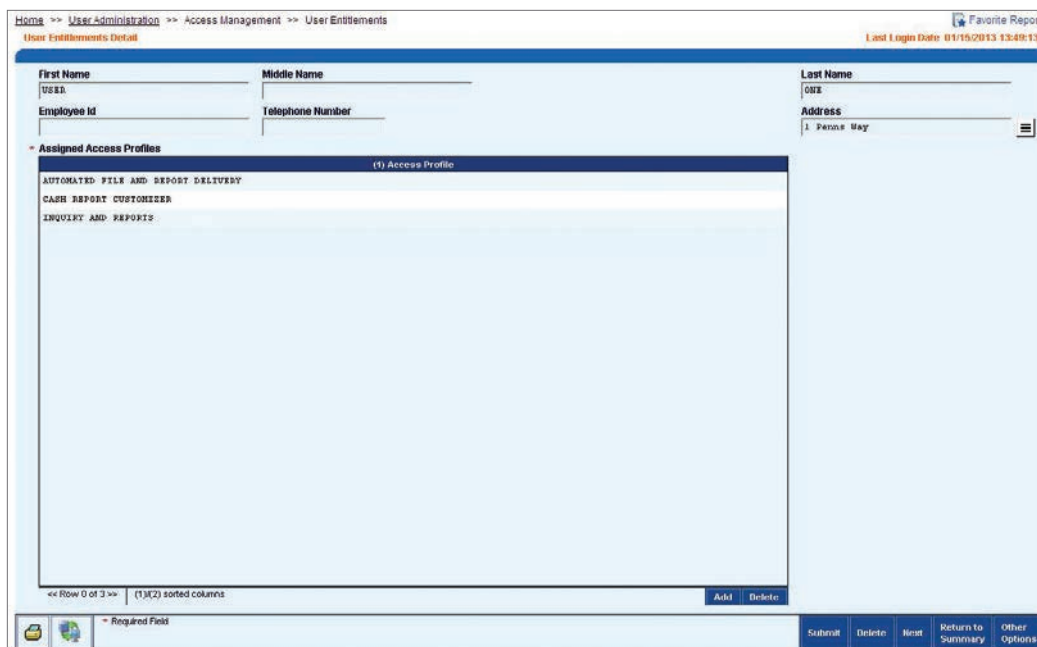


3. Click the New button. A Library Look Up Dialogue box appears.



4. Select one or more user profiles and click the OK button. The User Entitlements Detail form appears.
5. In the Assigned Access Profiles list box, click the Add button. A Library Look Up Dialogue box appears. A list of all processed access profiles for your organization is displayed. If a profile is not listed, check to ensure that it has been fully authorized and its status is Processed.
6. Select one or more access profiles and click the OK button. You can assign multiple access profiles to one user. The profiles are listed in the Assigned Access Profiles list box.





Home >> User Administration >> Access Management >> User Entitlements
 User Entitlements Detail Favorite Reports
Last Login Date: 01/15/2013 13:46:13

First Name: USER Middle Name: Last Name: CIBZ
 Employee Id: Telephone Number: Address: 1 Penna Way

Assigned Access Profiles

(1) Access Profile		
AUTOMATED FILE AND REPORT DELIVERY		
CASH REPORT CUSTOMIZER		
INQUIRY AND REPORTS		

<< Row 0 of 3 >> (1)(2) sorted columns Add Delete

Required Field Submit Delete Next Return to Summary Other Options

7. Click the Submit button to save the user entitlements record and enter it into the authorization queue. The status of the record changes to Authorization Required.

The user will not be able to access the services included in his or her assigned access profile until the user entitlement record is authorized.

Authorizing User Entitlements

When user entitlement records are ready for authorization, they are listed on the User Entitlements Summary form, on the Authorization Required tab where they can be selected and authorized by an entitled Security Manager. Authorization of user entitlement records is the final step in activating the user and giving him or her access to CitiDirect Online Banking.

You will see only the records you are entitled to authorize. The user cannot access CitiDirect until a second Security Manager authorizes his or her user entitlements record. If you created the user entitlements record, you cannot authorize it. During the authorization process, user entitlements records can be authorized, sent to repair or deleted.

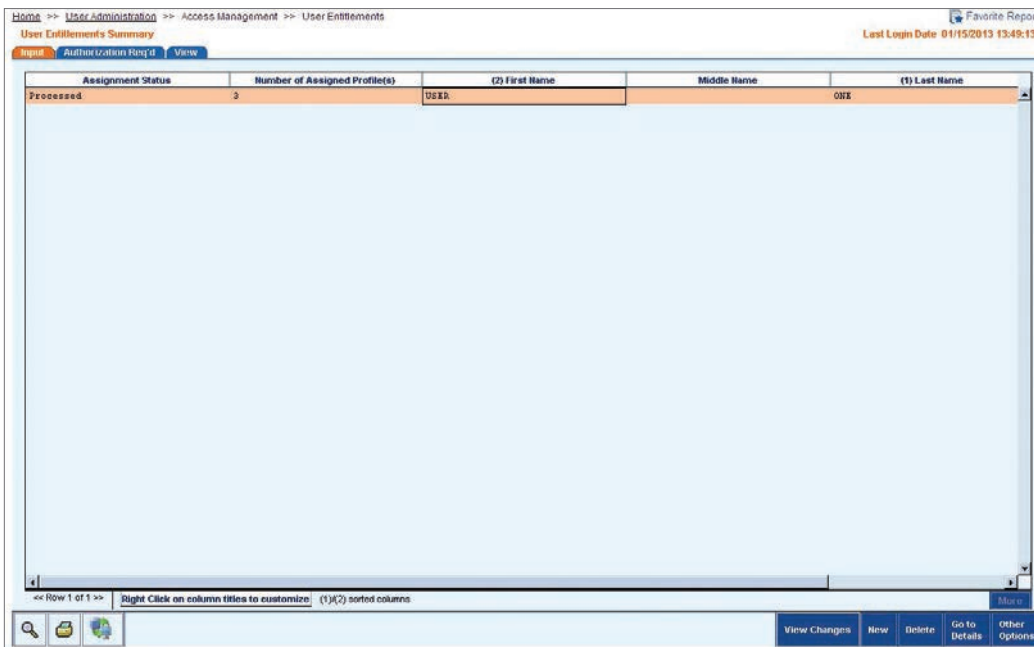
You are responsible for SafeWord card user support, which includes communicating initial sign-on procedures and rules.

Authorize user entitlements records by following the steps below:

1. On the CitiDirect menu under User Administration, click on User Entitlements as shown below.



2. The User Entitlements Summary form appears.



3. Click the Authorization Required tab to view a list of records awaiting your authorization.

Home >> User Administration >> Access Management >> User Entitlements

User Entitlements Summary Favorite Reports

Last Login Date 01/15/2013 13:49:13

Input **Authorization Req'd** View

Assignment Status	Number of Assigned Profile(s)	(2) First Name	Middle Name	(1) Last Name
Authorization Required	3	USER		ONE

Row 1 of 1 >> Right Click on column titles to customize | (1)(2) sorted columns

View Changes Authorize Send to Repair Reject Go to Details Other Options

- Select one or more user entitlements records to be authorized. Click the Go to Details button. The User Entitlements Detail form appears.

Home >> User Administration >> Access Management >> User Entitlements

User Entitlements Detail Favorite Reports

Last Login Date 01/15/2013 13:49:13

First Name: USER Middle Name: Last Name: ONE

Employee Id: Telephone Number: Address: 1 Penns Way

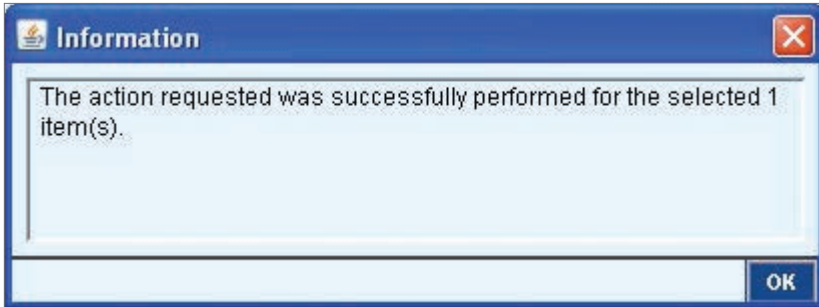
Assigned Access Profiles (1) Access Profile

AUTOMATED FILE AND REPORT DELIVERY
CASH REPORT CUSTOMIZER
INQUIRY AND REPORTS

Row 0 of 3 >> (1)(2) sorted columns

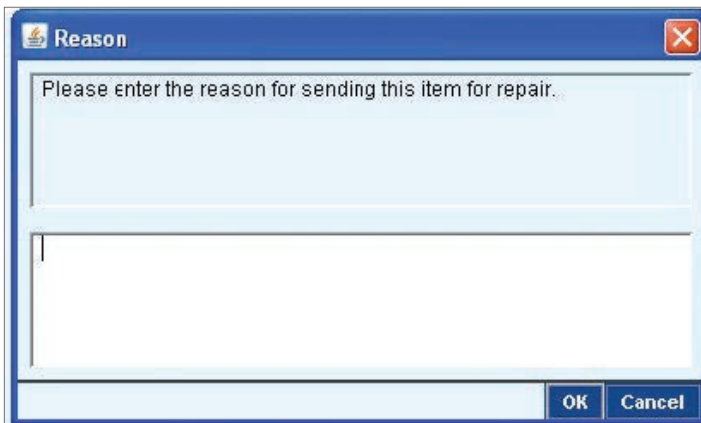
Required Field Add Authorize Send to Repair Reject Next Return to Summary Other Options

5. Review the accuracy of the assigned access profiles to verify that the record is ready for authorization. Then, proceed with one of the following steps.
 - Click the Authorize button if the user entitlements records are ready for activation. A message appears.



Click the OK button to close the box.

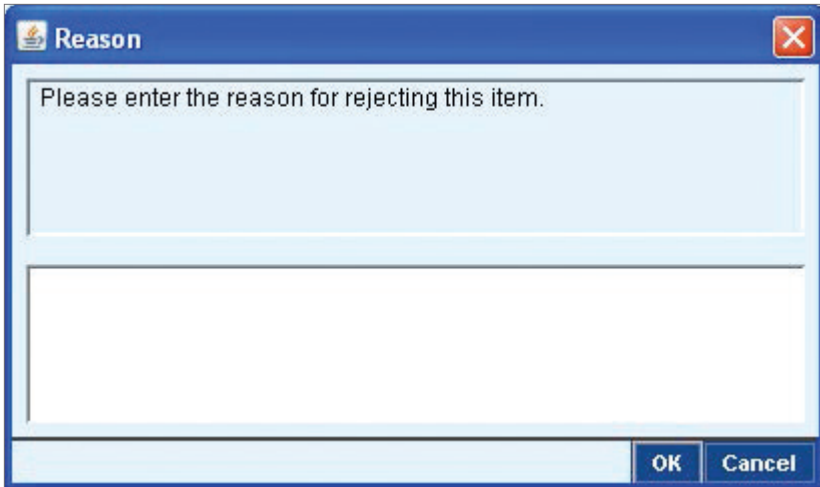
- Click the Send to Repair button if the user entitlement record requires correction. A dialogue box appears.



Enter the reason for the repair request and then click the OK button to close the dialogue box. The status of the record changes to Repair Required.

Note: Entering a detailed explanation gives the creator a starting point for revising the user entitlements record before resubmitting it.

- Click the Reject button if the User Entitlements record needs to be deleted. A dialogue box appears.



Enter the reason for the rejection/deletion and then click the OK button. The user entitlements record is deleted from the application.

Note: Rejecting entitlements deletes it from the application, but creates an audit trail of your action, along with your reason for rejection. If the user is assigned other access profiles, he or she can still use CitiDirect but not for the services included in the user entitlement record that has been rejected.

- Click the Next button if you have selected multiple records, and you do not want to perform any action on the current user entitlements record.

Modifying or Repairing User Entitlements

Periodically, you may need to modify or change the entitlements of existing users. These changes are made in user entitlement records that have already been processed. In addition, there may be instances when you are required to repair records that contain certain errors.

The original user entitlement remains active until a second Security Manager has authorized the modification. The Status column on the Input tab indicates the current status of each record and assists you in determining what action, if any, is needed.

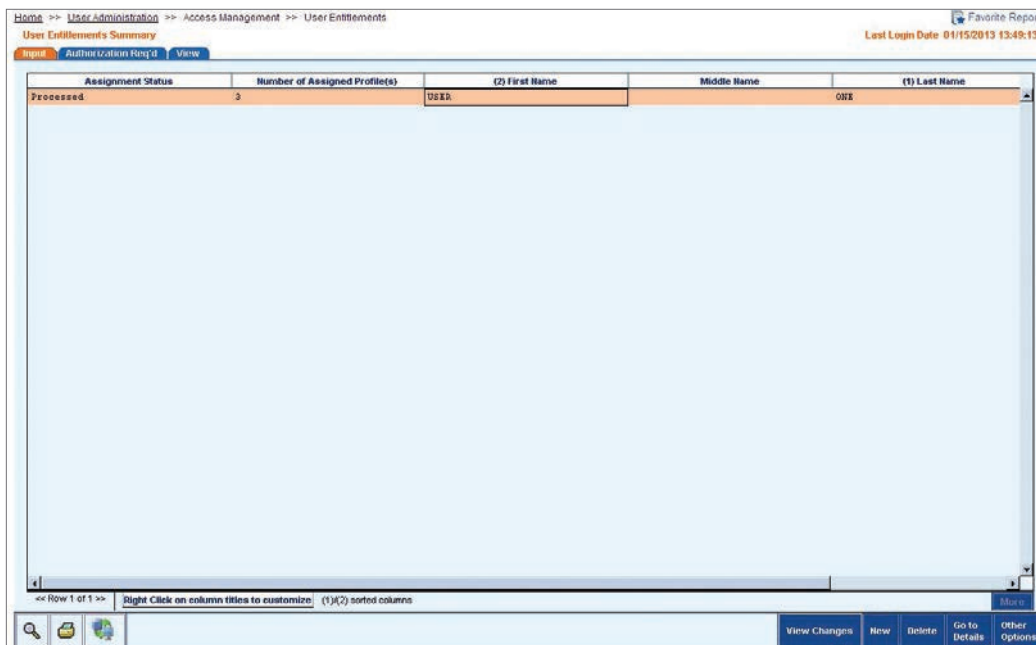
1. A status of Processed means that the record has been authorized, and is currently being used in CitiDirect.
2. A status of Input means that the record has been auto-saved, but not submitted. Additional information must be entered before it can be submitted for processing.
3. All user entitlements records with a status of Invalid (the profile did not pass CitiDirect server validation) are listed on the Input tab where they can be selected and modified or repaired.
4. A status of Repair Required means that another Security Manager has determined that the user entitlement record contains incorrect information.

Modify or repair user entitlements records by following the steps below:

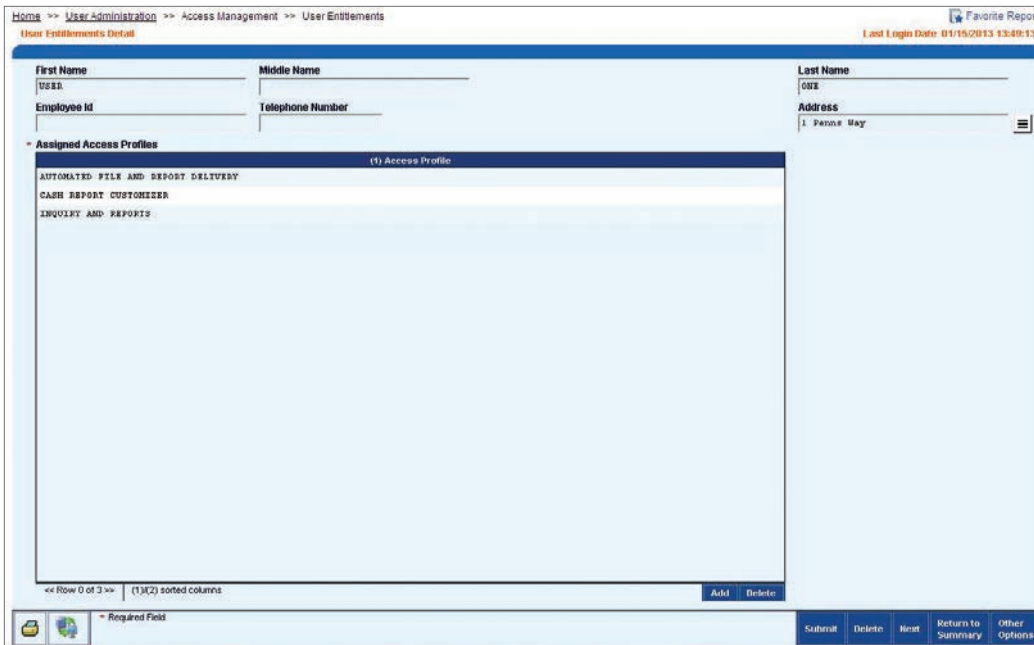
1. On the CitiDirect menu under User Administration, click on User Entitlements as shown below.



2. The User Entitlements Summary form appears.

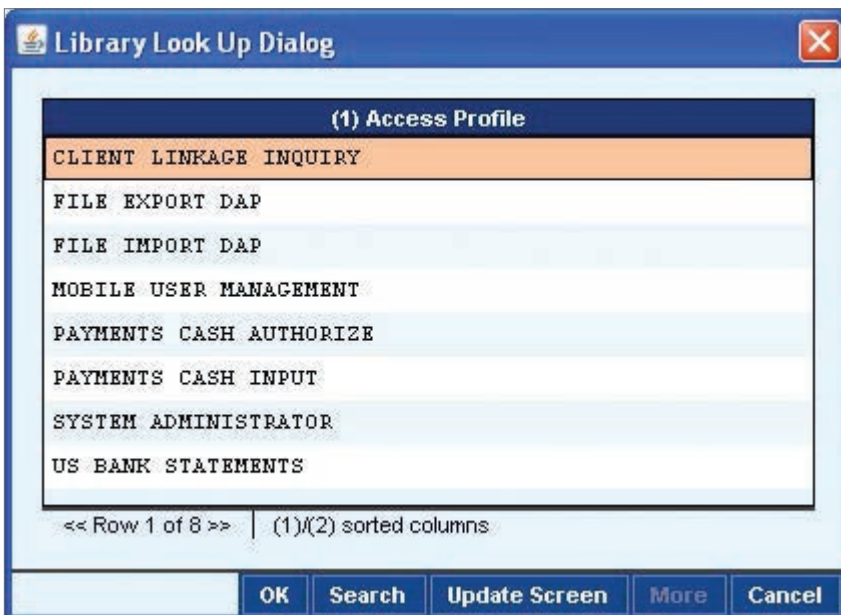


3. Select one or more user entitlements records to modify, and then click the Go to Details button. The User Entitlements Detail form appears.



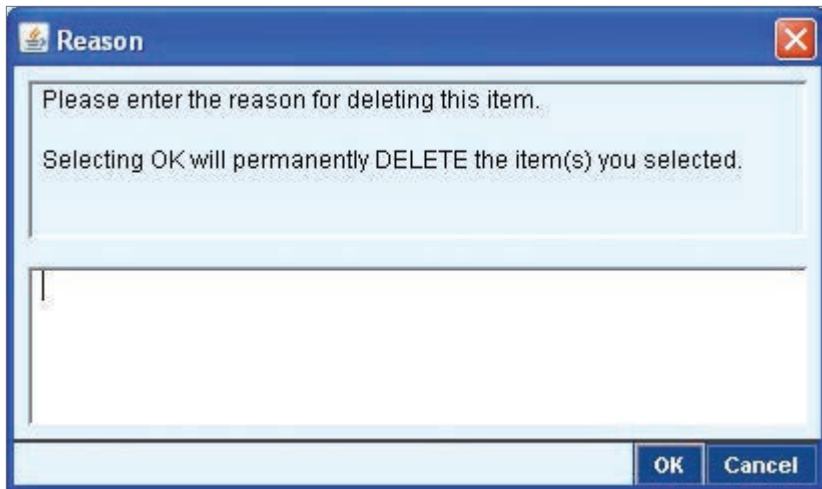
4. Proceed with one of the following steps:

- Click the Add button in the Assigned Access Profiles list box to assign additional access profiles to this user. A Library Look Up Dialogue box appears.



Select one or more access profiles, and then click the OK button to close the dialogue box. The profiles appear in the Assigned Access Profiles list box.

- Select an access profile in the Assigned Access Profiles list box and click the Delete button to delete a profile. A warning message appears.



Click the OK button to close the dialogue box.

5. Review the modified or repaired user entitlements record for accuracy and then click the Submit button. The status of the record is changed to Authorization Required and it is moved to the authorization queue. The modification or repair is not final until the profile is authorized.

Deleting User Entitlements Records

Occasionally, it is necessary to terminate access to CitiDirect and remove users from the platform. To do this properly, you must first delete the appropriate user entitlement record, and then delete the user profile. For information on deleting the user profile, please refer to the "Deleting User Profiles" section of this guide.

Delete user entitlements records by following the steps below.

1. On the CitiDirect menu under User Administration, click on User Entitlements as shown below.



2. The User Entitlements Summary form appears.

Home >> User Administration >> Access Management >> User Entitlements

User Entitlements Summary Favorite Reports

Last Login Date: 01/15/2013 13:49:13

Input Authorization Req'd View

Assignment Status	Number of Assigned Profile(s)	(2) First Name	Middle Name	(1) Last Name
Processed	3	DEED		ONE

<< Row 1 of 1 >> Right Click on column titles to customize (1)(2) sorted columns

View Changes New Delete Go to Details Other Options

3. Select one or more user entitlements records to delete, and then click the Delete button. A Reason dialogue box appears.

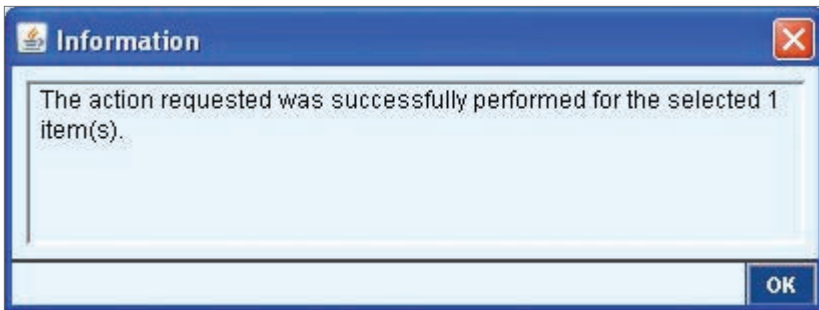
Reason ✖

Please enter the reason for deleting this item.

Selecting OK will permanently DELETE the item(s) you selected.

OK Cancel

4. Enter the reason for deleting the user entitlements record, and then click the OK button. A dialogue box appears.



Note: The reason for the deletion must apply to all selected user entitlements records. If each user entitlements record has a different reason for deletion, you must select and delete each record individually.

- Click the OK button to close the dialogue box. The status of the user entitlements record is changed to Authorization Required for Delete. The record remains active until another Security Manager authorizes its deletion.

Viewing User Entitlements

The View tab contains a summary list of all user entitlements records, which are user profile records that have assigned access profiles. This information is useful because it gives a snapshot of the current state of each entitlement record, letting you know which steps to take next.

View user entitlements records by following the steps below:

- On the CitiDirect menu under User Administration, click on User Entitlements as shown below.



- The User Entitlements Summary form appears.

Home >> User Administration >> Access Management >> User Entitlements

User Entitlements Summary Favorite Reports
Last Login Date 01/15/2013 13:49:13

Input Authorization Req'd View

Assignment Status	Number of Assigned Profile(s)	(2) First Name	Middle Name	(1) Last Name
Processed	3	USER		ONR

<< Row 1 of 1 >> Right Click on column titles to customize (1)(2) sorted columns More

View Changes New Delete Go to Details Other Options

3. Click the View tab to view all user entitlements records in CitiDirect.

Home >> User Administration >> Access Management >> User Entitlements

User Entitlements Summary Favorite Reports
Last Login Date 01/15/2013 16:04:51

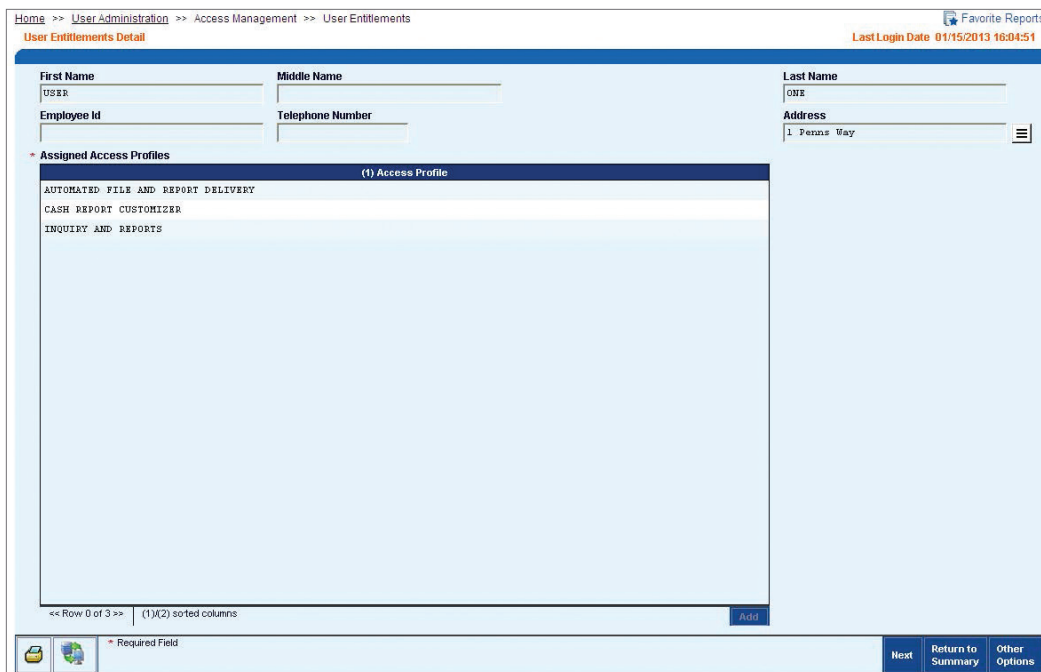
Input Authorization Req'd View

Assignment Status	Number of Assigned Profile(s)	(2) First Name	Middle Name	(1) Last Name
Processed	3	USER		ONR

<< Row 1 of 1 >> Right Click on column titles to customize (1)(2) sorted columns More

View Changes Go to Details Other Options

4. Select one or more records, and then click the Go to Details button. The User Entitlements Detail form appears.



Home >> User Administration >> Access Management >> User Entitlements

User Entitlements Detail Favorite Reports

Last Login Date 01/15/2013 16:04:51

First Name USER	Middle Name	Last Name ONE
Employee Id	Telephone Number	Address 1 Perms Way

* Assigned Access Profiles

(1) Access Profile
AUTOMATED FILE AND REPORT DELIVERY
CASH REPORT CUSTOMIZER
INQUIRY AND REPORTS

<< Row 0 of 3 >> (1)(2) sorted columns Add

Required Field Next Return to Summary Other Options

5. Review the access profiles in the Assigned Access Profiles list box.
6. If you selected more than one profile, click the Next button.

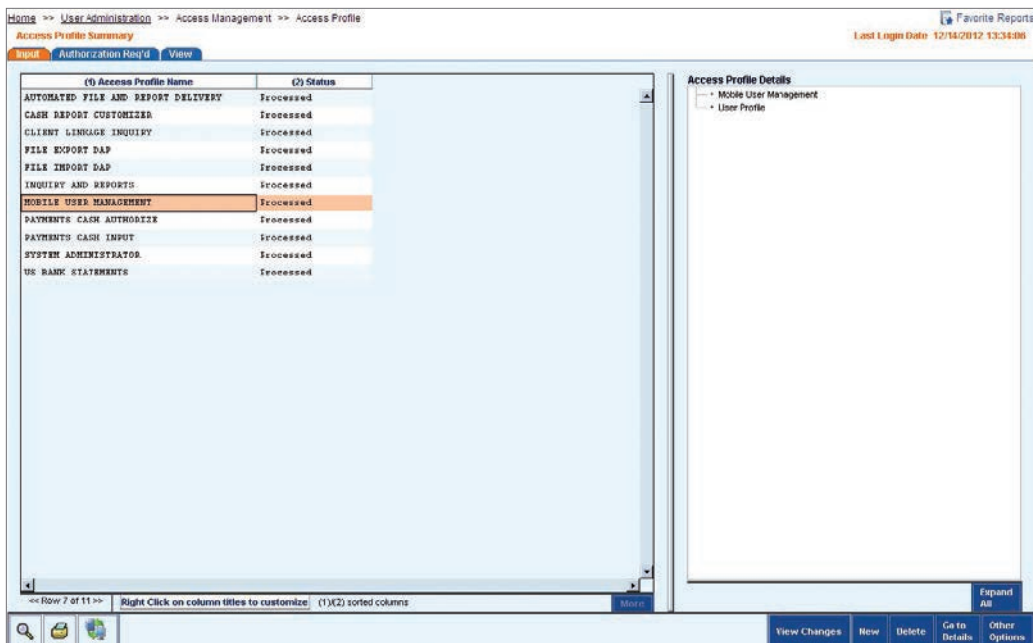
Note: You can run the Access Profile Detail Report to review all processed profiles and the entitlements included in each profile. For more information, refer to the "Access Profile Detail Report" section of this guide.

CitiDirect BE Mobile User Setup

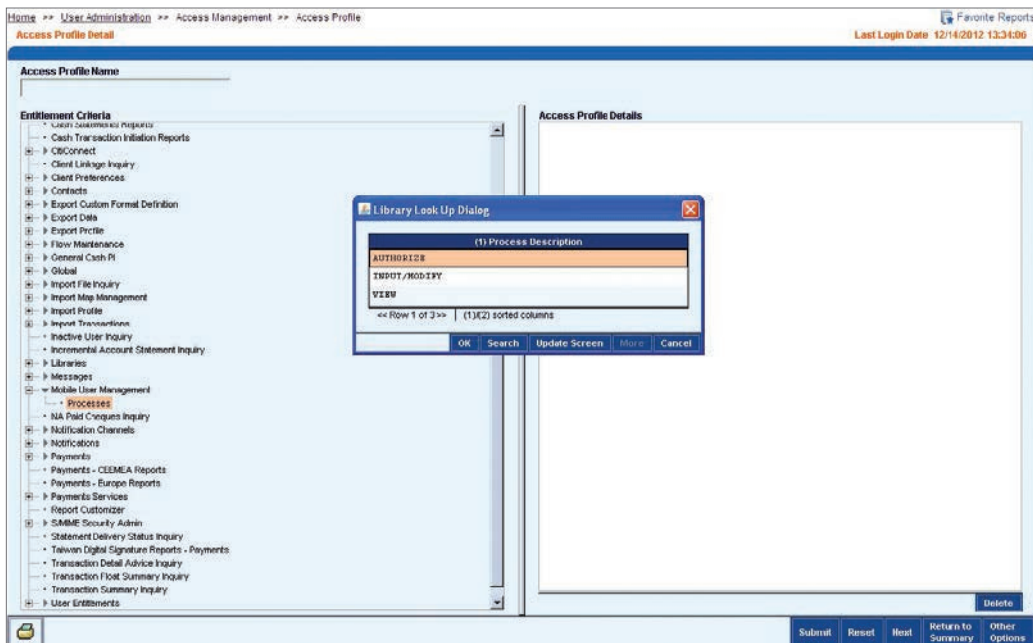
When setting up users for CitiDirect BE^S Mobile you will need to follow the below steps:

Access Profile – Onboarding:

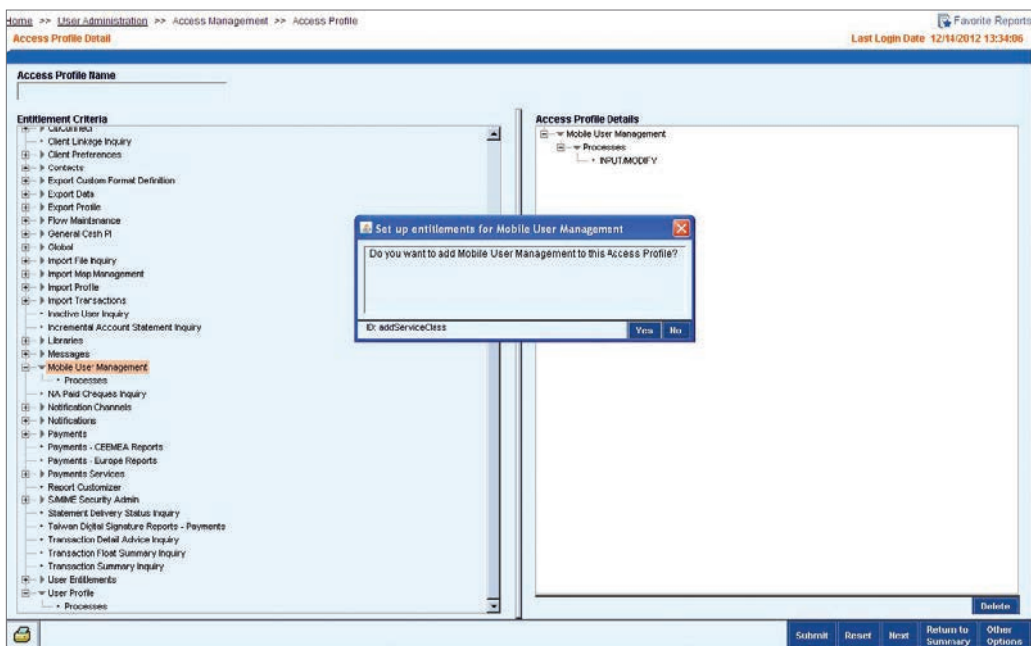
1. In the Applet, under User Administration -> Access Management -> Access profile click on "New" located at the bottom of the Access Profile summary screen.



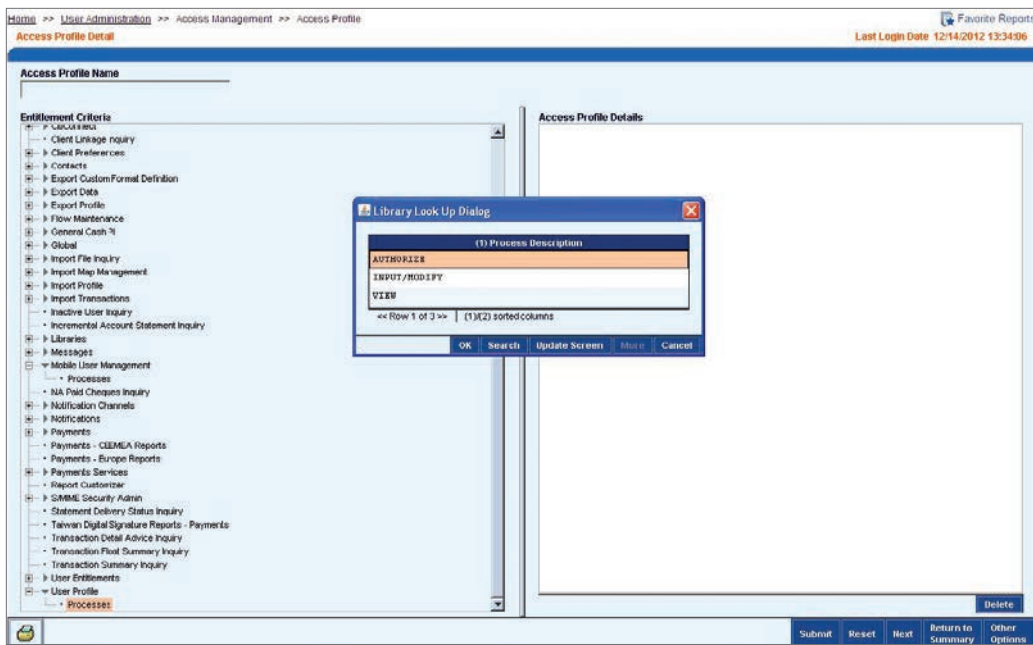
2. Scroll to Mobile User Management and click on processes. Within the library lookup dialogue, select the applicable processes and press Ok.



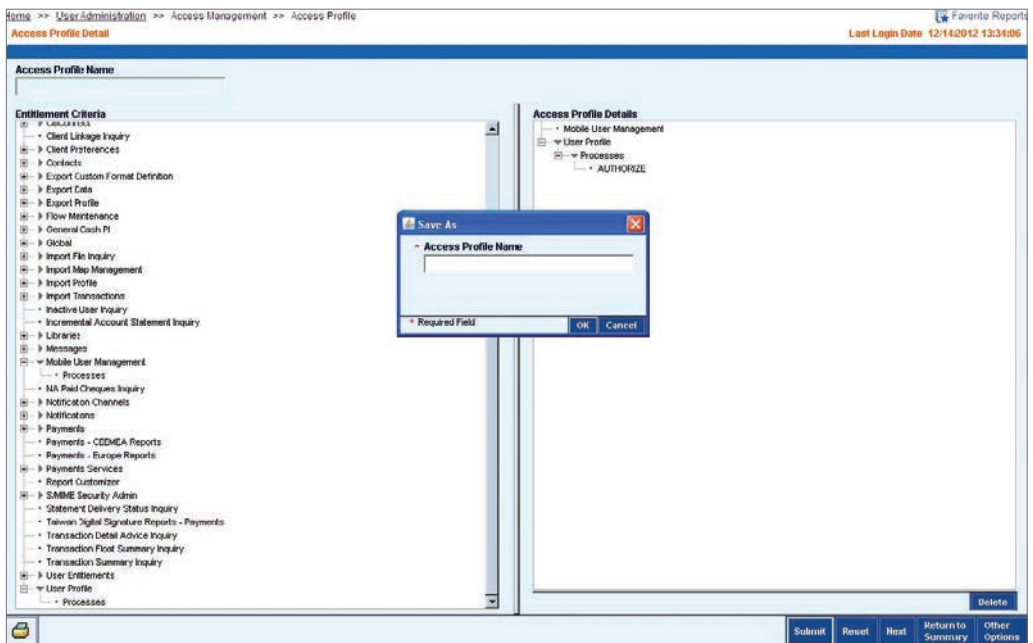
- If all the processes are applicable for the user, click on Mobile User Management in the entitlement criteria. It will open a dialogue box as below. Click OK to select all processes for that access profile. You will be able to see Mobile User Management under Access profile Details on the right-hand side.



3. Scroll to User Profile and use the same method as explained for Mobile User Management in the previous steps.

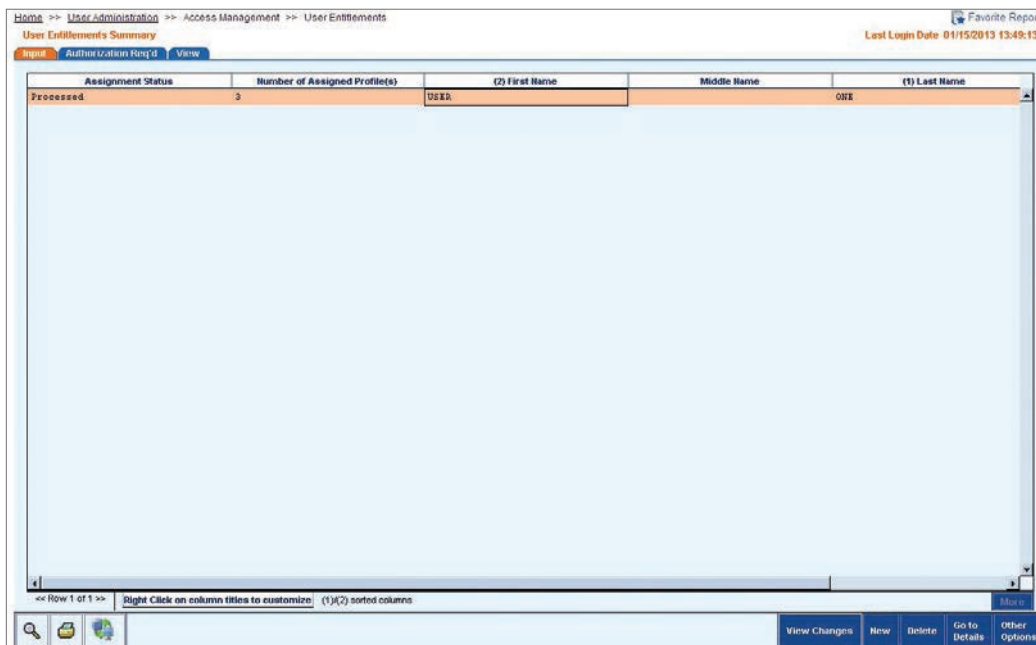


- Once the above steps have been completed the click Submit button located on the bottom of Access Profile Detail screen. Within the dialogue enter the name you wish to save the profile as. Please take note of this name as it will be used in a later step.



Entitling Client Security Manager Onboarding:

1. When entitling your Security Manager, there is no need to log out of the CitiDirect portal. Entitlements are automatically saved.
2. Once the access profile has been created you must add it to the client Security Managers' user profiles. Go to User Entitlements located at User Administration -> Access Management -> User Entitlements in the **Applet** page.

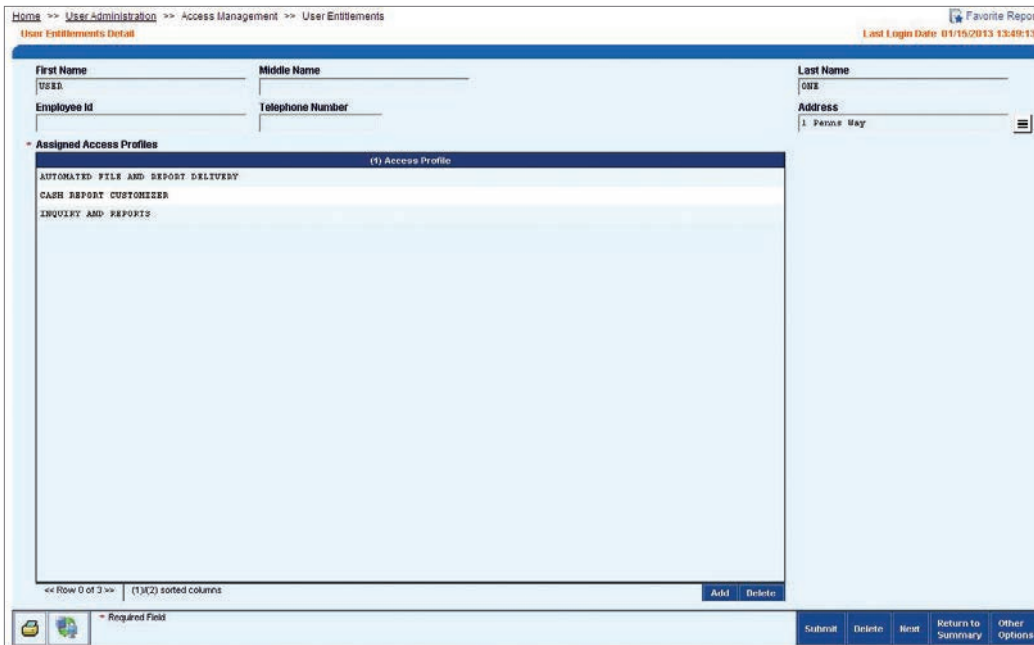


3. Once the New button has been clicked the User Library Look Up Dialogue popup box will be displayed. Select Client Security Manager.

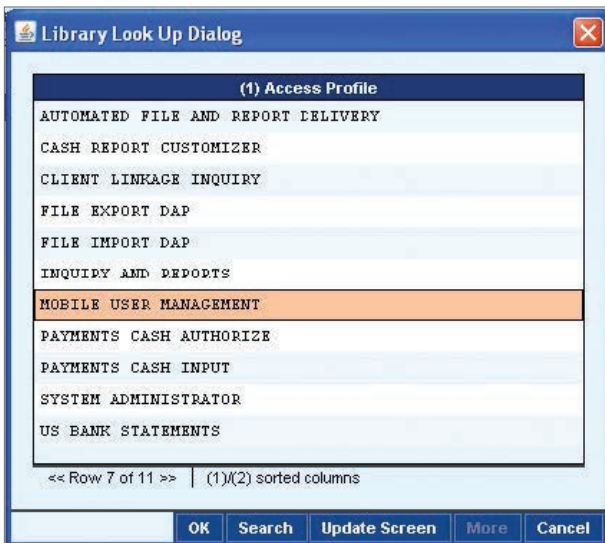


Note: If the Security Manager already has an existing profile, this step does not apply. The Search functionality is available to select Client Security Managers from the list of existing profiles.

4. Within the User Entitlements Detail screen click on the Add button located on the bottom of the Access Profile window.



5. In the Library Look Up Dialogue select the new Access Profile created as part step 2 above and Click OK.
6. Click on the Submit button located on the bottom of the User Entitlement screen to save the changes.

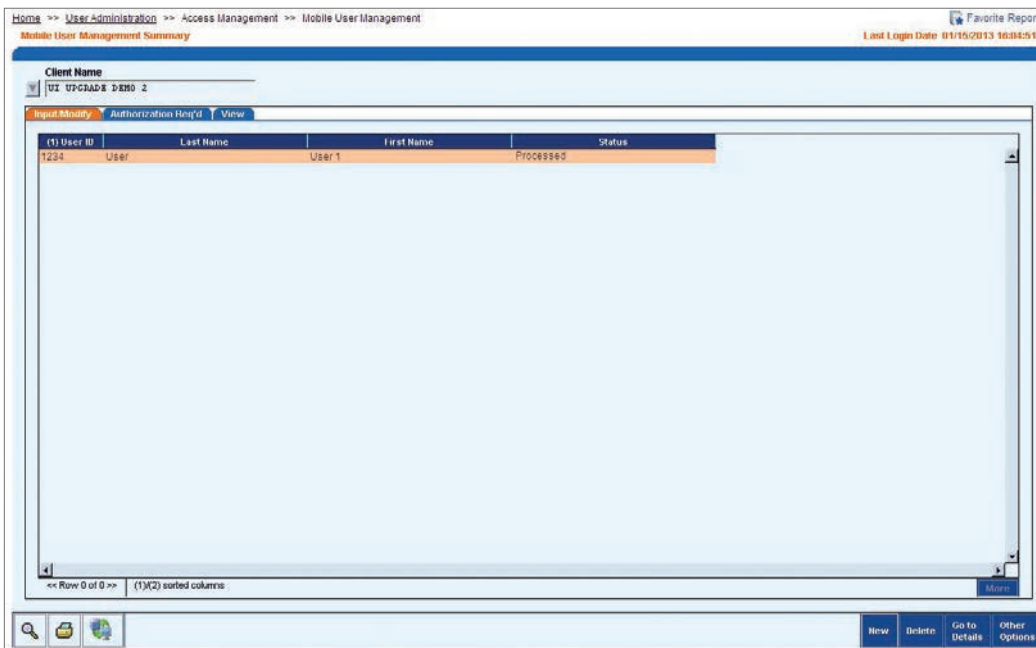


Entitling Users – Client Security Manager

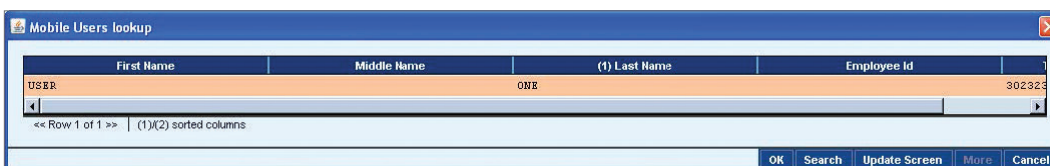
1. You need to log out of the portal before entitling new users.
2. Access Mobile User Management located under Access Management in the Applet menu.



3. Mobile User Management Summary page will open.

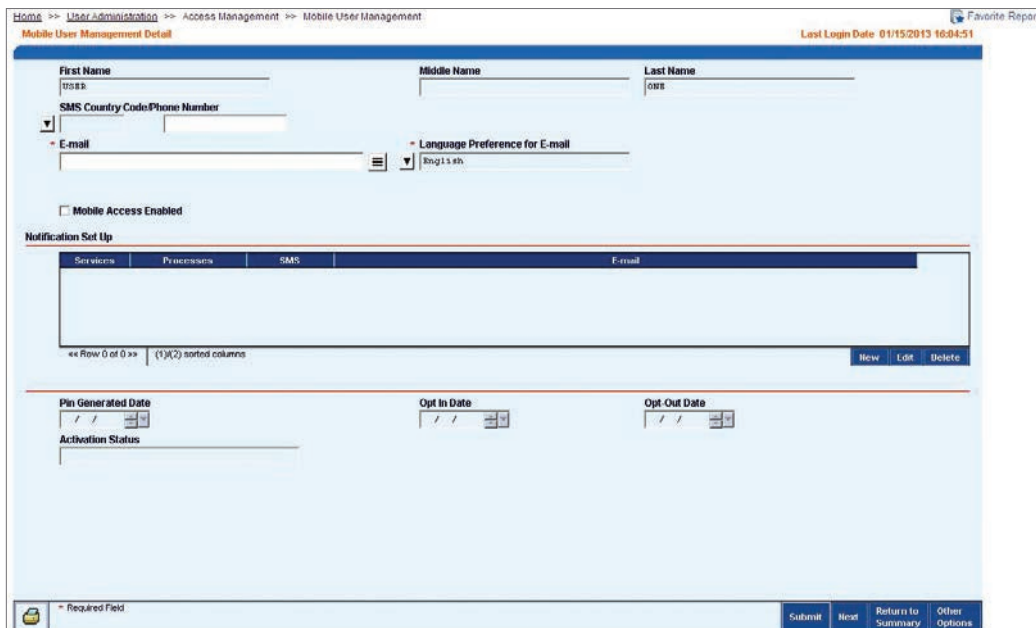


4. Once the client has been selected click New to select the user and set up Mobile Channel access and/or Notification and/or Event Notification.



5. On opening the user screen will be pre-populated with the following data from the users profile:

- First Name, Middle Name, Last Name



Home >> User Administration >> Access Management >> Mobile User Management

Mobile User Management Detail Last Login Date: 01/15/2013 16:04:51

Favorite Reports

First Name Middle Name Last Name

SMS Country Code/Phone Number

E-mail Language Preference for E-mail

Mobile Access Enabled

Notification Set Up

Services	Processes	SMS	E-mail

« Row 0 of 0 » (1)(2) sorted columns New Edit Delete

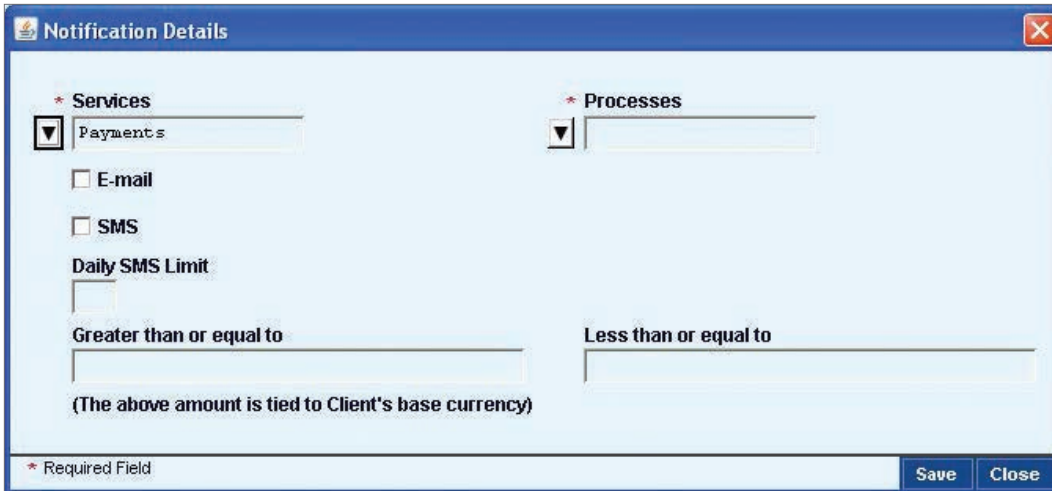
Pin Generated Date Opt In Date Opt Out Date

Activation Status

* Required Field Submit New Return to Summary Other Options

6. The Security Manager will be required to complete the required fields within the screen:

- SMS Country Code/Phone Number: Required for SMS Notifications.
- E-mail: Required if the users wish to receive the new payment authorization notification via e-mail.
- Services: Payments
- Processes: Authorize
- Mobile Access Enabled: Users can be configured to receive either one or both SMS and e-mail notifications. For example, clients can: Have mobile access, and only SMS, only e-mail, both SMS and e-mail, or no notifications. Have no mobile access and only SMS, only e-mail, both SMS and e-mail, or no notifications



7. New Notification:

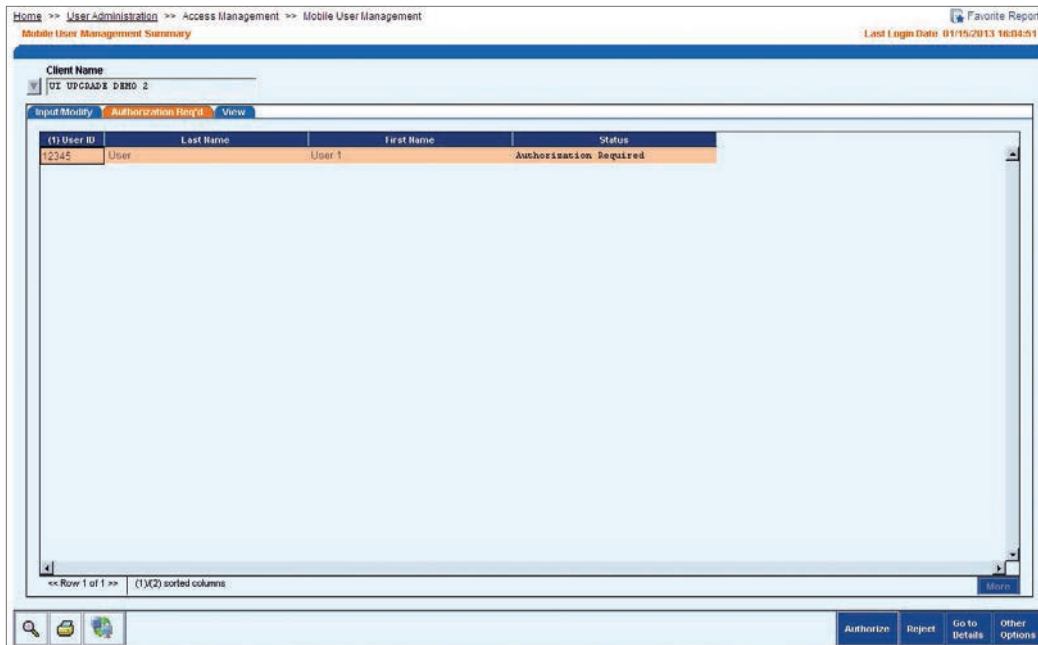
- Notification Enabled: Required for the user to receive Payment Authorization Notification via SMS and e-mail.
- Greater than, Less than, Daily SMS Limit:
 - We recommend that users limit the number of e-mail notifications by setting a monetary threshold to avoid receiving a notification for each payment pending authorization. Otherwise, users could receive many notifications a day, which could cause users to exceed their inbox limits. In order to set controls on the volume of e-mail notifications, Citi recommends that users set thresholds appropriate to their daily transaction activity. For Daily SMS Limit, Citi recommends that users set this to ten.
 - When setting thresholds, please note that the monetary range field is set in the local currency of the CitiDirect BE client definition that you are entitled on. When making nonlocal transactions, the monetary amount will be converted using the latest FX rate, and evaluated against your threshold criteria prior to sending a notification.

8. Existing Notification: Allow SMS for Event Notification: Check if the user wishes to receive SMS notification on existing notification. Daily SMS Limit: This is a user preference.

9. Security Manager clicks the submit button after entering the required details.

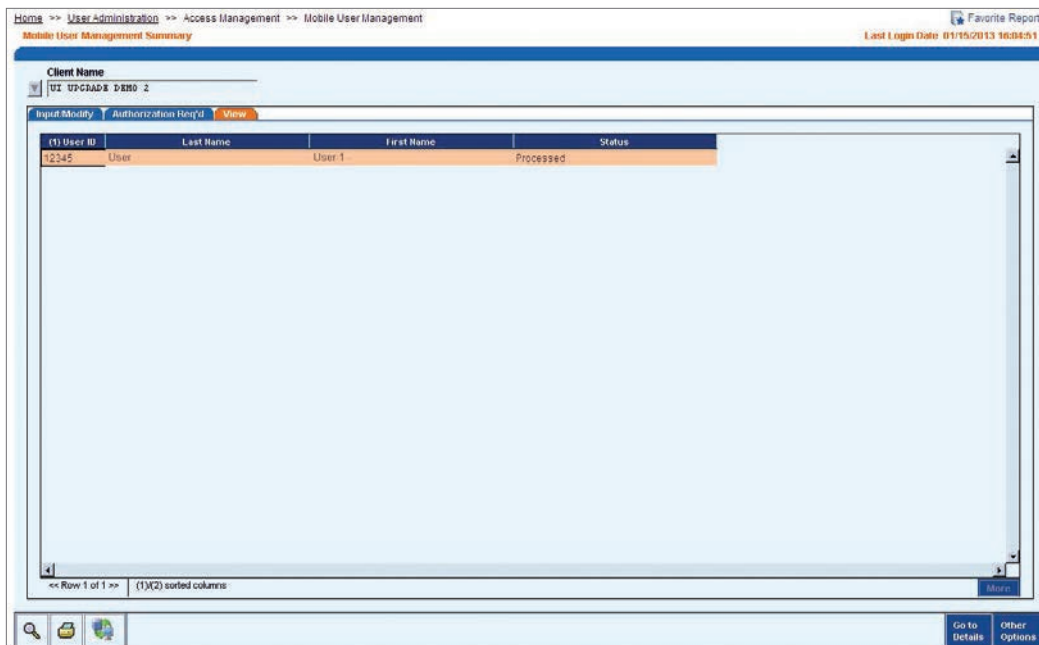
Note: If no notification option is selected, user will not receive a Welcome SMS or E-mail message.

Once the user has been created it must be authorized from the Mobile User Management section – Authorization Required screen.



Note the creator cannot authorize their own changes.

10. Security Manager clicks the Authorize button to complete the user setup.
11. Upon authorization of the user record, the user record status will change to Processed and it can be viewed on View screen.



Home >> User Administration >> Access Management >> Mobile User Management

Module: User Management Summary Last Login Date: 01/15/2013 16:04:51

Client Name: UI UPGRADE DEMO 2

(1) User ID	Last Name	First Name	Status
12345	User	User 1	Processed

<< Row 1 of 1 >> (1/1) sorted columns

Go to Details Other Options

Note: Only CD Security Administrators can set up new CDM users. All CDM users should have SafeWord cards. Users should have e-mail address set up in setup screen. CitiDirect BE Mobile will default to the language setting on your mobile device. If the language you are using is not supported the application will display in English.

Functional and Run-Time Users

Within the CitiDirect Online Banking platform, particularly in Automated File and Report Delivery (AFRD), entitled users have the ability to schedule reports and run automated file imports and exports. These scheduled events, often used across their enterprise, are associated with their specific CitiDirect User ID.

When any CitiDirect user makes an employment transition and their CitiDirect credentials are deleted or revoked, the scheduled events associated with that User ID become defunct and will no longer run.

As CitiDirect does not allow for the transference of scheduled events between users, the removal of the User ID requires the re-creation of all the event schedules. Creating a functional and/or run-time user will allow scheduled/automated events to run without disruption regardless of user status.

Functional User

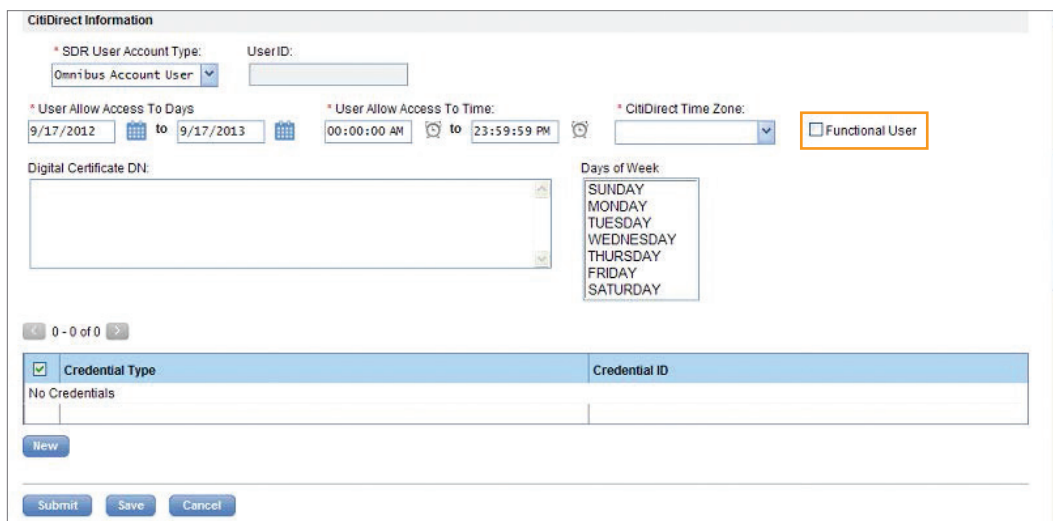
At the platform level, the Functional User feature allows for the creation of a virtual user so that schedules created in the File Delivery space will continue to run until it is determined that the schedule is no longer needed, rather than the schedule being discontinued due to the removal of the CitiDirect User ID associated with the scheduled events.

Characteristics of a functional user:

1. A functional user is a unique system-generated user.
2. A functional user is a virtual user or system server name, permanently signed on and active in the platform background. Once created on the platform, a functional user will never sign onto CitiDirect.
3. A functional user cannot sign onto CitiDirect and work in the platform.
4. A functional user cannot be switched to a credentialed user (e.g., use a SafeWord device to sign on).
5. An existing credentialed CitiDirect user cannot be switched to a functional user.
6. Citigroup must turn on the "Allow Functional Users" utility in the Client Configuration service class for the feature to become locally available to the Security Manager.
7. Local Security Managers can create or delete a functional user after Citi turns on the utility.
8. Functional users cannot be automatically deleted due to inactivity.

Create functional user profiles by following the steps below:

1. On the CitiDirect menu in portal, on Self Service, Create User will be there under Client Administration Service.
2. Click to open the Create User page.
3. Before you enter the user details, click the Functional User checkbox. This automatically changes the required form fields (see the details in the table below). The screenshot has illustrated the checkbox to be checked for a Functional User.



The screenshot shows the 'CitiDirect Information' form. The 'Functional User' checkbox is checked and highlighted with an orange box. The form includes fields for SDR User Account Type (set to 'Omnibus Account User'), UserID, User Allow Access To Days (9/17/2012 to 9/17/2013), User Allow Access To Time (00:00:00 AM to 23:59:59 PM), CitiDirect Time Zone, Digital Certificate DN, and Days of Week (SUNDAY through SATURDAY). A table below shows 'Credential Type' with a checked box and 'No Credentials' listed. At the bottom are 'Submit', 'Save', and 'Cancel' buttons.

Required Form Fields	Optional Form Fields	Disabled Fields
First Name	Middle Name	Initials
Last Name	Street Address	No Available E-mail Address checkbox is selected
Enabled checkbox is selected	Building/Floor/Room	E-mail
Time Zone	Zip/Postal Code	User Account Type defaults to Omnibus Account
Country	Telephone	

Fields auto-filled but editable	Fields auto-filled and not editable
Allow User Access to Days Start Date: default date is user profile creation date End Date: default date is five years in the future	Allow User Access To Time Start Time: 00:00:00 End Time: 23:59:59 Days of the Week All days are selected

4. Enter details as required.
5. Click the Submit button to save the profile and enter it into the authorization queue. A Warning message will appear for functional user creation.

Note: The functional user profile is submitted without indicating credentials. Once the user profile is authorized, the Credentials grid will display a Credential Type and a Credential ID, and the Credentials grid will remain inactive.

Run-Time User

Within Automated File and Report Delivery (AFRD), the run-time user is a flexible user feature that allows for a virtual user to be created and assigned to event schedules within AFRD, rather than the schedule being discontinued due to the removal of the CitiDirect User ID associated with the schedule.

Characteristics of a run-time user:

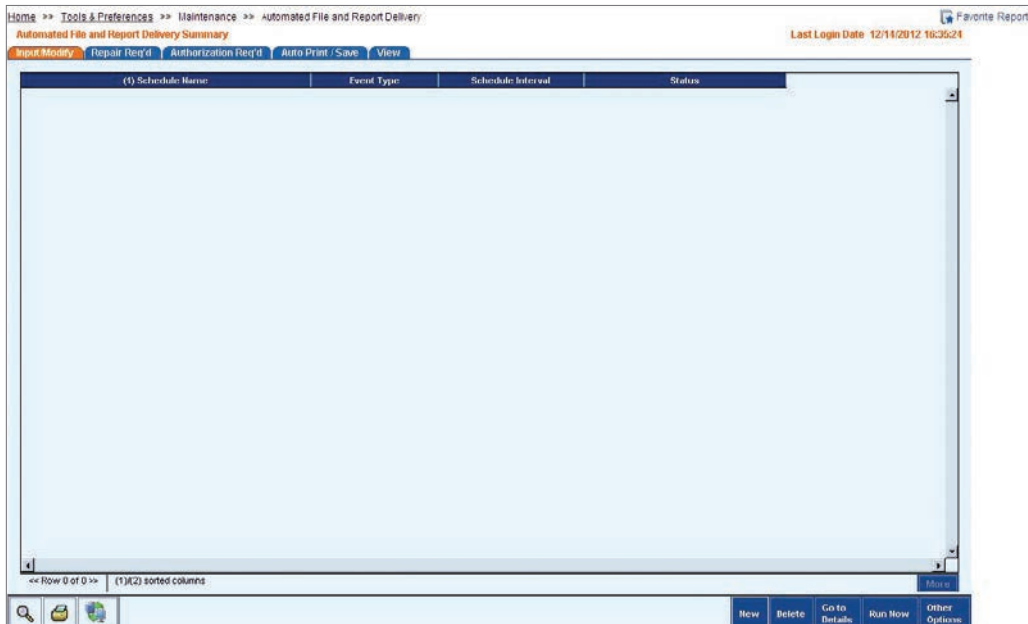
1. A run-time user must first be created as a functional user (this is a system security requirement).
2. A run-time user is a functional user under whose name the AFRD schedules are run.

Create a Run-Time user by following the steps below:

1. On the CitiDirect menu under Tools & Preferences, click Automated File and Report Delivery.



2. The Automated File and Report Delivery Summary form appears.



3. Click the New button. The Automated File and Report Delivery Details form appears.
4. Complete the form details to fit your scheduled event need.
5. Click the Run-Time User library lookup button. Select the functional user name from the library list. If there is a single functional user, the field will auto-fill with that name.

Notes:

The functional user profile must be authorized before it will appear in the Run-Time User library.

If the name does not immediately appear in the library list, use the search feature under Other Options to find the functional user name.

6. Click the Submit button.

CitiDirect® Online Banking Reports and Inquiries

Organizations have a greater need than ever before for reliable information and systematic internal controls. With CitiDirect BE you have access to a documented set of internal controls that provide web-based access to accurate, up-to-the-minute audit-trail information. On CitiDirect, you can follow transactions from beginning to end.

With authorization levels, flow controls and other security features you can establish a clear separation of duties to assist you in complying with legal and regulatory requirements. Information through the CitiDirect Inquiry and Reporting capabilities allows you to perform CitiDirect and user audits, and is critical to your role as Security Manager.

The CitiDirect Report functionality enables you to:

Select from a variety of standard reports that you can customize from available criteria and view real-time information.

1. Define report criteria to retrieve the information you need.
2. Save your customized reports to run as often as needed.
3. View your reports in a separate browser window in a format you specify.
4. Print report output and save the output file on your system.
5. Automate your reporting through the Automated File and Report Delivery feature.
 - a. Deliver reports to your browser – the View Reports tab.
 - b. Deliver reports to a secure server location via a secure HTTP/s Internet connection.
 - c. Deliver reports to an e-mail address via encrypted e-mail.
 - d. Deliver or retrieve your reports via an FTP connection. The CitiDirect Inquiry functionality enables you to:
6. Get immediate access to information for a specific point in time.
7. View information displayed on your screen, while you are signed onto CitiDirect Online Banking.

Note: Inquiries do not allow you to save criteria; once an inquiry is closed, the information is no longer available.

Security Manager Reports

The CitiDirect Online Banking reporting functionality provides real-time information to support your decision-making processes. When a report is run, you can print the report for a formal document or save the output in various formats (such as .xls or .pdf), on which you can then use the search feature to manipulate the data you need. In addition, you can elect to send your report to a secure server location using an HTTPS Internet connection or to an e-mail address using encrypted e-mail.

Note: For detailed instructions on selecting report criteria and running reports refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com in the CitiDirect Basics section's Basics Guides tab.

The following table lists the reports available in CitiDirect for Security Managers. The name of each report and its description are included.

Report Name	Description
Audit Reports	
Audit Log Summary Report	The Audit Log Summary Report enables you to track CitiDirect activity and usage. You can specify times and dates, users or auditable events. Audit Reports allow you to understand who is accessing CitiDirect and for what activities in order to minimize security risks. They can be run as a base report to display all auditable activities for the current or specific dates. You can tailor audit reports to show history on specific actions that can help you to monitor changes to key Security Manager actions.
Audit Log Detail Report	The Audit Log Detail Report lists the details of all activity on CitiDirect for a specific date range. If you do not apply filters to the date range, the report contains details on any activity for the current date.

Report Name	Description
Access Management Reports	
Account Management Summary Report	The Account Management Summary Report is a run-time report that provides a snapshot of account links Citibank is making on your behalf, which is assigning or deleting your organization's accounts to various services in CitiDirect. This report does not provide historical details of the account, but provides the most recent action taken against your accounts. This report is helpful when you are adding account entitlements to an Access Profile, and when you are troubleshooting account issues.
Access Profile Detail Report	The Access Profile Detail Report displays a comprehensive view of your entitlements definitions and lists all Access Profile Names, Statuses and Details.
Logon Activity Report	The Logon Activity Report provides a monitoring tool for logon activity into CitiDirect anytime a valid user credential is used. All logon attempts are captured at the web server and logged. This report gives Security Managers a view into logon activity relevant to their CitiDirect users.
User Profile and Entitlements Report	The User Profile and Entitlements Report is a powerful report that enables you to access both user profiles and entitlements information in one report. Use this report in conjunction with the Access Profile Detail Report for a complete view of user setup and entitlements.

Audit Reports

Audit reports enable you to track activity and usage of CitiDirect Online Banking. You can specify times and dates, users or auditable events. Audit reports allow you to understand who is accessing CitiDirect, for what activities and when.

Audit Log Summary Report

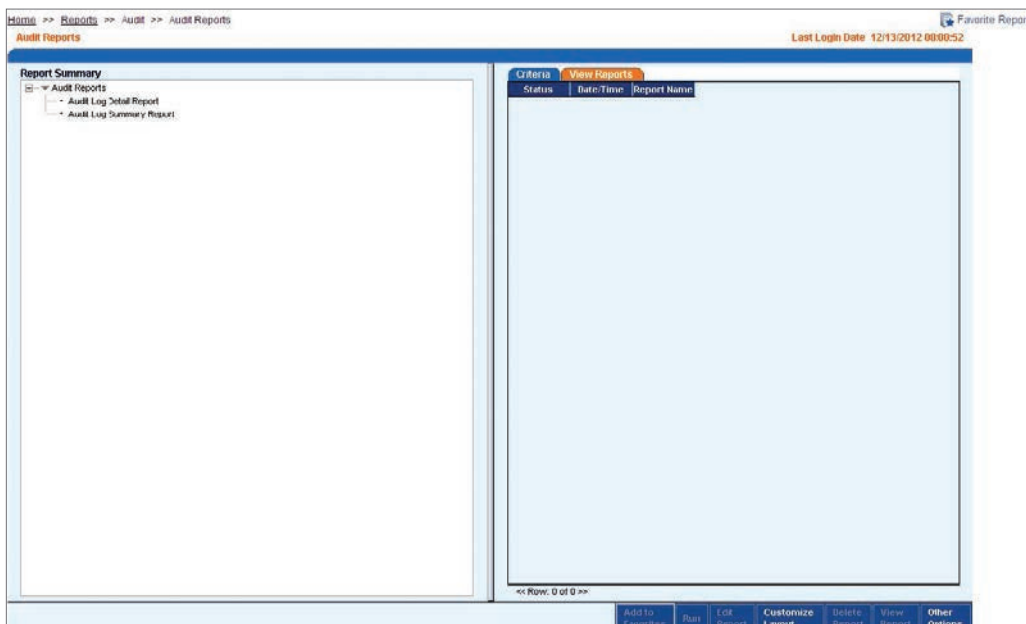
The Audit Log Summary Report lists a summary of all activity in CitiDirect Online Banking for a specific date or date range. If you do not apply filters to the date range, the report provides a summary of activity for the current date.

Run the Audit Log Summary Report by following the steps below:

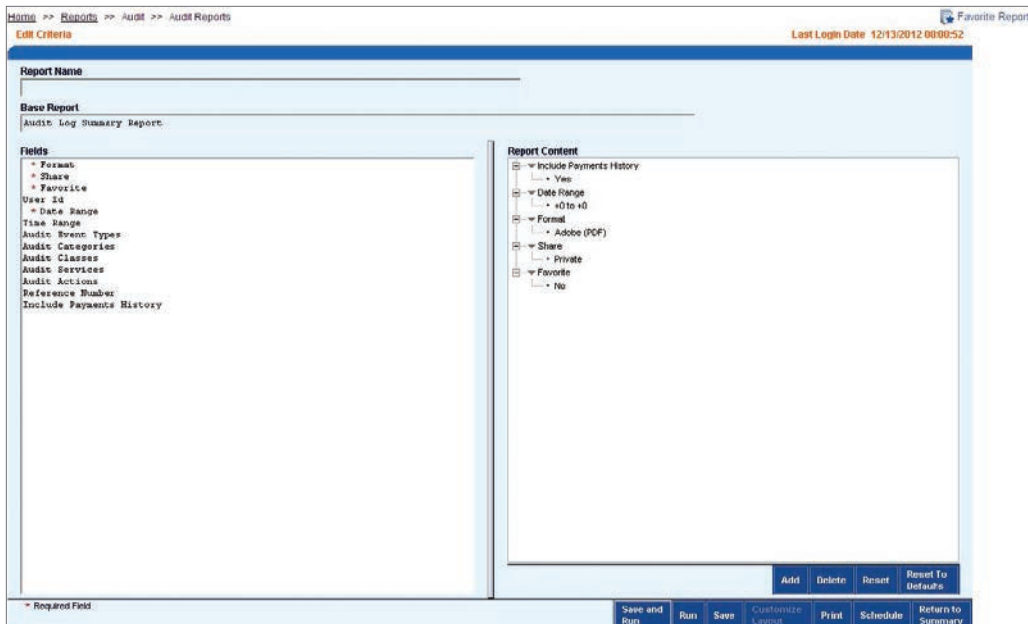
1. On the CitiDirect menu under Reports, click Audit Reports as shown below.



2. The Audit Reports form appears.



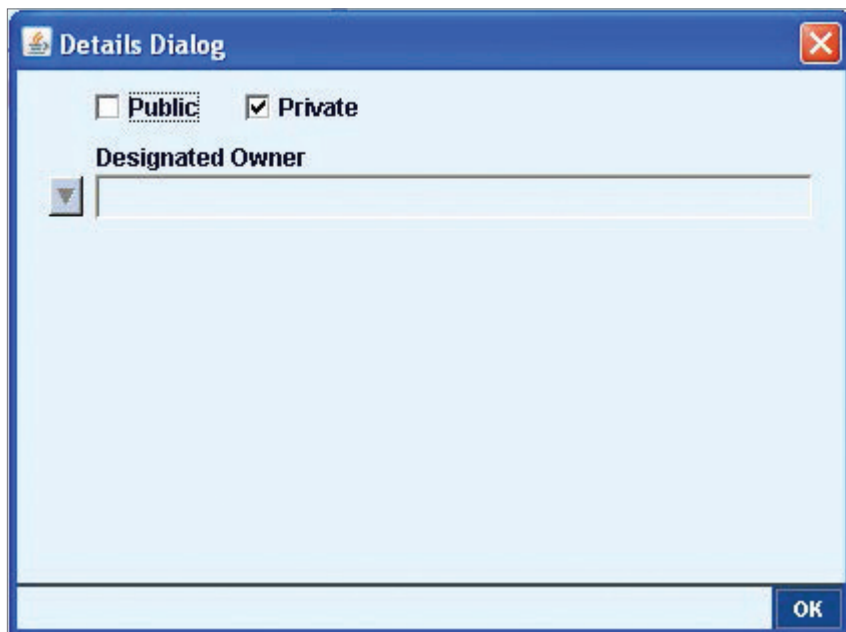
3. In the Report Summary list box on the left, select the Audit Log Summary Report, and then click the Edit Report button. The Edit Criteria form appears.



4. Define the content of your report by selecting criteria elements from the Fields list box, as described below.
 - Select the Format criterion to change the format of your report. If you do not specify a format, the report is displayed in PDF (Acrobat Reader 9.0 required), the CitiDirect-defined default format for reports. The other available report formats are Comma Separated Values (CSV), Microsoft Excel (XLS) and DHTML

Note: The DHTML output format is only available for CitiDirect reports that contain drilldown links.

- Select the Share criterion to allow other users at your organization to run or view this report. A dialogue box appears.



The CitiDirect-defined default is Private and the Designated Owner field displays the name of the signed-on user (typically your name).

To make the report public, select the Public checkbox. If you want to make another user the owner of the report, select that user's name from the Designated Owner field.

Notes:

Only the designated owner can modify or delete the report.

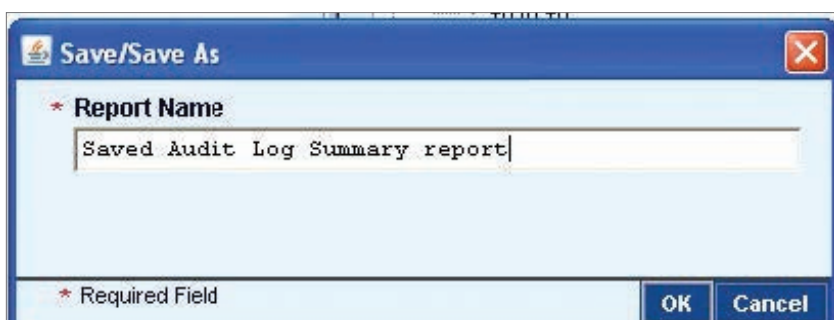
Once changes are saved, you will lose ownership rights to the report if you have designated someone else the owner. Only the newly designated owner may entitle you to resume ownership of the report.

- Select the Favorite criterion to add the report to your Favorite Report list in the Report Assistant. After the report is saved, you can press ALT+R on your keyboard to navigate directly to the Report Assistant from anywhere in CitiDirect. For more information on using the Report Assistant, refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com.
- Select the User ID criterion to select the unique CitiDirect number associated with an individual's first and last name. If you do not select a User ID, your report will include the activities of all users.
- Select the Date Range criterion to enter the time period you want the report to cover. The date range must fall within the last nine months. This is a required field.
- Select the Audit Actions criterion to select the auditable actions taken to complete an event. If no information is selected, the Citibank-defined value is All.
- Select the Reference Number criterion to enter a reference number to limit the report data. If nothing is entered, the Citibank-defined value is blank.

Note: Citi recommends keeping the default value of All for the following criteria: Audit Event Types, Audit Categories, Audit Classes, and Audit Services. Modifying these criteria can restrict your results and limit the usefulness of this report.

5. After you have selected your report criteria, proceed with one of the following steps:

- Click the Run button to run the report.
The report is run and its name appears on the Report Summary list and on the View Reports tab with the notation Unsaved before the report name. The status of the report changes from Waiting to Running to Available.
When the status is available, click the View Report button. The report appears in a separate browser window.
- Click the Save button to save the current report. The Save/Save As dialogue box appears. Enter a Report Name and click the OK button. The new report name is added to the Report Summary list.



- Click the Save and Run button to save and immediately run the report.
The Save/Save As dialogue box appears. After you enter a Report Name and click the OK button, as described above, the report is run.
The report name is added to the Report Summary list and the View Reports tab. After a brief period, its status changes from Waiting to Running to Available. When the status is Available, you can view the report. Click the Print button to print the report criteria.

Note: The criteria listed in the Report Content list box is printed, not the actual report.

- Click the Schedule button to schedule the report to run at specific times.
This allows you access to Automated File and Report Delivery (AFRD). For more information on AFRD, refer to the Automated File/Report Delivery guides in the Learning Center at www.citidirect.com.
- Click the Return to Summary button to return to the Audit Reports form.
If you have selected criteria, you will be prompted to save the report.

Note: If you are editing a report that you have created and saved, the report name appears in the Report Name field in the Save/Save As dialogue box. If you do not want to overwrite the original report, enter a new name for this report.

Sample Audit Log Summary Report

Report content varies based on the criteria you have selected.

citi		CitiDirect® Online Banking						
Audit Log Summary Report								
Sequence Number	Date	Time	User	Service Category	Service Class	Service	Action	Event
Client Name UI UPGRADE DEMO 2								
1	2012/2012	14:52:49		Maintenance	Libraries	Preformat_Group_Library_Detail	Create	Audit
Reference	PAYMENTS				Initiated By	Customer Support		
2	2012/2012	14:53:34		Activation	Pref_Maint	Pref_Maint_Library_Detail	Submit	Audit
Reference	DEFAULT				Initiated By	Customer Support		
3	2012/2012	14:54:06		Activation	Pref_Maint	Pref_Maint_Library_Detail	Submit	Audit
Reference	PAYMENTS				Initiated By	Customer Support		
4	2012/2012	14:54:38		Access_Mgmt	Pref_Maint	Pref_Maint_Library_Detail	Submit	Audit
Reference	PAYMENTS				Initiated By	Customer Support		
5	2012/2012	14:55:20		Activation	Account_Management	Summary	Create	Audit
Reference	BC87BC1B92C511E				Initiated By	Customer Support		
6	2012/2012	14:55:35		Activation	Account_Management	Summary	Create	Audit
Reference	B67DFE12920111D				Initiated By	Customer Support		
7	2012/2012	14:56:38		Activation	Pref_Maint	Pref_Maint_Library_Detail	Submit	Audit
Reference	DEFAULT				Initiated By	Customer Support		
8	2012/2012	14:59:21		Access_Mgmt	Entitlement	Access_Profile_Maint_Detail	Submit	Audit
Reference	SYSTEM ADMINIS				Initiated By	Customer Support		
9	2012/2012	14:59:36		Access_Mgmt	Entitlement	Access_Profile_Maint_Summary	Delete	Audit
Reference	FILE IMPORT NO F				Initiated By	Customer Support		
10	2012/2012	14:59:36		Access_Mgmt	Entitlement	Access_Profile_Maint_Summary	Delete	Audit
Reference	FILE IMPORT TES1				Initiated By	Customer Support		
11	2012/2012	15:01:06		Access_Mgmt	Entitlement	Access_Profile_Maint_Detail	Submit	Audit
Reference	FILE EXPORT DAP				Initiated By	Customer Support		
Report Date 01/15/2013 17:54:41 (EST)				Unsaved Audit Log Summary Report				1 of 108

Below is a listing of the information contained in this report:

1. Action
2. Service Category
3. Date
4. Service Class
5. Event
6. Time
7. Service
8. User

Notes:

Click the Date hyperlink to view details of an item. The Audit Log Detail report appears. All available details for the selected items are displayed.

If you do not view your report after it becomes available, an Audit Report Outputs Available message is sent to your Inbox and is available for viewing for 24 hours.

Audit Log Detail Report

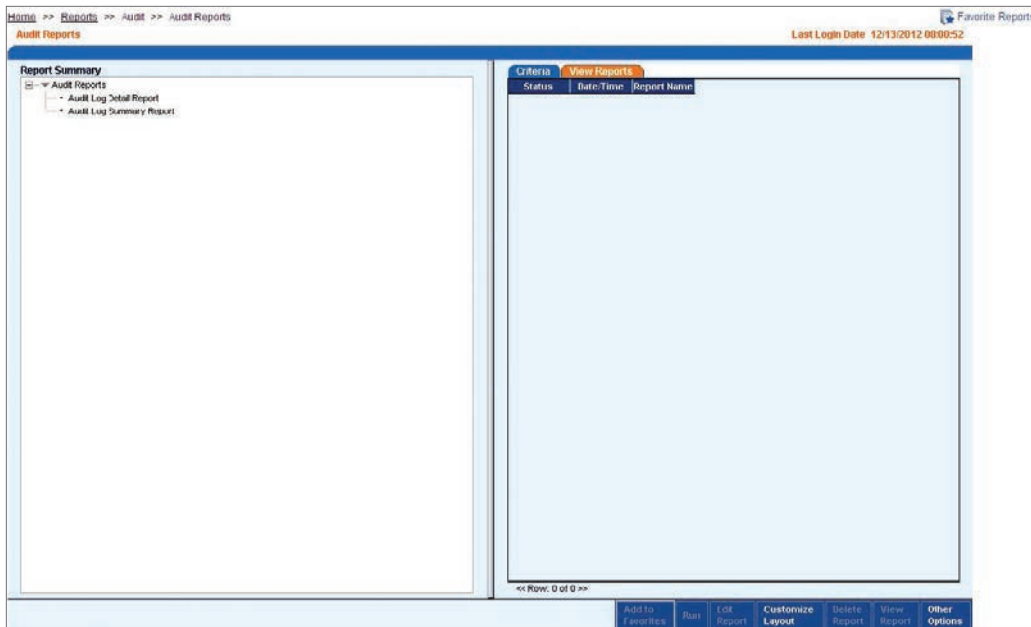
The Audit Log Detail Report lists the details of all activity in CitiDirect for a specific date range. If you do not apply filters to the date range, the report contains details of any activity for the current date.

Run the Audit Log Detail Report by following the steps below.

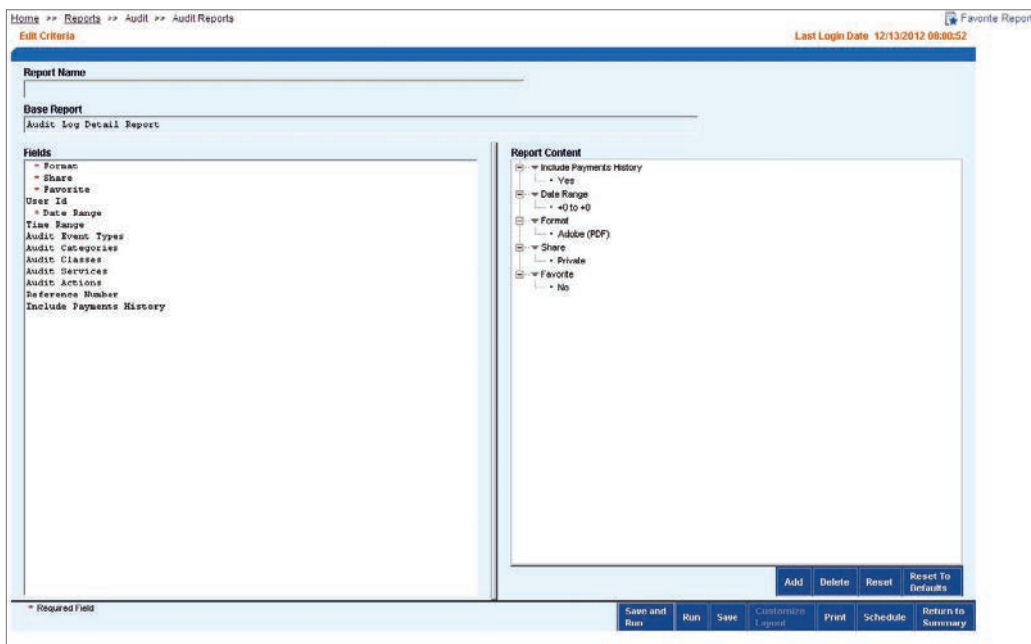
1. On the CitiDirect menu under Reports, click Audit Reports.



2. The Audit Reports form appears.



3. In the Report Summary list box on the left, select the Audit Log Detail Report, and then click the Edit Report button. The Edit Criteria form appears.



4. Define the content of your report by selecting criteria elements from the Fields list box, as described below.
 - Select the Format criterion to change the format of your report. If you do not specify a format, the report is displayed in PDF (Acrobat Reader 9.0 required), the CitiDirect-defined default format for reports. The other available report formats are Comma Separated Values (CSV), Microsoft Excel (XLS) and DHTML.

Note: The DHTML output format is only available for CitiDirect reports that contain drilldown links.

- Select the Share criterion to allow other users at your organization to run or view this report. The Details dialogue box appears:



The CitiDirect-defined designation is Private and the Designated Owner field displays the name of the signed-on user (typically your name).

To make the report public, select the Public checkbox. If you want to make another user the owner of the report, select that user's name from the Designated Owner field.

Notes:

Only the designated owner can modify or delete the report.

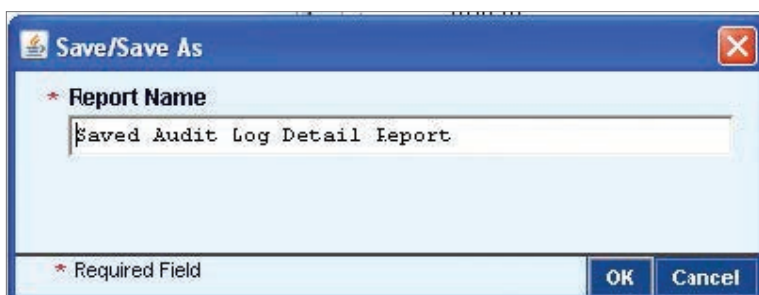
Once changes are saved, you will lose ownership rights to the report if you have designated someone else the owner. Only the newly designated owner may entitle you to resume ownership of the report.

- Select the Favorite criterion to add the report to your Favorite Report list in the Report Assistant. After the report is saved, you can press ALT+R on your keyboard to navigate directly to the Report Assistant from anywhere in CitiDirect. For more information on using the Report Assistant, refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com.
- Select the User ID criterion to select the unique Citibank number associated with an individual's first and last name.
If you do not select a User ID, your report will include the activities of all users.
- Select the Date Range criterion to enter the time period you want the report to cover. The date range must fall within the last nine months. This is a required field.

- Select the Audit Actions criterion to select the auditable actions taken to complete an event. If no information is selected, the CitiDirect-defined value is All.
- Select the Reference Number criterion to enter a reference number to limit the report data. If nothing is entered, the Citibank-defined value is blank.

Note: Citibank recommends keeping the default value of All for the following criteria: Audit Event Types, Audit Categories, Audit Classes and Audit Services. Modifying these criteria can restrict your results and limit the usefulness of this report.

5. After you have selected your report criteria, proceed with one of the following steps:
 - Click the Run button to run the report.
The report is run and its name appears on the Report Summary list and on the View Reports tab with the notation Unsaved before the report name. The status of the report changes from Waiting to Running to Available.
When the status is Available, click the View Report button. The report appears in a separate browser window.
 - Click the Save button to save the current report. The Save/Save As dialogue box appears.




Enter a Report Name and click the OK button. The new report name is added to the Report Summary list.

- Click the Save and Run button to save and immediately run the report.
The Save/Save As dialogue box appears. After you enter a Report Name and click the OK button, as described above, the report is run.
The report name is added to the Report Summary list and the View Reports tab. After a brief period, its status changes from Waiting to Running to Available. When the status is Available, you can view the report.
- Click the Print button to print the report criteria.
- Click the Schedule button to schedule the report to run at specific times.
This allows you access to Automated File and Report Delivery (AFRD). For more information on AFRD, refer to the Automated File/Report Delivery guides in the Learning Center at www.citidirect.com.
- Click the Return to Summary button to return to the Audit Reports form.
If you have selected criteria, you will be prompted to save the report.

Sample Audit Log Detail Report

Report content varies based on the criteria you have selected.

Sequence Number	Date	Time	User	Service Category	Service Class	Service	Action	Event	
 CITIDirect® Online Banking									
Audit Log Detail Report									
Client Name	UI UPGRADE DEMO 2								
1	01/19/2013	16:55:52		Infrastructure	Application_Framework	Client_Profile	Successful_Log on	Audit	
Reference	User logged on: 1: Portal Application = Portal Integrated CITIDirect								
Details	User logged on: User id: Login id: Language id: en_US OS: Windows XP 6.1 Service Pack 3 32 bit Browser: Internet Explorer 7.0 JRE: Portal Application: Portal Integrated CITIDirect								
2	01/19/2013	16:58:04		Infrastructure	Services	Report	Save_New_Crit ica	Non_Financial	
Reference	AuditLogDetail								
Details	Report Service Class: Audit Reports Report Name: Unsaved Audit Log Detail Report User Criteria: Share: N Digitl Signature: N Include Payments History: Y - Yes Compress with WinZip: N Date Range: +0 To +0 Format: Adobe (PDF)								
3	01/19/2013	16:58:08		Infrastructure	Services	Report	Run_Now	Non_Financial	
Reference	AUDITARP-AuditLogDetail								
Details	Report Service Class: Audit Reports Report Name: Unsaved Audit Log Detail Report InstanceID: 193223556 Criteria: Share: N Digitl Signature: N Include Payments History: Y - Yes Compress with WinZip: N Date Range: +0 To +0 Format: Adobe (PDF)								
Total Records in the Report				3					
Report Date 01/19/2013 16:08:08 (EST)				Unsaved Audit Log Detail Report				1 of 2	

Below is a listing of the information contained in this report:

1. Action
2. Service
3. Application Server
4. Service Category
5. Date
6. Service Class
7. Details
8. Time
9. Event
10. User
11. Reference

Notes:

If you do not view your report after it becomes available, an Audit Reports Outputs Available message is sent to your Inbox and is available for viewing for 24 hours.

Where applicable, reasons are also provided for login failures. The following are examples of reasons for login failures: user's access has expired, user not currently enabled to use the system, user not authorized to use the system on this day of the week, and user not authorized to use the system at this time of day.

Access Management Reports

The Access Management Reports service class contains the following reports, which are specifically designed to provide the information you need to fulfill your responsibilities as a Security Manager:

1. Account Management Summary Report.
2. Access Profile Detail Report.
3. Logon Activity Report.
4. User Profile and Entitlement Report.

A description of each report and procedures for specifying report content, running, saving and printing are presented in this section.

Account Management Summary Report

The Account Management Summary Report is a run-time report that provides a snapshot of any actions Citibank is taking on your behalf, that is, linking your organization's accounts to CitiDirect services, deleting account links, etc. It does not provide historical details of accounts, but it does provide the most recent action taken against your accounts.

Note: Accounts that are closed for more than 20 months will be automatically un-entitled and be deleted by the system.

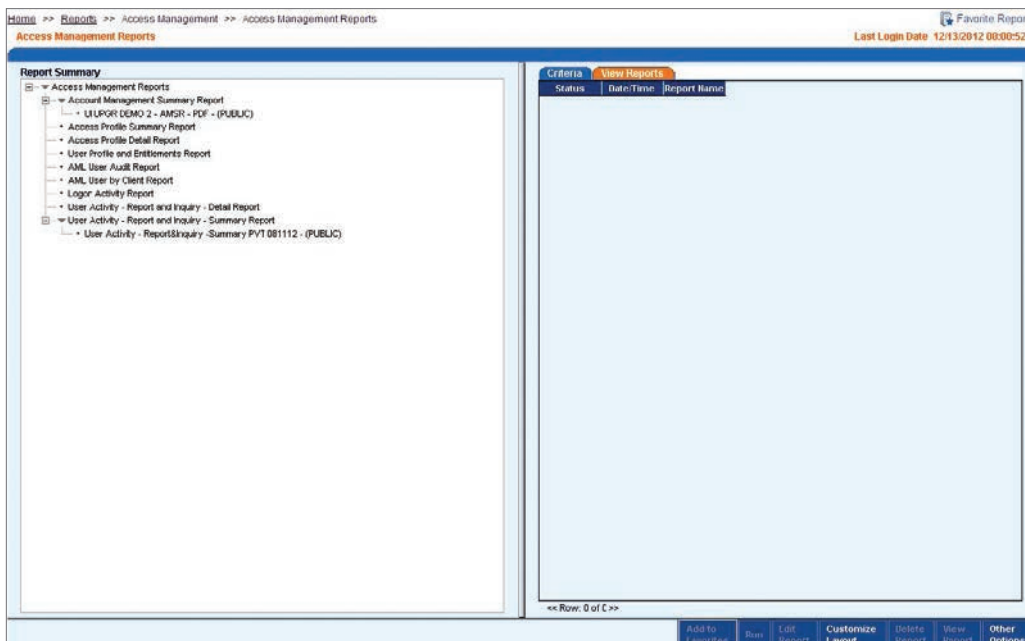
This report is helpful when you have requested an account to be linked and you are checking its availability to be used, when you are adding account entitlements to an access profile and when you are performing CitiDirect maintenance.

Run the Account Management Summary Report by following the steps below:

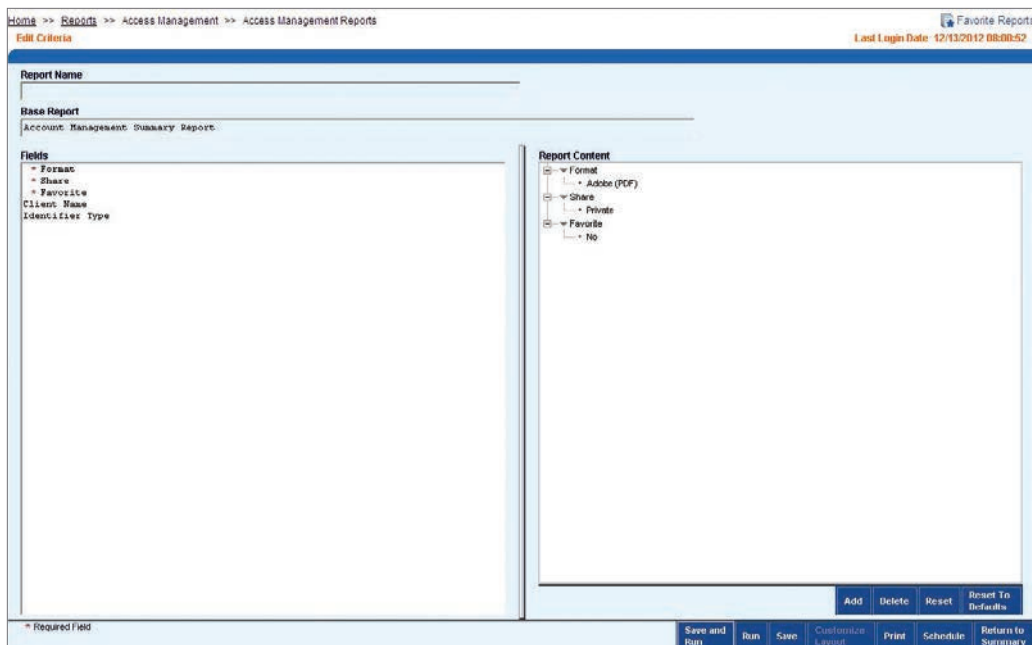
1. On the CitiDirect menu under Reports, click the Access Management Reports as shown below.



2. The Access Management Reports form appears.

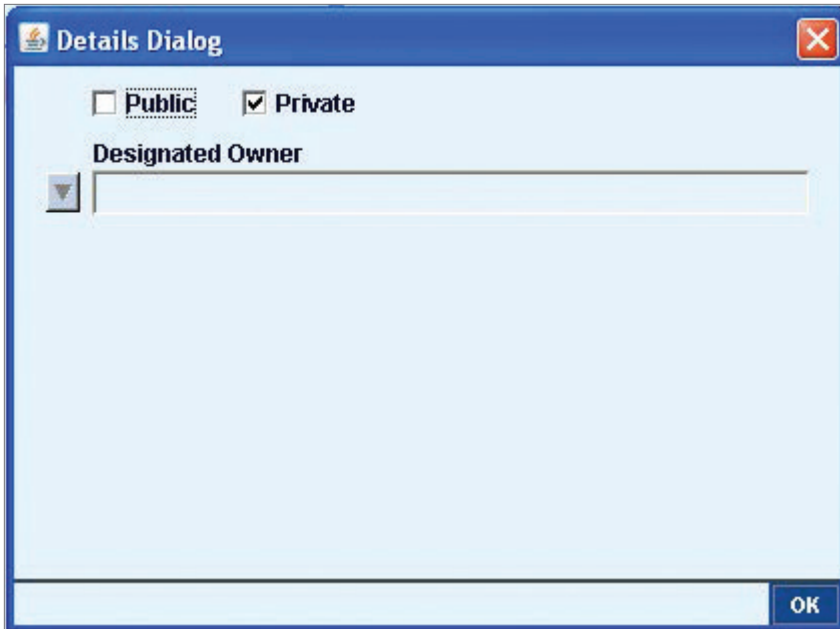


3. In the Report Summary list box on the left, select the Account Management Summary Report, and then click the Edit Report button. The Edit Criteria form appears.



4. Define the content of your report by selecting criteria elements from the Fields list box, as described below: Select the Format criterion to change the format of your report.
 - If you do not specify a format, the report is displayed in PDF (Acrobat Reader 9.0 required), the CitiDirect-defined default format for reports. The other available report formats are Comma Separated Values (CSV), Microsoft Excel (XLS) and DHTML

Note: The DHTML output format is only available for CitiDirect reports that contain drilldown links. Select the Share criterion to allow other users at your organization to run or view this report. The Details dialogue box appears:



The CitiDirect-defined designation is Private and the Designated Owner field displays the name of the signed-on user (typically your name).

To make the report public, select the Public checkbox. If you want to make another user the owner of the report, select that user's name from the Designated Owner field.

Notes:

Only the designated owner can modify or delete the report.

Once changes are saved, you will lose ownership rights to the report if you have designated someone else the owner. Only the newly designated owner may entitle you to resume ownership of the report.

- Select the Favorite criterion to add the report to your Favorite Report list in the Report Assistant.
 - After the report is saved, you can press ALT+R on your keyboard to navigate directly to the Report Assistant from anywhere in CitiDirect. For more information on using the Report Assistant, refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com.
 - Select the Identifier Type criterion to identify the type of account.
Options are Account, Account via Base Number, Base Number, GFCID, Smart Account Group, and WorldLink ID.
5. After you have selected your report criteria, proceed with one of the following steps: Click the Run button to run the report.

The report is run and its name appears on the Report Summary list and on the View Reports tab with the notation Unsaved before the report name. The status of the report changes from Waiting to Running to Available.

When the status is Available, click the View Report button. The report appears in a separate browser window.

- Click the Save button to save the current report. The Save/Save As dialogue box appears.



Enter a Report Name and click the OK button. The new report name is added to the Report Summary list.

- Click the Save and Run button to save and immediately run the report. The Save/Save As dialogue box appears. After you enter a Report Name and click the OK button, as described above, the report is run. The report name is added to the Report Summary list and the View Reports tab. After a brief period, its status changes from Waiting to Running to Available. When the status is Available, you can view the report.
- Click the Print button to print the report criteria. The criteria listed in the Report Content list box is printed, not the actual report.
- Click the Schedule button to schedule the report to run at specific times. This allows you access to Automated File and Report Delivery (AFRD). For more information on AFRD, refer to the Automated File/Report Delivery guides in the Learning Center at www.citidirect.com.
- Click the Return to Summary button to return to the Access Management Reports. If you have selected criteria, you will be prompted to save the report.

Sample Account Management Summary Report

Report content varies based on the criteria you have selected.

citi		CitiDirect® Online Banking					
Account Management Summary Report							
Client Name		UI UPGRADE DEMO 2					
Additions							
Identifier Type	Number	Name	Country of Domicile	Currency	Date Available	Time Available	Associated With
Account			US	USD	06/27/2012	15:05:14	Cash PI
Account			US	USD	06/27/2012	15:05:14	Payments
Account			US	USD	06/27/2012	15:05:14	Cash PI
Account			US	USD	06/27/2012	15:05:14	Payments

This report is able to show linked account data dating back 18 months. Data before this date are unavailable for viewing.

Below is a listing of the information contained in this report:

1. Account Name
2. Currency
3. Account Number
4. Date Available
5. Associated With (what Identifier Type management structure the account is associated with. For example, Payments or Liquidity PI)
6. Country of Domicile

Access Profile Detail Report

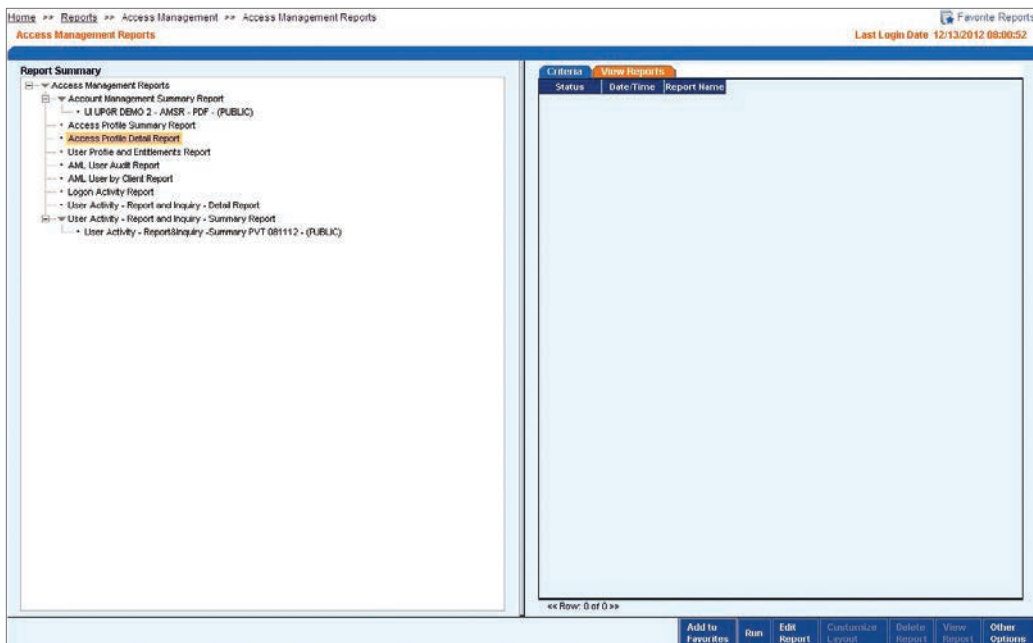
The Access Profile Detail Report is a fast, efficient way to review all access profile information. This is an excellent tool for flow control and user access maintenance. For example, if you have modified a flow, you can use this report to ensure you have access profiles that will enable the process to be performed, as defined by the new flow.

Run the Access Profile Detail Report by following the steps below:

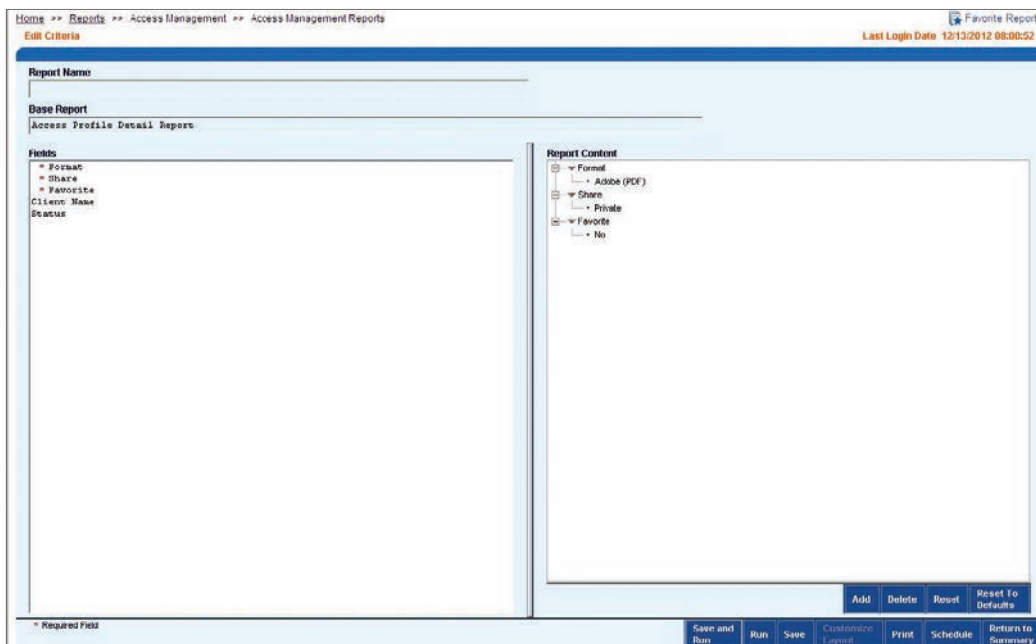
1. On the CitiDirect menu under Reports, click the Access Management Reports.



2. The Access Management Reports form appears.



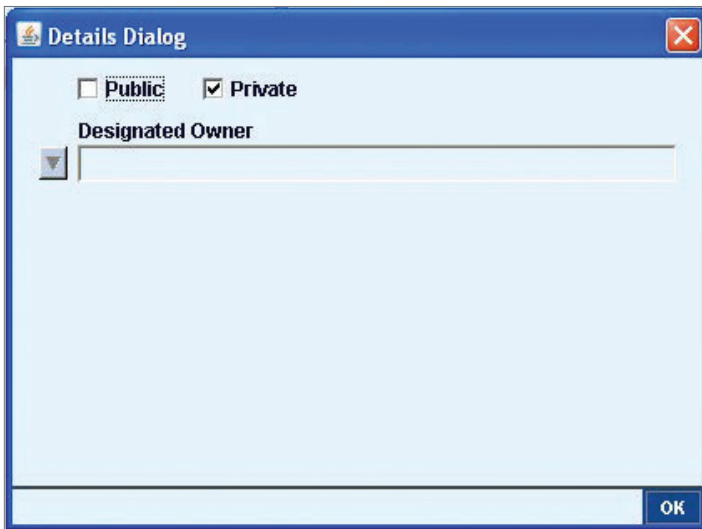
- In the Report Summary list box on the left, select the Access Profile Detail Report, and then click the Edit Report button. The Edit Criteria form appears.



4. Define the content of your report by selecting criteria elements from the Fields list box, as described below. Select the Format criterion to change the format of your report.
 - If you do not specify a format, the report is displayed in PDF (Acrobat Reader 9.0 required), the CitiDirect-defined default format for reports. The other available report formats are Comma Separated Values (CSV), Microsoft Excel (XLS), and DHTML

Note: The DHTML output format is only available for CitiDirect reports that contain drilldown links.

- Select the Share criterion to allow other users at your organization to run or view this report. The Details dialogue box appears:



The CitiDirect-defined designation is Private and the Designated Owner field displays the name of the signed-on user (typically your name).

To make the report public, select the Public checkbox. If you want to make another user the owner of the report, select that user's name from the Designated Owner field.

Notes:

Only the designated owner can modify or delete the report.

Once changes are saved, you will lose ownership rights to the report if you have designated someone else the owner. Only the newly designated owner may entitle you to resume ownership of the report.

- Select the Favorite criterion to add the report to your Favorite Report list in the Report Assistant. After the report is saved, you can press ALT+R on your keyboard to navigate directly to the Report Assistant from anywhere in CitiDirect. For more information on using the Report Assistant, refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com.
- Select the Status criterion to select the status of the access profile, which can be either Authorization Required or Processed.

5. After you have selected your report criteria, proceed with one of the following steps:
 - Click the Run button to run the report. The report is run and its name appears on the Report Summary list and on the View Reports tab with the notation Unsaved before the report name. The status of the report changes from Waiting to Running to Available.

When the status is Available, click the View Report button. The report appears in a separate browser window.

- Click the Save button to save the current report. The Save/Save As dialogue box appears.



Enter a Report Name and click the OK button. The new report name is added to the Report Summary list.

- Click the Save and Run button to save and immediately run the report.
- The Save/Save As dialogue box appears. After you enter a Report Name and click the OK button, as described above, the report is run. The report name is added to the Report Summary list and the View Reports tab. After a brief period, its status changes from Waiting to Running to Available. When the status is Available, you can view the report.
- Click the Print button to print the report criteria. The criteria listed in the Report Content list box is printed, not the actual report.
- Click the Schedule button to schedule the report to run at specific times. This allows you access to Automated File and Report Delivery (AFRD). For more information on AFRD, refer to the Automated File/Report Delivery guides in the Learning Center at www.citidirect.com.
- Click the Return to Summary button to return to the Access Management Reports form. If you have selected criteria, you will be prompted to save the report.

Note: If you are editing a report that you have created and saved, the report name appears in the Report Name field in the Save/Save As dialogue box. If you do not want to overwrite the original report, enter a new name for this report.

Sample Access Profile Detail Report

Report content varies based on the criteria you have selected. This report provides you with:

- A list of your access profiles.
- The detailed criteria within each access profile.

Citi		CitiDirect® Online Banking
Access Profile Detail Report		
Client Name	UI UPGRADE DEMO 2	
Access Profile Name	SYSTEM ADMINISTRATOR	
Status	Processed	
Access Profile Detail	<ul style="list-style-type: none"> Access Management Reports Access Profile Audit Reports Client Preferences Flow Maintenance Inactive User Inquiry User Entitlements User Profile 	
Access Profile Name	FILE EXPORT DAP	
Status	Processed	
Access Profile Detail	<ul style="list-style-type: none"> Export Custom Format Definition Export Data - Straight Through Reconciliation - No Export Profile Libraries - Library Name - File Export BAI, ISO and SWIFT Code Library - Processes - MODIFY - VIEW - DELETE - IMPORT - INPUT - LEVEL 1 AUTHORIZATION 	
Access Profile Name	FILE IMPORT DAP	
Status	Processed	
Access Profile Detail	<ul style="list-style-type: none"> Import File Inquiry Import Profile Import Transactions Libraries - Library Name - File Import Map Definition Rule Set - Processes - DELETE - IMPORT - INPUT - LEVEL 1 AUTHORIZATION - MODIFY - VIEW 	
Access Profile Name	MOBILE USER MANAGEMENT	
Status	Processed	
Access Profile Detail	<ul style="list-style-type: none"> Mobile User Management User Profile 	
Report Date 01/15/2013 18:11:19 (EST)	Unsaved Access Profile Detail Report	1 of 5

Logon Activity Report

The Logon Activity Report provides Security Managers with a monitoring tool for user logon activity. All logon attempts are captured at the web server and logged. This report gives you a view into this activity relevant to your CitiDirect users.

Data will be captured for up to 50 sessions per day per user credential, for the past nine months. No more than 25 attempts can be counted per user per session. A "*" appears if the count is 26 or more.

Run the Logon Activity Report by following the steps below.

1. On the CitiDirect menu under Reports, click Access Management Reports as shown below.

Reports

Tools & Preference

Payment Reports

- [Cash Balances Reports](#)
- [Cash Statements Reports](#)
- [Cash Transaction Initiation Reports](#)
- [Bank Statements - US Reports](#)

Tools

- [Automated File and Report Delivery Reports](#)
- [Report Customizer](#)

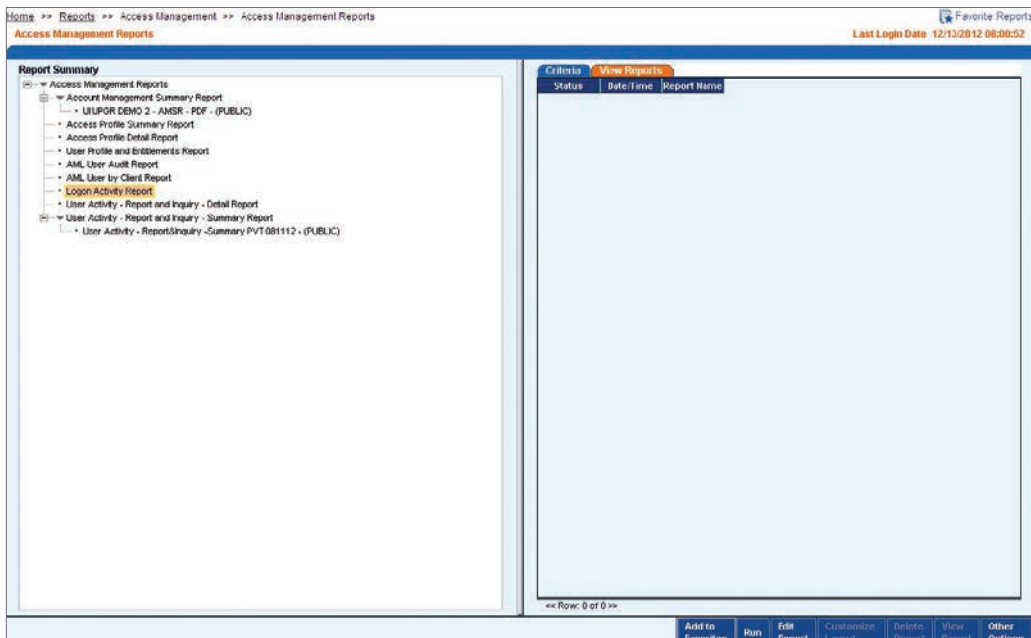
Audit

- [Audit Reports](#)

Access Management

- [Access Management Reports](#)

2. The Access Management Reports form appears.

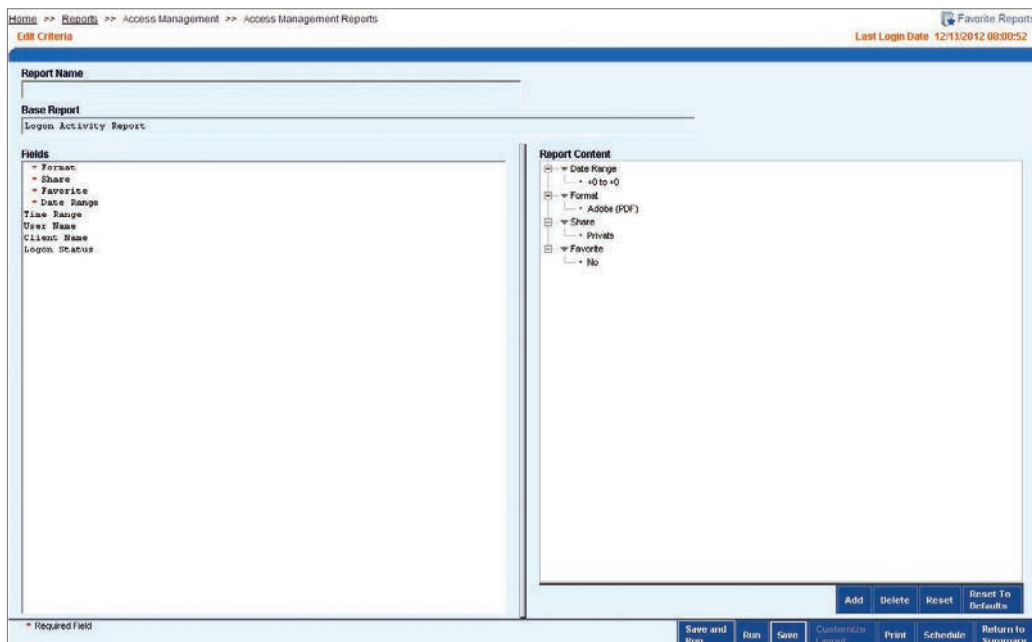


The screenshot shows the 'Access Management Reports' page. At the top, there is a breadcrumb trail: Home >> Reports >> Access Management >> Access Management Reports. The page title is 'Access Management Reports' and the last login date is 12/13/2012 08:08:52. The main content area is divided into two sections:

- Report Summary:** A tree view showing the following reports:
 - Account Management Summary Report
 - ULIPOR DEMO 2 - AMSR - PDF - (PUBLIC)
 - Access Profile Summary Report
 - Access Profile Detail Report
 - User Profile and Entitlements Report
 - AML User Audit Report
 - AML User by Class Report
 - Logon Activity Report
 - User Activity - Report and Inquiry - Detail Report
 - User Activity - Report and Inquiry - Summary Report
 - User Activity - ReportInquiry - Summary PVT 081112 - (PUBLIC)
- Criteria View Reports:** A table with columns for Status, Date/Time, and Report Name. The table is currently empty.

At the bottom of the page, there is a navigation bar with the following buttons: Add to Favorites, Run, Edit Report, Customization Legend, Delete Report, View Report, and Other Options. Below the table, it says '<< Row: 0 of 0 >>'.

- In the Report Summary list box on the left, select the Logon Activity Report, and then click the Edit Report button. The Edit Criteria form appears.

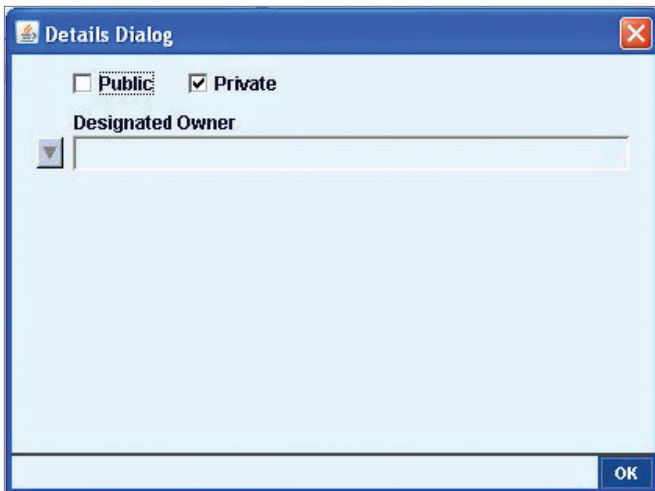


Note: If you do not click the Edit Report button before running the report, the CitiDirect predefined report is run. You will receive information regarding all actions taken by all users. Use the Edit Report feature to filter the data.

- Define the content of your report by selecting criteria elements from the Fields list box, as described below.
 - Select the Format criterion to change the format of your report. If you do not specify a format, the report is displayed in PDF (Acrobat Reader 9.0 required), the CitiDirect-defined default format for reports. The other available report formats are Comma Separated Values (CSV), Microsoft Excel (XLS), and DHTML

Note: The DHTML output format is only available for CitiDirect reports that contain drilldown links.

- Select the Share criterion to allow other users at your organization to run or view this report. The Details dialogue box appears:



The CitiDirect-defined designation is Private and the Designated Owner field displays the name of the signed-on user (typically your name).

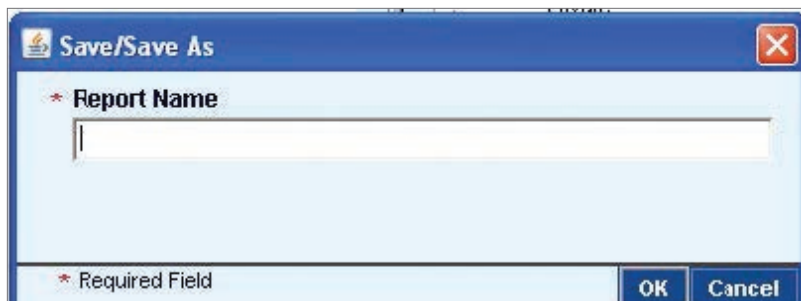
To make the report public, select the Public checkbox. If you want to make another user the owner of the report, select that user's name from the Designated Owner field.

Notes:

Only the designated owner can modify or delete the report.

Once changes are saved, you will lose ownership rights to the report if you have designated someone else the owner. Only the newly designated owner may entitle you to resume ownership of the report.

- Select the Favorite criterion to add the report to your Favorite Report list in the Report Assistant. After the report is saved, you can press ALT+R on your keyboard to navigate directly to the Report Assistant from anywhere in CitiDirect. For more information on using the Report Assistant, refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com.
 - Select the Date Range criterion to enter the time period you want the report to cover. The date range must fall within the last nine months.
 - Select the Time Range criterion to enter the range of time the event was performed.
 - Select the User Name criterion to select a particular user, usually by First or Last Name, User ID, SafeWord card.
 - Select the Logon Status to select the status of the last logon attempt, either Successful or Unsuccessful.
5. After you have selected your report criteria, proceed with one of the following steps:
- Click the Run button to run the report.
The report is run and its name appears on the Report Summary list and on the View Reports tab with the notation Unsaved before the report name. The status of the report changes from Waiting to Running to Available.
When the status is Available, click the View Report button. The report appears in a separate browser window.
 - Click the Save button to save the current report. The Save/Save As dialogue box appears.



Enter a Report Name and click the OK button. The new report name is added to the Report Summary list.

- Click the Save and Run button to save and immediately run the report. The Save/Save As dialogue box appears. After you enter a Report Name and click the OK button, as described above, the report is run. The report name is added to the Report Summary list and the View Reports tab. After a brief period, its status changes from Waiting to Running to Available. When the status is Available, you can view the report.
- Click the Print button to print the report criteria. The criteria listed in the Report Content list box is printed, not the actual report.
- Click the Schedule button to schedule the report to run at specific times. This allows you access to Automated File and Report Delivery (AFRD). For more information on AFRD, refer to the Automated File/Report Delivery guides in the Learning Center at www.citidirect.com.
- Click the Return to Summary button to return to the Access Management Reports. If you have selected criteria, you will be prompted to save the report.

Sample Logon Activity Report

Report content varies based on the criteria you have selected.

citi		CitiDirect® Online Banking			
Logon Activity Report					
Client Name UI UPGRADE DEMO 2					
Logon ID	User Name	First Logon Date/Time	Last Logon Date/Time	# of Attempts	Status of Logon
CSA_100	USER 1	07/02/2012 13:58:47	07/02/2012 13:58:47	1	SUCCESSFUL
CSA_100	USER 1	08/14/2012 14:25:15	08/14/2012 14:25:15	1	SUCCESSFUL

Below is an alphabetic listing of the information contained in this report:

1. Client Name
2. Number of Attempts
3. First Logon Date/Time
4. Status of Logon
5. Logon Date/Time
6. User Name
7. Logon ID

User Profile and Entitlements Report

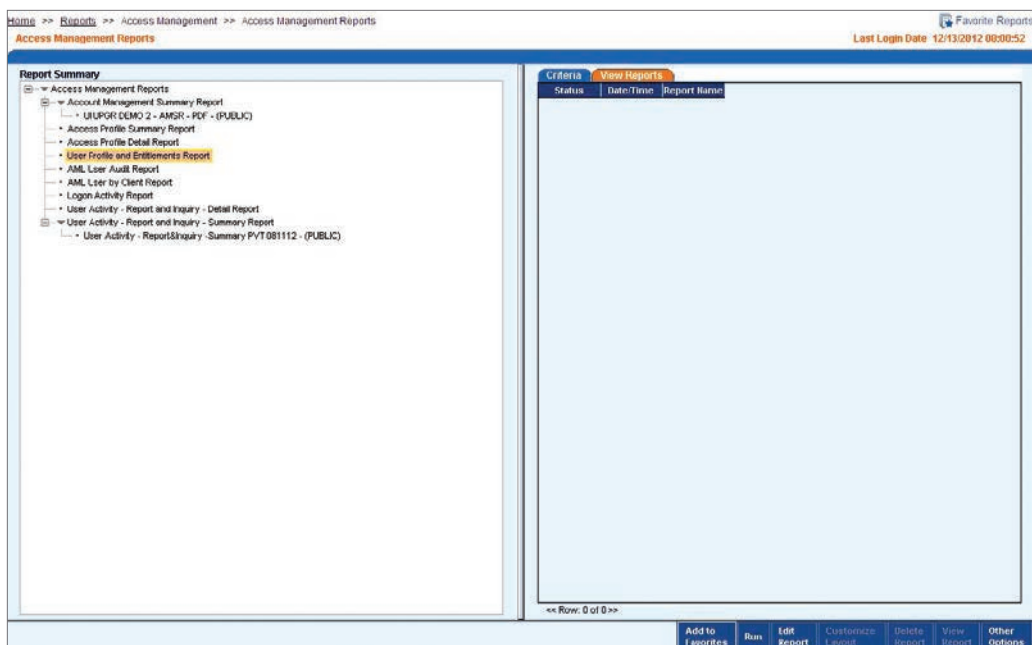
The User Profile and Entitlements Report is a powerful report that enables you to access both user profiles and entitlements information in one report. This report can be very useful for audit purposes and troubleshooting. For example, the report can be structured, based on the input criteria you select, to display all users with a specific access profile, all users in a particular country, SafeWord card users only and which users are set to expire on CitiDirect. Additionally, the report provides a hyperlink to drill down from the access profile name to the access profile detail report.

Run the User Profile and Entitlements Report by following the steps below:

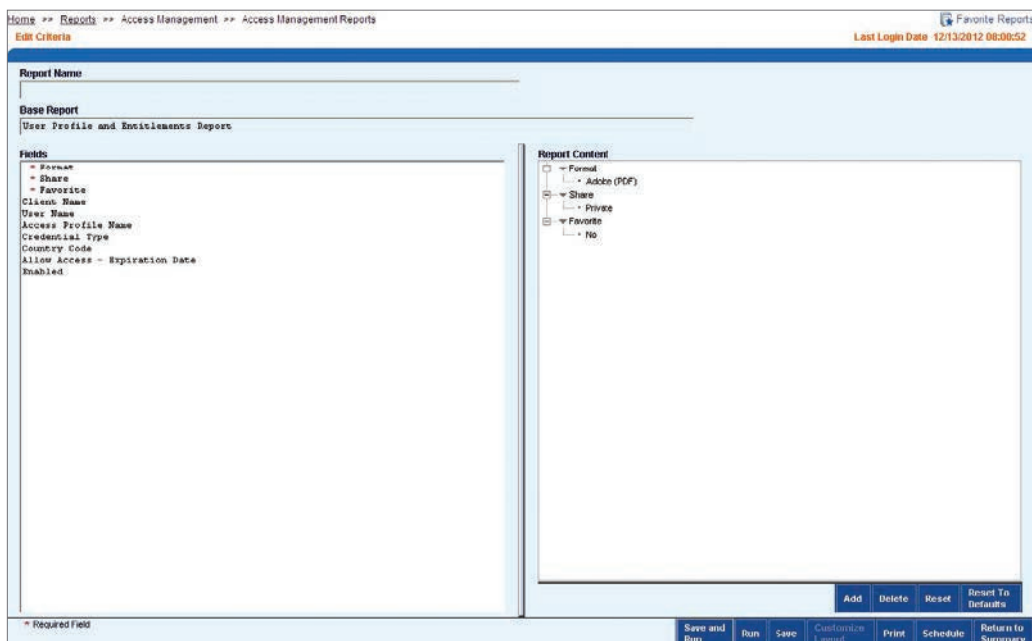
1. On the CitiDirect menu under Reports, click Access Management Reports as shown below.



2. The Access Management Reports form appears.



3. In the Report Summary list box on the left, select the User Profile and Entitlements Report, and then click the Edit Report button. The Edit Criteria form appears.



Note: If you do not click the Edit Report button before running the report, the CitiDirect predefined report is run. You will receive information regarding all actions taken by all users. Use the edit report feature to filter the data.

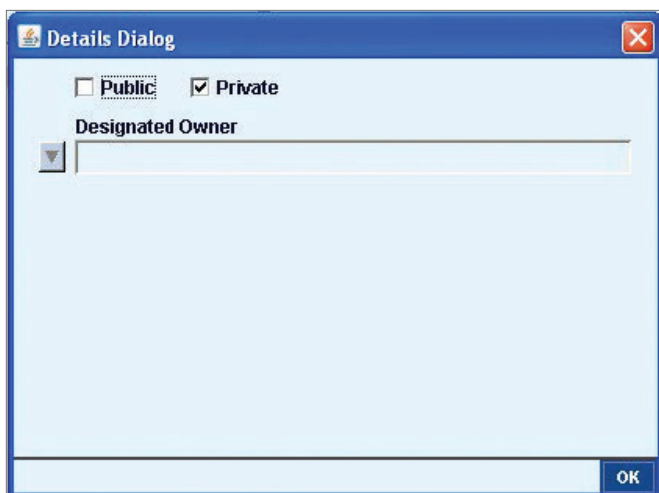
4. Define the content of your report by selecting criteria elements from the Fields list box, as described below.

- Select the Format criterion to change the format of your report.

If you do not specify a format, the report is displayed in PDF (Acrobat Reader 9.0 required), the CitiDirect-defined default format for reports. The other available report formats are Comma Separated Values (CSV), Microsoft Excel (XLS) and DHTML

Note: The DHTML output format is only available for CitiDirect reports that contain drilldown links.

- Select the Share criterion to allow other users at your organization to run or view this report. The Details dialogue box appears:



The CitiDirect-defined designation is Private and the Designated Owner field displays the name of the signed-on user (typically your name).

To make the report public, select the Public checkbox. If you want to make another user the owner of the report, select that user's name from the Designated Owner field.

Notes:

Only the designated owner can modify or delete the report.

Once changes are saved, you will lose ownership rights to the report if you have designated someone else the owner. Only the newly designated owner may entitle you to resume ownership of the report.

- Select the Favorite criterion to add the report to your Favorite Report list in the Report Assistant. After the report is saved, you can press ALT+R on your keyboard to navigate directly to the Report Assistant from anywhere in CitiDirect. For more information on using the Report Assistant, refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com.
- Select the User Name criterion to search for and select a particular user by First or Last Name, User ID, SafeWord ID or Secured Password ID.
- Select the Access Profile Name criterion to search for and select a particular access profile by name.
- Select the Credential Type criterion to select the type of security credential.
- Options are SafeWord ID Only or Secured Password Only. If nothing is selected, the Citibank-defined value is All.

- Select the Country Code criterion to select the ISO country code that represents the country for which you want to see data.
- Select the Allow Access - Expiration Date criterion to select a date, or date range, on which the user profiles are active on CitiDirect.
- This field corresponds to the Allow User Access to Days field on the User Profile Detail form and can be used to determine when users are set to expire on CitiDirect.
- Select the Enabled criterion to select the current status of the users to include in the report data.

5. After you have selected your report criteria, proceed with one of the following steps:

- Click the Run button to run the report.
The report is run and its name appears on the Report Summary list and on the View Reports tab with the notation Unsaved before the report name. The status of the report changes from Waiting to Running to Available.
When the status is Available, click the View Report button. The report appears in a separate browser window.
- Click the Save button to save the current report. The Save/Save As dialogue box appears.



Enter a Report Name and click the OK button. The new report name is added to the Report Summary list.

- Click the Save and Run button to save and immediately run the report.
The Save/Save As dialogue box appears. After you enter a Report Name and click the OK button, as described above, the report is run.
The report name is added to the Report Summary list and the View Reports tab. After a brief period, its status changes from Waiting to Running to Available. When the status is Available, you can view the report.
- Click the Print button to print the report criteria. The criteria listed in the Report Content list box is printed, not the actual report.
- Click the Schedule button to schedule the report to run at specific times. This allows you access to Automated File and Report Delivery (AFRD). For more information on AFRD, refer to the Automated File/Report Delivery guides in the Learning Center at www.citidirect.com.
- Click the Return to Summary button to return to the Access Management Reports. If you have selected criteria, you will be prompted to save the report.

Sample User Profile and Entitlements Report

Report content varies based on the criteria you have selected.

Client Name		UI UPGRADE DEMO 2	
First Name	USER	Middle Name	
Last Name	ONE	Initials	
Enabled	Y	Street Address	
Building/Floor/Room		City	
State/Province/Territory	DE	Zip Code	
Telephone		Country Code	
Time Zone	EST	Employee ID	
User Account Type	OMNI	E-Mail Address	
Allow User Access To Days	1/10/2013 to 1/10/2014	Days of the Week	Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday
Allow User Access To Time	00:00:00 to 23:59:59		
Credential Type	Credential ID		
Secured Password ID			
Selfword ID			
Assigned Access Profiles	Client Name		
AUTOMATED FILE AND REPORT DELIVERY	UI UPGRADE DEMO 2		
CASH REPORT CUSTOMIZER	UI UPGRADE DEMO 2		
INQUIRY AND REPORTS	UI UPGRADE DEMO 2		
Billing Account Number			
Total Number of Users	1		

Below is an alphabetical listing of the information contained in this report:

1. Allow User Access Days
2. Employee ID
3. Allow User Access Time
4. Enabled
5. Assigned Access Profiles
6. First Name
7. Building/Floor/Room
8. Initials
9. City
10. Last Name
11. Client Name
12. Middle Name
13. Country Code
14. State/Province/Territory
15. Credential ID
16. Street Address
17. Credential Type
18. Telephone
19. Days of the Week
20. Time Zone
21. E-mail Address
22. Total Number of Users
23. User Account Type (Same Day Reconciliation clients – the values are either Omnibus Account or Sub Account.)
24. Zip Code

Security Manager Inquiries

The Inquiries and Search category on the CitiDirect menu contains service classes that represent individual inquiries, each designed for a specific business purpose. Inquiries provide a snapshot of information as of the current point in time.

Note: For detailed instructions on selecting report criteria and running inquiries refer to the Reports and Inquiry guide, available in the Learning Center at www.citidirect.com, in the CitiDirect Basics section, Basics Guides tab.

Inactive User Inquiry

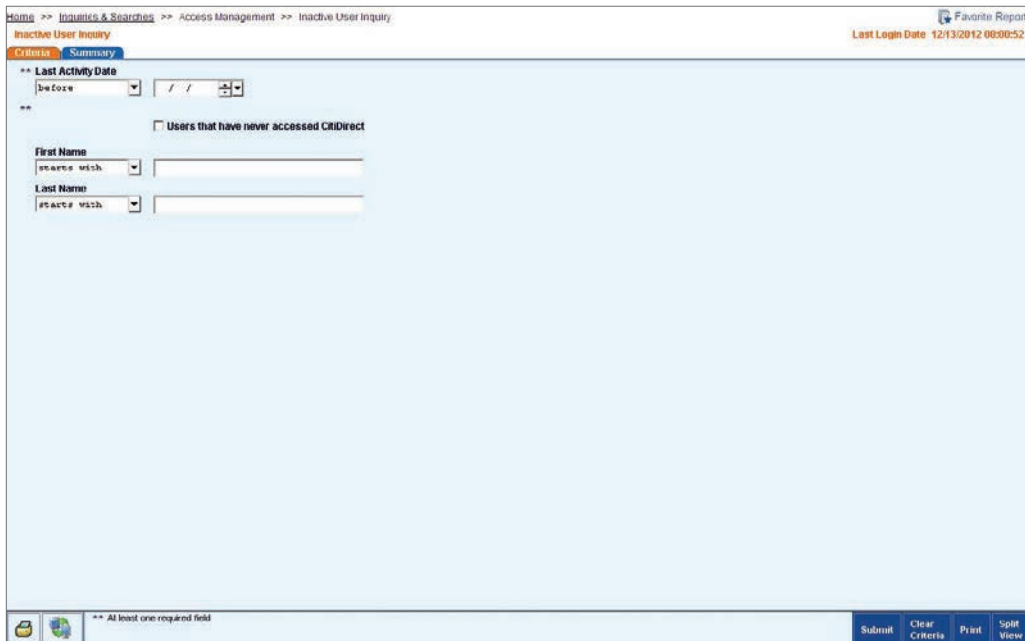
CitiDirect Online Banking tracks application usage and automatically generates a report listing users who have not signed onto the application for a period of at least 60 calendar days prior to the last activity date. As a Security Manager, you should run this inquiry periodically to determine if a user profile should be disabled or deactivated.

Specify search criteria and submit an Inactive User Inquiry by following the steps below:

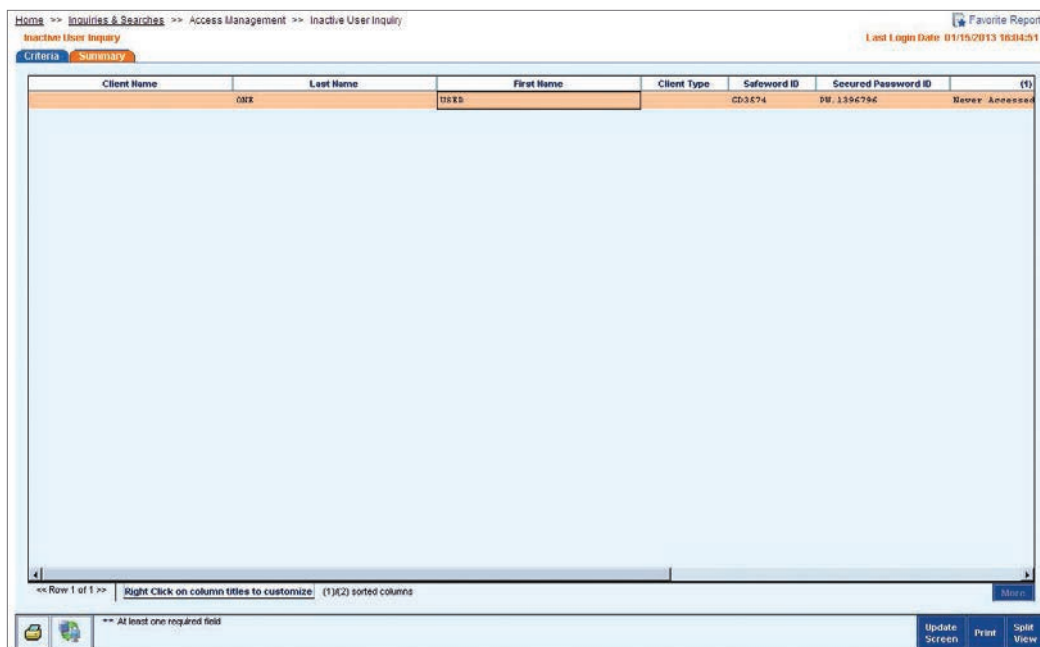
1. On the CitiDirect menu under Inquiries & Searches, click Inactive User Inquiry as shown below.



2. The Inactive User Inquiry form appears.



3. Enter search criteria to find the information you need by completing one or more of the fields below.
 - In the Last Activity Date field, enter a date for which you want to track the last activity in CitiDirect.
 - Select the Users that have never accessed CitiDirect checkbox to include the names of all established CitiDirect users in your organization who have never signed onto CitiDirect.
 - To view activity associated with a specific user, enter the name of the user in the First Name and Last Name fields.
4. Click the Submit button. All inactive users who match your search criteria appear on the Summary tab.



5. Select one or more rows and proceed with one of the following:
 - Click the Update Screen button to update the summary list with the most recent information.
 - Click the Print button to print a summary list of the selected records, including column headings.
 - Click the Split View button to split the form and see the Criteria and Summary tabs on one screen.

Security Manager Support Functions

This section provides detailed instructions for support functions that you are typically required to perform as a Security Manager.

SafeWord™ Platinum Card Distribution

Depending on your region and organizational practice, you may be responsible for distributing SafeWord Platinum cards to the CitiDirect Online Banking users in your organization.

If you distribute SafeWord cards to your users, factors that can affect activation of a new card are how quickly the second Security Manager can authorize the user profile and how quickly you can distribute the new SafeWord card to the user.

If Citibank is distributing the SafeWord cards, please allow for mailing time. It is crucial that the name and address information included in a user profile is complete and accurate, as the cards are shipped from Citi directly to the addresses listed in users' profiles.

For more information about user profiles and security credentials, refer to the Creating New User Profiles section of this guide.

Replacing SafeWord Platinum Card Security Credentials

As Security Manager, you may be required to replace malfunctioning or lost SafeWord cards. For malfunctioning cards, advise the user to return the original SafeWord card to you via the most secure method possible. For lost or stolen cards, immediately contact Citi.

Note: In the Asia-Pacific region, the process used by a Security Manager to replace a lost SafeWord card is to delete the existing user profile and create a new user profile.

Replace SafeWord security credentials by following the steps below:

1. On the CitiDirect portal menu, click User Worklist under Self Service.



2. Click on Processed to view the Processed users.

Self Service > Client Administration Service > User Worklist

User(s): Processed

Client: UI UPGRADE DEMO 2 | Subscription: 2 Products, 13 Services

Users: To Authorize To Modify Processed Print

Filters

Created From: To: First Name: Last Name: Status:

Filtered By - First Name

Processed 1 - 1 of 1 Customize

Last Name	First Name	Status	Comments
User	User 1	Active	

3. Click on the First Name of any user to load the User Detail form.

User- To Processed Print

* Required Field

User Details
Workflow Status: Processed Status: Active

General Information

User Alias: Employee ID: * First Name: * Last Name: Middle Name: Initial:

Building/Floor/Room: * Street Address 1: Street Address 2: Street Address 3: * Country:

* State/Province/Territory: * City: Zip/Postal Code: * Time Zone: * Telephone:

* Email: User Manager:

CitiDirect Information

* SDR User Account Type: User ID:

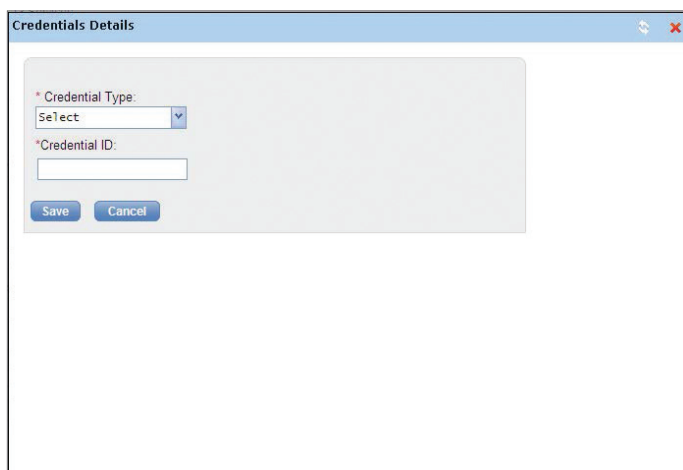
* User Allow Access To Days: to * User Allow Access To Time: to * CitiDirect Time Zone:

Days of Week:

1 - 1 of 1

Credential Type	Credential ID
<input type="checkbox"/> Sefeword_ID	Dummy

4. In the Credentials list box, select the SafeWord ID credential line and then click the Delete button.
5. Click the New button to create the new SafeWord credential. The Credentials Details dialogue box appears.



The screenshot shows a dialog box titled "Credentials Details". Inside the dialog, there is a section with a light gray background. At the top of this section is the label "* Credential Type:" followed by a dropdown menu currently showing "Select". Below this is the label "* Credential ID:" followed by an empty text input field. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

6. Select a SafeWord ID from the Credential Type dropdown list.
7. Proceed with one of the following steps:
 - If your organization distributes SafeWord security credentials, enter the SafeWord card number (found on the back of the card) into the Credentials ID field.
 - If Citi distributes SafeWord security credentials, you can complete this field once the user receives the new card from Citi and notifies you.
8. Click the Save button to save the new SafeWord credential information, and then click the Close button to close the dialogue box.
9. Click the Submit button to save the profile and enter it into the authorization queue. A Warning message appears.

Note: As described in the “Client ID and Initial Sign On/Modified Security Credentials” section of this guide, each new user is required to enter the Client ID at their first sign-on to CitiDirect or after any modification to their security credentials takes place (e.g., a new SafeWord card is assigned to the profile).

- This dialogue box offers you the opportunity to print your company's Client ID information to send to the user. The Client ID information can also be identified in the following ways:
- By placing the cursor over the company name field when working in any CitiDirect form.
- By looking inside the PIN mailer of your security credentials.

Note: Asia/Pacific security managers can obtain Client ID information from the CitiDirect Implementation Manager.

10. Click the Yes button to print the information for the new user or click the No button to continue without printing.

Note: You must instruct the user to delete his or her Sign-on Name and sign onto CitiDirect as a new user by entering the replacement card number in the appropriate fields when he or she signs onto CitiDirect using the new card for the first time. The new Credential ID is the new Sign-on ID the user is required to enter when they sign onto CitiDirect.

The initial secure password is eight alphanumeric characters with the following pattern:

- The first and fifth characters are uppercase letters.
- The third and seventh characters of the password are lowercase letters.
- The second, fourth, sixth and eighth characters of the password are numbers.

For example, if the password generated was A1j2C3l4, the second character will be a 1 (one), and the seventh character will be a lowercase L.

Secured Password Rules

Upon sign-on to CitiDirect Online Banking, the user will be prompted to change their initial password. Secured passwords: Must not be the same as the User ID.

- Must be a minimum of six characters, and consist of mixed alphabetic and numeric characters.
- Must not consist of all numbers, all special characters or all alphabetic characters.
- Must not contain leading or trailing blanks.
- Must not contain more than two consecutive identical characters.
- Must be changed at least every 30 days.

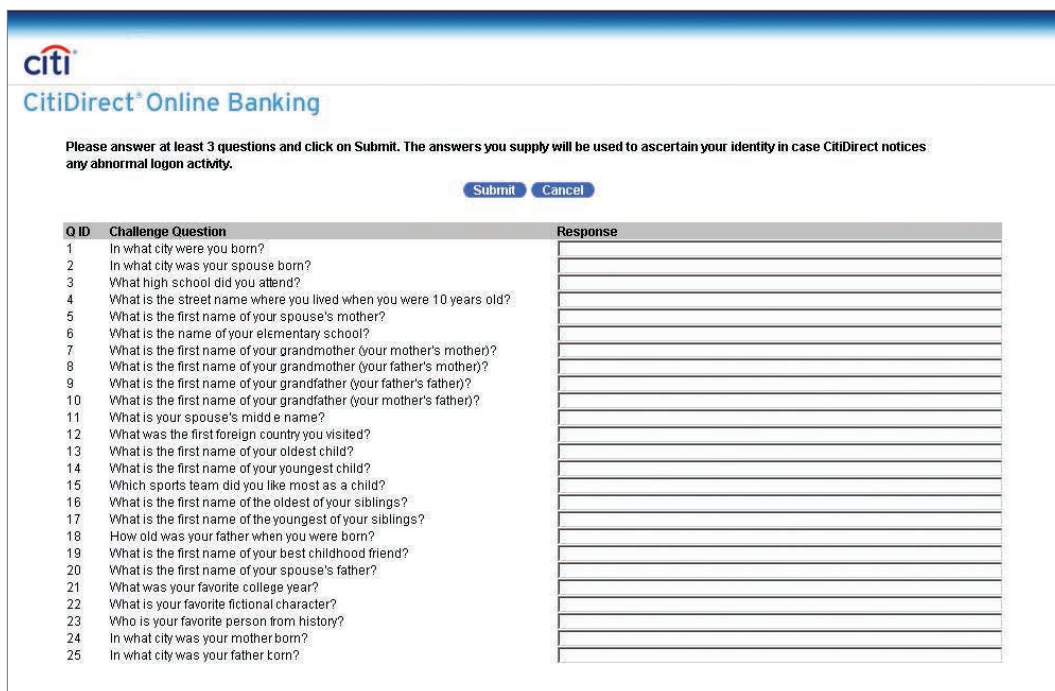
Risk-Based Authentication and Secure Passwords

Citi has risk-based authentication for Secure Password users. Risk-based authentication provides a secondary layer of security that further validates a user's identity during the sign-on process. This second layer of authentication is only applied when an end user changes a usage behavior.

After a sufficient user sign-on history is established, Secure Password users are presented with a series of questions. The user is required to provide private answers to five questions. Should there be a change in sign-on behavior, the end user might be challenged to provide an answer to three randomly chosen questions.

For example, a Secure Password user who commonly signs onto CitiDirect Online Banking from the same computer every day might be challenged with one, two, or three random challenge questions (depending on risk level) when signing on from a different computer or geographical location.

Examples of the questions on the Challenge/Response input screen are provided below (all questions are not shown).



Please answer at least 3 questions and click on Submit. The answers you supply will be used to ascertain your identity in case CitiDirect notices any abnormal logon activity.

Submit Cancel

Q ID	Challenge Question	Response
1	In what city were you born?	
2	In what city was your spouse born?	
3	What high school did you attend?	
4	What is the street name where you lived when you were 10 years old?	
5	What is the first name of your spouse's mother?	
6	What is the name of your elementary school?	
7	What is the first name of your grandmother (your mother's mother)?	
8	What is the first name of your grandmother (your father's mother)?	
9	What is the first name of your grandfather (your father's father)?	
10	What is the first name of your grandfather (your mother's father)?	
11	What is your spouse's middle name?	
12	What was the first foreign country you visited?	
13	What is the first name of your oldest child?	
14	What is the first name of your youngest child?	
15	Which sports team did you like most as a child?	
16	What is the first name of the oldest of your siblings?	
17	What is the first name of the youngest of your siblings?	
18	How old was your father when you were born?	
19	What is the first name of your best childhood friend?	
20	What is the first name of your spouse's father?	
21	What was your favorite college year?	
22	What is your favorite fictional character?	
23	Who is your favorite person from history?	
24	In what city was your mother born?	
25	In what city was your father born?	

Answers/Locked IDs

The end user must respond to the questions as answered on the initial input form to complete the sign-on/authentication process. If a response is incorrect, the user is prompted with another question (from the questions set up earlier).

After six incorrect/failed answer attempts to the questions, the user is prevented from completing their sign-on to CitiDirect. The user must call CitiDirect Support to have the User ID unlocked in the system.

Notes:

This secondary authentication method will only affect Secure Password users (User ID and Password only). Users who have been provided a SafeWord card will not be affected.

Citi recommends that end users have a single method of authentication (SafeWord or Secure Password). Users with both SafeWord and Secure Password should be converted to SafeWord only.

Changing a User's Security Credential Type

You can change a user's security credential type based on the needs of his or her job and your organization's business rules and information security policies. For example, a user may move from a job requiring view-only functions to a job requiring that he or she create or authorize transactions.

Change a user's security credential type by following the steps below:

1. On the CitiDirect portal menu, click User Worklist under Self Service.



2. Click on Processed to view the Processed users.

Self Service > Client Administration Service > User Worklist

User(s): Processed

Client: UI UPGRADE DEMO 2 Subscription: 2 Products, 13 Services

Users: To Authorize To Modify Processed [Print](#)

Filters

Created From: [mm/dd/yyyy] To: [mm/dd/yyyy] First Name: [] Last Name: [] Status: [Select] [Go](#) [Reset](#)

Filtered By - First Name

Processed 1 - 1 of 1 [Customize](#)

Last Name	First Name ▲	Status	Comments
User	User 1	Active	

3. Click on the First Name of any user to load the User Detail form.

User- To Processed
Print

* Required Field

User Details
 Workflow Status: Processed Status: Active

General Information

User Alias: <input type="text" value="dudu9005"/>	Employee ID: <input type="text" value="12345"/>	* First Name: <input type="text" value="USER 1"/>	* Last Name: <input type="text" value="USER"/>	Middle Name: <input type="text"/>	Initials: <input type="text"/>
Building/Floor/Room: <input type="text"/>	* Street Address 1: <input type="text" value="1234"/>	Street Address 2: <input type="text"/>	Street Address 3: <input type="text"/>	* Country: <input type="text" value="UNITED STATES"/>	
* State/Province/Territory: <input type="text" value="DE"/>	* City: <input type="text" value="XYZ"/>	Zip/Postal Code: <input type="text" value="12345"/>	* Time Zone: <input type="text" value="Eastern Time (US & Ca)"/>	* Telephone: <input type="text" value="1234567890"/>	
* Email: <input type="text" value="user@citi.com"/>	User Manager: <input type="text"/>				

CitiDirect Information

* SDR User Account Type: User ID:

* User Allow Access To Days: to
 * User Allow Access To Time: to
 * CitiDirect Time Zone:

Days of Week:
 SUNDAY
 MONDAY
 TUESDAY
 WEDNESDAY
 THURSDAY
 FRIDAY
 SATURDAY

1 - 1 of 1

Credential Type	Credential ID
<input type="checkbox"/> SafeWord ID	Dummy

In this example, the user has an existing SafeWord ID, and you are adding a Secured Password ID.

Note: If the user no longer requires Secured Password access to CitiDirect, click the Secured Password security credential line and click the Delete button to remove the credential from the profile.

1. In the Credentials list box, click the New button.
2. Select Secured Password ID from the Credential Type dropdown list.

Credentials Details
Close

* Credential Type:

Credential ID:

3. Proceed with one of the following steps:

- If your organization distributes Secured Password security credentials, enter the Secured Password into the Credentials ID field.
- If Citi distributes Secured Password security credentials, leave the Credentials ID field blank.

Citi Transaction Services
transactionservices.citi.com

© 2013 Citibank, N.A. All rights reserved. Citi and Arc Design and CitiDirect are registered service marks of Citigroup Inc.
CitiDirect BE is a service mark of Citigroup Inc.
SafeWord is a trademark of Secure Computing Corporation.
1056609 GTS25194 02/13

