

Q2central Administration Guide

4.3 Release

April 2017

Q2ebanking.com

Notices

This document (including all rights and attachments) contains confidential information and intellectual property belonging to Q2 Software, Inc. Unauthorized use or reproduction of this document or of any aspect of Q2 Software, Inc. confidential information and/or intellectual property as described herein is expressly prohibited without the express written consent of Q2 Software, Inc.

The specifications and information regarding the products in this guide are subject to change without notice. All statements, information, and recommendations in this guide are believed to be accurate but are presented without warranty of any kind, express or implied.

Users must take full responsibility for their application of any products. All document files and software are provided "as is" with all faults. Q2 Software, Inc. and its suppliers disclaim all warranties, express or implied including, without limitation, those of merchantability, fitness for a particular purpose, and noninfringement arising from a course of dealing, usage, or trade practice. In no event shall Q2 Software, Inc. or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of their use or inability to use this guide, even if Q2 Software, Inc. or its suppliers have been advised of the possibility of such damages.

© 2017, Q2 Software, Inc., a Q2 Holdings company. All rights reserved. Q2 and mark, Q2access, Q2assist, Q2central, Q2clarity, Q2mobile Web, Q2mobility Apps, Q2mobile Remote Deposit Capture (RDC), Q2online, Q2security, Q2text, and Q2voice are trademarks. All other trademarks are property of their respective owners.

Document: 10-2423-01

Contents

PREFACE 14
Purpose 14
Audience 14
System requirements 15
Document conventions 15
Q2 Customer Portal 16
Contacting Q2 17
Let us hear from you 17
For more information 17
SECTION I - ADMINISTRATION - SYSTEM CONFIGURATION 18
CHAPTER 1: CSR ROLES 19
CSR Roles overview 19
CSR Roles reference 20
CSR Roles General tab 20
CSR Roles Forms tab 21
CSR Roles tasks 21
Editing a CSR Role 21
CHAPTER 2: CSR USERS 22
CSR Users overview 22
Understanding CSR User Login Types 22
CSR Users reference 23
CSR Users General tab 24
CSR Users Contact Information tab 26
CSR Users Message Groups tab 27
CSR Users Symantec VIP Credential tab 29
CSR Users tasks 30
Adding a CSR User 30
Editing a CSR User 31
Assigning CSR Users to CSR Roles 31

Changing the Admin password 31
Enrolling CSR Users in Secure Messaging groups 32
Deleting a CSR User 32

CHAPTER 3: CSR NOTIFICATIONS 33
CSR Notifications overview 33
Recommended CSR Notifications 34
CSR Notifications reference 38
Manage CSR Notifications page 39
Home page 41
CSR Notification tasks 42
Configuring widgets on the Home page 42
Adding a CSR Notification 43
Editing a CSR Notification 44
Deleting a CSR Notification 45

CHAPTER 4: GROUP ACCESS MAPPING 46
Group Access Mapping overview 46
Understanding Group Access Mapping rights 47
CSR Team examples 48
Group Access Mapping reference 49
Group Access Mapping tasks 51
Preparing for Group Access Mapping 52
Adding a CSR Team 54
Editing a CSR Team 54
Deleting a CSR Team 55
Using the Show CSRs with Full Rights option 55

CHAPTER 5: AUDITING 56
Auditing overview 56
Auditing reference 56
Auditing tasks 57
Retrieving a Customer IP address with action types 58
Verifying User creation 58

Viewing end-user activities 59
Viewing security-related actions by CSRs 59

CHAPTER 6: PASSWORD AND LOGIN POLICIES 61
Password policies overview 61
Password Policy reference 61
Password Policy General tab 61
Password Policy Passwords tab 64
Password Policy tasks 66
Adding a login policy for a channel 67
Adding a password policy for a channel 68

CHAPTER 7: BANK HOLIDAYS 69
Bank Holidays overview 69
Bank Holidays reference 69
Manage Bank Holidays page 70
Edit Bank Holiday page 71
Bank Holidays tasks 72
Adding Bank Holidays 72
Editing Bank Holidays 73
Defining processing for Bank Holidays 74
Deleting Bank Holidays 74

CHAPTER 8: SECURITY FEATURES IN Q2CENTRAL 75
Security codes 76
Secure access codes 76
Symantec VIP token codes 77
Authorizing suspect transactions 78
Mobile authorization codes 79
Multi-factor authentication 80
Challenge questions 81
Session expiration timers 81
Q2 Sentinel reports 82
End user security controls 83

CHAPTER 9: MERCHANT SERVICES FOR Q2VOICE 85
SECTION II - USER MANAGEMENT - END USER CONFIGURATION 86
CHAPTER 10: UNDERSTANDING USER MANAGEMENT 87
User management definitions and relationships 87
Groups 88
Customers 89
Users 90
Login IDs 91
Examples of Customers in Groups 91
CHAPTER 11: CORPORATE BANKING POLICIES AND USERS 93
Corporate Banking overview 93
Differences between Business and Corporate Banking 96
Understanding Dual Action 97
Corporate Banking Policies 98
Group Policies list 99
Group Policy 100
Customer Policy 113
Company Policy 114
Corporate Banking User Roles 115
User Roles 115
CHAPTER 12: DEFINING GROUPS 135
Group overview 135
Group reference 135
Group General tab 135
Group Features tab 143
Group ACH tab 170
Group Preferences tab 174
Group Policy Dashboard tab overview (Corporate Banking) 176
Group Policy Dashboard tab features (Corporate Banking) 178
Group tasks 178
Adding a Group 179

Displaying a Group 179
Editing a Group 179
Copying a Group 180
Deleting a Group 180
Enabling features for a Group 181
Enabling mobile remote deposit capture (mRDC) for a Group 181
Viewing a Group's Customer records 182
Sending a Secure Message to a Group, Customer, User, or Login ID 182

CHAPTER 13: WORKING WITH CUSTOMERS 184

Customer overview 184
Customer accounts overview 185
Customer reference 186
Customer General tab 187
Customer Account Management tab 191
Customer Account List tab 193
Customer External Accounts tab 193
Customer Users tab 194
Customer Rights tab 196
Customer ACH tab 198
Customer Features tab 200
Customer Policy Dashboard tab overview 203
Customer Policy Dashboard tab features 203
Customer tasks 205
Adding a new Customer 205
Editing a Customer 206
Deleting a Customer 208
Using the Add Account wizard 208
Managing Customer accounts 209
Using the Add Account wizard 210
Using the Add External Accounts wizard 211
Viewing Users that belong to a Customer 212

CHAPTER 14: MANAGING USERS 213
User overview 213
User enrollment 214
Understanding User Statuses 217
User reference 218
User General tab 218
User Symantec VIP Credential tab 221
User Secure Access tab 222
User Account Management tab 224
User Accounts tab 226
User External Accounts tab 227
User Logins tab 228
User Rights tab 229
User Features tab 233
User Policy Dashboard Overview tab (Corporate) 240
User Policy Dashboard Features tab (Corporate) 241
User Policy Dashboard Accounts tab (Corporate) 242
User tasks 243
Adding a new User 243
Adding a Q2voice User 244
Adding accounts to a User record 244
Managing User account access 246
Managing User access to external accounts 247
Editing a User 247
Enabling features for a User 247
Enabling all account management rights for a User 248
Enabling User rights to view, draft, approve, or cancel transactions 248
Maintaining secure access information for Users 250
Changing a Password 251
Activating a User 251
Enabling a User 252
Disabling a User 252
Disabling all Users 253

Deleting a User 253
Determining when a User record was created 253
CHAPTER 15: WORKING WITH LOGIN IDS 254
Login IDs overview 254
Login IDs reference 255
New User Login window 255
Logins tasks 257
Adding a new Login 258
Editing a Login 259
Viewing a Login 259
Deleting a Login 260
Disabling a Login 260
Enabling a Login 260
Renewing an initial password 261
Unlocking a password 261
Using CSR Assist 261
Using Q2assist 263
Troubleshooting Login issues 264
CHAPTER 16: MANAGING SUBSIDIARIES 265
Subsidiaries overview 265
Understanding Organizations 266
FI staff requirements 266
Subsidiaries reference 266
Organization Details pane 267
Subsidiaries tasks 269
Searching for an Organization 269
Adding a subsidiary 269
Viewing subsidiary details 270
Editing a subsidiary 271
Deleting a subsidiary 271

SECTION III - CONFIGURATION 272
CHAPTER 17: TRANSACTION CODES 273
Transaction Codes overview 273
Transaction Code reference 273
New or Edit Transaction Code page 274
Transaction Code Tasks 276
Adding a Transaction Code 276
Editing a Transaction Code 276
Deleting a Transaction Code 277
CHAPTER 18: TRANSACTION CODE GROUPS 278
Transaction Code Groups overview 278
Transaction Code Group reference 278
Transaction Code Group tasks 279
Adding a Transaction Code Group 279
Editing a Transaction Code Group 279
Deleting a Transaction Code Group 279
CHAPTER 19: FEE PLANS 280
Fee Plans overview 280
Fee Plan maintenance 281
Configuring the Fee Plan Setup window 281
Fee Plan reference 283
Monthly base fees versus usage fees 283
Custom fees for auditable events 284
Charge only if used option 284
Potential base fee income summary 284
Fee Plan Setup window 284
Fee Plan tasks 285
Creating a Fee Plan 286
Copying a Fee Plan 286
Viewing or editing a Fee Plan 286
Deleting a Fee Plan 287

Generating fees and Fee Plan processing 287
Applying a Fee Plan to a Customer 287
Processing Monthly Fees 289
Fee Plan processing options 290
Viewing output files for processed activity 290
Oversee Fee Plan activity 291
Supplemental information 291
Credit and debit definitions 291
Fee types in Q2central 292
SECTION IV - COMMUNICATION 296
CHAPTER 20: SECURE MESSAGING 297
Secure Messaging overview 297
Configuring Secure Messaging 298
Secure Messaging reference 301
Secure Messaging page 302
Managing Secure Messaging page 304
Secure Messaging tasks 308
Viewing secure messages 308
Sending secure messages 308
Forwarding messages on the Secure Messaging page 309
Sending a secure broadcast message to all end users 310
Sending a secure message to all Users in a Group 310
Sending a secure message to all Users linked to a Customer 311
Sending a secure message to a single user 312
Sending a secure message to a login ID 313
CHAPTER 21: MARKETING MESSAGES 314
Marketing Messages overview 314
Ad types 315
Ad Elements overview 315
Banners and sidebars 316
Interstitial page 319
Logoff page 321

Image recommendations 321
System Notifications overview 322
Marketing Messages tasks 323
Configuring an Ad Element 323
Adding a System Notification 326
Setting or editing dates for an ad 327
Deleting an ad 327
Adding a marketing message to a theme 327
Marketing Messages FAQs 328
Ad Elements 328
System Notifications 329
SECTION V - DAILY PROCESSING - SYSTEM ALERTS 330
CHAPTER 22: SYSTEM ALERTS 331
Suspect Transactions overview 331
New Postings overview 332
Locked Logins overview 333
Login statuses 334
Restoring end user access 336
Forgotten and first-time passwords 337
Resetting an end user's password 337
Retrieving an end user's secure access code 338
Disabled Logins overview 338
CSR User Lockouts overview 339
CSR Disabled Logins overview 339
New Messages overview 340
New Messages tasks 340
End user alerts overview 345
APPENDIX A: HELPFUL TIPS FOR WORKING WITH Q2CENTRAL 347
Q2central search techniques 347
Default searches 347
Filtering search results 347
Searching for information in Q2central 348

Using the Field Chooser 349
Filtering data 349
Grouping data columns 351
Q2central Documentation 352

PREFACE

This section explains the purpose and audience of this guide, Q2central system requirements, and the document conventions used in this guide. It also describes how to access the Q2 Customer Portal and contact Q2.

Purpose

This guide describes how to use Q2central to manage financial institution (FI) users, auditing, password policies, holidays, Corporate Banking entitlements, security features, and online banking end users. It also explains how to configure secure messaging, system alerts, and more for your FI.



Note: Some menu options, features, and functionality mentioned herein may not be available, depending on how Q2central is configured for your FI.

Audience

This guide is designed for FI staff that use Q2central to perform daily tasks, plus those responsible for the administration and setup of Q2central users, Groups, Customers, online banking end users, Transaction Codes, etc.

This guide assumes that you can access all areas in Q2central needed to perform assigned tasks, and that you've read the *Getting Started with Q2central* guide that provides an overview of Q2central, including navigation and search techniques, terminology, and more.

System requirements

Here are the minimum requirements necessary for client computers used to access Q2central:

- Pentium 4, 1-GHz processor, and 500 MB RAM or greater
- Microsoft Windows 7 or later (Windows 10 is recommended)
- Microsoft .NET 4.6.1 Framework or later
- A valid email address for CSR Notifications
- A cable, DSL, or ISDN Internet connection
- Microsoft Excel (recommended)



Note: For optimal results, set the display size to Smaller (100%) in Windows Control Panel. The Medium (125%) setting may result in occasional text display issues.

Document conventions

Unless otherwise noted, the following conventions are used:

Document conventions

Bold	Bold words include attributes, menu names, dialog box names, commands, operators, options, button names, and statements.
Italic	Italicized words include new or emphasized terms and variables for which you must supply an appropriate value, as in a file name.
" "	Words enclosed in quotations include document titles and cross-references to related information that may prove helpful.
`Monospaced`	Words appearing in a monospaced font represent code examples, system information, and words you enter, such as command syntax.
[ ]	Square brackets enclose optional information, as in [log_ name].
< >	A pair of angle brackets enclose labels, tags, and variables.

Document conventions (cont'd)

>	A single angle bracket separates menu options in a single procedure. For example, File > Open.
|	The vertical bar (pipe) indicates choices that may be entered, as in <5 | 6 | 7>.
	Text with this symbol indicate a Note. Notes provide information that supplements the main text, or refers to special situations.
	Text with this symbol indicates a tip. Tips provide information for an alternate method of performing a process or solving a problem.
	Text with this symbol indicates a caution. Cautions advise users of critical situations or situations that could result in a loss of data or system stability.
	Text with this symbol indicates the feature was added from an Idea submitted to the Q2 Customer Portal.

Q2 Customer Portal

During implementation, Q2 provided your FI with a custom link to the Q2 Customer Portal. All Q2 product documentation is available in this portal. In addition to the Q2 Customer Portal, the Q2central guides are also available from the Help > User Guide option in the Q2central menu bar.

If you are unsure about how to log into the Q2 Customer Portal, contact your online banking system administrator for details.

Contacting Q2

Postal Address	Q2 Software, Inc. 13785 Research Blvd., Suite 150 Austin, TX 78750
Phone	(512) 275-0072
Web	https://www.q2ebanking.com/
Blog	https://www.q2ebanking.com/blog/
Support	(512) 275-0072, select option 1

Let us hear from you

Q2 appreciates your comments and suggestions. As a user of our documentation, you can provide unique and valuable input that can directly impact future releases of all documentation. If you have ideas or comments about our product documentation, please send us an email to docfeedback@q2ebanking.com with "Documentation Feedback" in the Subject line.

For more information

For support issues that cannot be resolved with the information provided here, contact Q2 Customer Support at (512) 275-0072, option 1.

For non-support issues, contact your Q2 Relationship Manager.

Section I - Administration - System Configuration

This section includes details about options in the Administration menu of Q2central that you can use to configure various aspects of the online banking system used by your financial institution (FI), including:

- FI staff rights, roles, and notifications
- Group Access Mapping
- Auditing FI-staff and end-user activities
- Password Policies
- Bank Holidays
- Security features

CHAPTER 1: CSR ROLES

In Q2central, FI staff that assist online banking end users are referred to as customer service representative (CSR) Users.

Each CSR User is assigned to a CSR Role that provides the structure for rights (that is, permissions) to use the various features and functionality available in Q2central. For example, one CSR Role may allow CSR Users to access login-related pages to assist end users locked out of online banking, but restrict access to other pages used for auditing.



Tip: For security purposes, be conservative about assigning any unnecessary rights to CSR Roles.

This chapter includes the following sections to help you understand the importance of CSR Roles within Q2central:

- "CSR Roles overview" on page 19
- "CSR Roles reference" on page 20
- "CSR Roles tasks" on page 21

CSR Roles overview

CSR Roles are initially established during implementation, when Q2 staff configures online banking for your FI.

After implementation, FI staff is responsible for maintaining how CSR Users are assigned to CSR Roles. Each CSR User is assigned to exactly one CSR Role. CSR Roles range from level 1 (L1) through level 5 (L5). The CSR-L5 role is a "super user" that is typically reserved for administrators.



Caution: Assign CSR Users to the CSR-L5 role with caution, as the rights included in that CSR Role are virtually unlimited.

If your FI uses the optional Group Access Mapping feature, you can use it to control the ability of CSRs to view and edit records. See "Group Access Mapping" on page 46.

CSR Roles reference

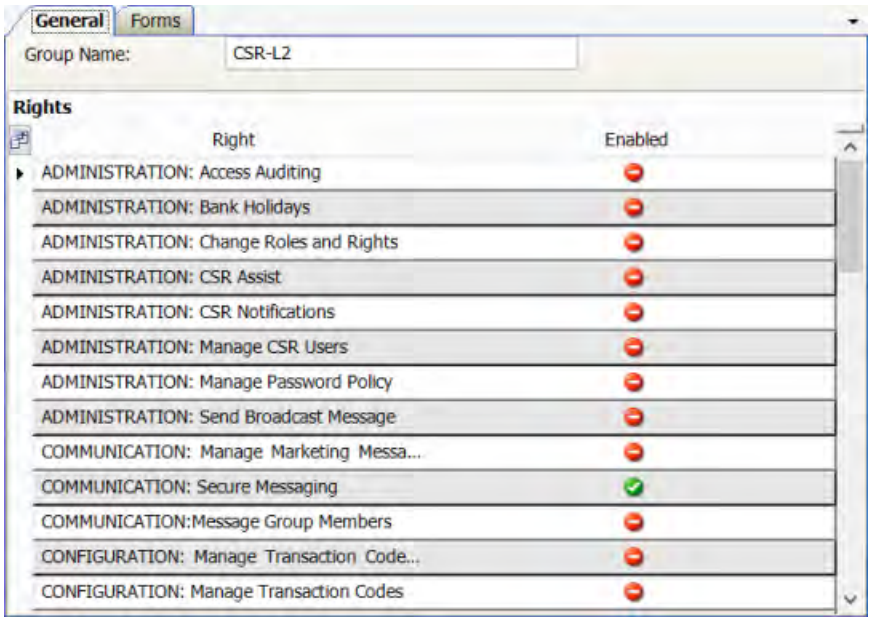
This section describes the tabs available on the CSR Role page. Navigate to the **Administration > CSR Roles** in the Q2central workspace tree to access this page and display a list of CSR Roles. When the CSR Roles page appears, double-click a CSR Role record to view details about it.

CSR Roles General tab

The General tab in the CSR Roles page lists the available rights, grouped by Q2central workspace tree areas. For a complete list of available rights, refer to the *Q2central Reference Lists* document.

You can also change the name of a CSR Role by editing the Group Name at the top of the General tab. By default, the CSR Roles are called CSR-L1, CSR-L2, etc.

CSR Roles General tab

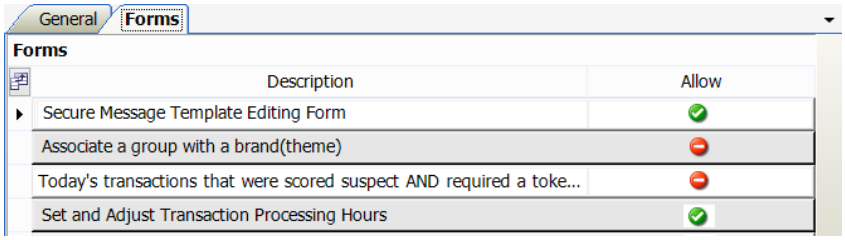


Note: Only enable the *USER MANAGEMENT: Corporate Policy Management* right if your FI purchased Corporate Banking. Otherwise, a non-functional Corporate option will appear in the workspace tree.

CSR Roles Forms tab

The Forms tab lists forms that a CSR assigned to the role can access.

CSR Roles Forms tab



CSR Roles tasks

CSR Roles are assigned to FI staff to allow and restrict functionality in Q2central.

Tip: Your CSR Role must have the *ADMINISTRATION: Change Roles and Rights* right enabled to edit a CSR Role.

Editing a CSR Role

Caution: Changes to a CSR Role impact all CSRs assigned to a role.

To edit a CSR Role

1. In the workspace tree, click **Administration > CSR Roles**.
2. Right-click the CSR Role you want to edit, and click **Edit CSR Group**.
3. On the General tab of the CSR Role page, click the Disabled icon (⛔) for each right to enable it. The Enabled icon (✅) will appear.
4. Switch to the Forms tab and enable each form that CSRs assigned to this role will be able to access.
5. In the toolbar, click **Save and Close**.

Tip: Many rights and forms allow FI staff to directly affect data. Administer permissions accordingly.

CHAPTER 2: CSR USERS

FI staff that use Q2 products are known as *CSR Users* in Q2central. CSR User details, including login ID, password, contact information, messaging groups, and optional Symantec VIP credentials are all managed via the **Administration > CSR Users option** in Q2central.

This chapter includes the following sections:

- "CSR Users overview" on page 22
- "CSR Users reference" on page 23
- "CSR Users tasks" on page 30

CSR Users overview

You can use CSR Users workspace to display details about all FI staff that have rights in Q2central. Each row represents one FI employee.

Tip: You must be assigned to a CSR Role that has the *ADMINISTRATION: Manage CSR Users* right enabled to manage CSR Users.

Understanding CSR User Login Types

When setting up CSR Users, you can select from two types of authentication to be used when a CSR User logs into Q2central. An FI can have CSRs with a mixture of both authentication types in its CSR pool.

One method called *Internal Password Authentication* can be used if your FI supports ad-hoc creation of login IDs and passwords for CSR Users. When a CSR User logs into Q2central, the system compares the login ID and password with encrypted data stored in the Q2 database to authenticate the login.

A second method, *Windows Authentication*, allows FI staff to log into Q2central using network credentials stored in Microsoft Active Directory. Q2 uses Lightweight Directory Access Protocol over SSL (LDAPS) Global Catalog (GC) for this method, which provides these benefits:

- The FI can maintain login and password data in one place, and
- FI staff have fewer credentials to remember.

The FI is responsible for establishing and maintaining the Active Directory (AD) server, software, credentials, and the SSL certificates that digitally bind cryptographic keys. The FI provides those details to Q2 during implementation so that Q2platform components can pass through the FI's firewall, as necessary.



Note: Although Q2central checks the Global Catalog on the FI's server to verify CSR credentials, the actual credentials are not known to Q2. The information remains encrypted.

CSR Users reference

The settings for creating, contacting, and authorizing CSR Users in Q2central are contained in the CSR Users page. To access this page, navigate to **Administration > CSR Users** to display a list of existing CSR Users and then double-click a CSR User record.

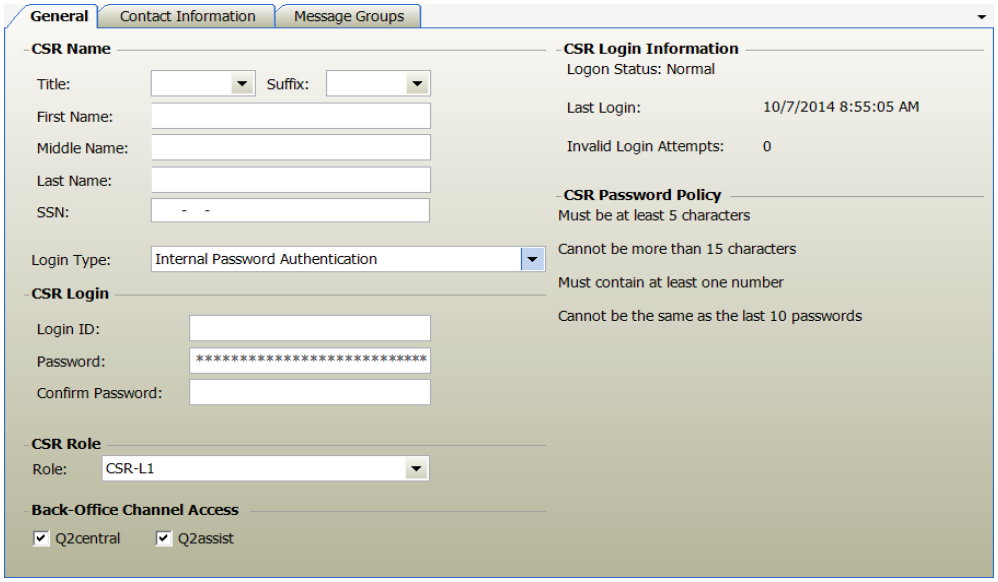
The CSR Users page contains the following tabs for setting up CSR Users:

- "CSR Users General tab" on page 24
- "CSR Users Contact Information tab" on page 26
- "CSR Users Message Groups tab" on page 27

CSR Users General tab

The CSR Users General tab provides login, password, CSR Role, and back-office channel access for FI staff. It also displays recent login data and the FI password policy.

CSR Users General tab



CSR General tab options

Option	Description
CSR Name section	
Title	The title of the CSR User (for example, Dr., Mr., or Ms.).
Suffix	The name suffix for the CSR User (for example, Jr or Sr.
First Name	The first name of the CSR User.
Middle Name	The middle name of the CSR User.
Last Name	The last name of the CSR User.
SSN	The Social Security number for the CSR User.

CSR General tab options (cont'd)

Option	Description
Login Type	The type of authentication used for the CSR User: *Internal Password Authentication*, or *Windows Authentication*. See "Understanding CSR User Login Types" on page 22 for details.
CSR Login section	
Login ID	The identifier used by the CSR User to log into Q2central.
Password	Click **Change Password** to open the Change Password dialog box and either establish or change a CSR's password. When finished, communicate the password details directly to the CSR User. **Tip:** The Password Policy displayed on this tab displays your FI's rules for passwords.
CSR Role	The CSR Role assigned to the CSR User. **Note:** If a CSR User has access to Q2assist but not Q2central, this field will not appear on the General tab.
Back-Office Channel Access	Select the programs the CSR User can access: Q2central and/or Q2assist. (To learn more about Q2assist, see "Using Q2assist" on page 263.) **Note:** If a CSR User that only has access to Q2assist attempts to log into Q2central, an "Invalid Password" message appears.
CSR Login Information	Displays the current login status (see "Login statuses" on page 334) of the CSR User; date and time of most recent login; and number of invalid login attempts.

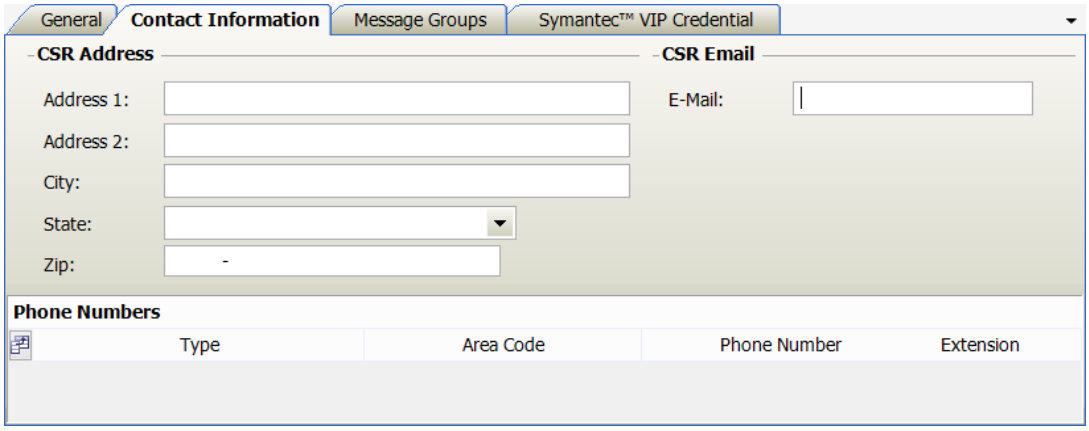
CSR General tab options (cont'd)

Option	Description
CSR Password Policy	Displays requirements for the CSR User's password, as defined on the Password Policy page. See "Password and Login Policies" on page 61.

CSR Users Contact Information tab

You can use the CSR Users Contact Information tab to track the mailing address, email address, and phone numbers for CSRs. Maintaining current email address is critical so CSRs can receive system-generated notifications. Your FI determines if you collect address and phone contact information.

CSR User Contact Information tab



CSR Contact Information tab options

Option	Description
CSR Address	
Address 1	The first line of the address of the CSR's mailing address (if applicable).
Address 2	The second line of the address of the CSR's mailing address (if applicable).
City	The city for the CSR's mailing address.

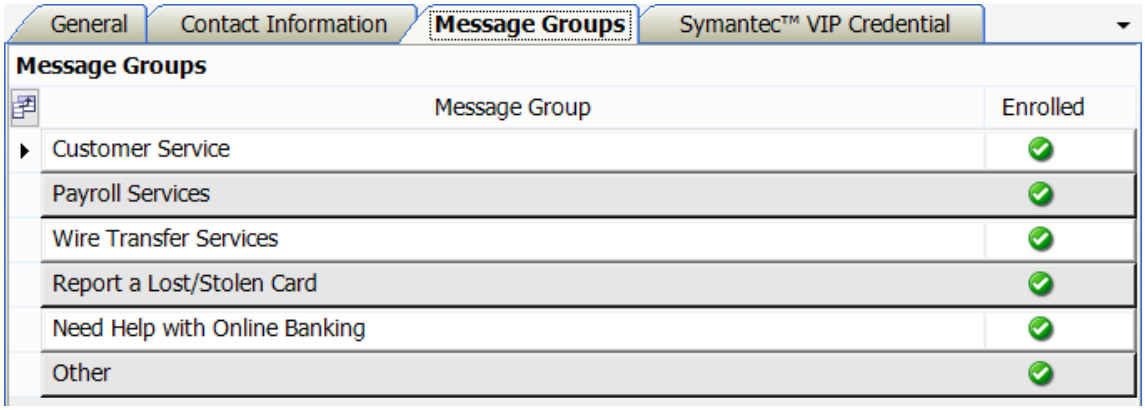
CSR Contact Information tab options (cont'd)

Option	Description
State	The state for the CSR's mailing address.
ZIP	The ZIP code for the CSR's mailing address.
CSR Email	
E-mail	The email address for the CSR.
Phone Numbers	
New Phone Number	**To add a phone number for a CSR** 1. Right-click in the Phone Numbers area of the Contact Information tab. 2. Click **New Phone Number** in the shortcut menu that appears. 3. Enter details in the fields provided. 4. Click **Save**.
Delete Phone Number (Right-click menu)	**To delete a phone number** 1. Select a row in the Phone Numbers area of the Contact Information tab. 2. Right-click to open the shortcut menu. 3. Click **Delete Phone Number** 4. Click **Yes** to confirm the deletion.

CSR Users Message Groups tab

You can use the Message Groups tab to enroll a CSR User in one or more Secure Messaging groups, which are distribution groups that receive messages from end users. For example, CSRs enrolled in the Payroll Services group receive a copy of any message sent to that category. See "Secure Messaging overview" on page 297.

CSR Users Message Groups tab



CSR Users Message Groups tab options

Option	Description
Message Group	The name of the Secure Messaging group.
Group Description	A brief description of the Secure Messaging group. **Note:** This field appears if the option was enabled during implementation and the field is selected in the Field Chooser. See "Understanding Secure Messaging group descriptions" on page 307.
Enrolled	Indicates if a CSR is enrolled in or excluded from a Secure Messaging group.

Tip: Make sure the CSR has a valid email address on file by using the Field Chooser to display the NotificationEmailAddress column on this tab. See "Using the Field Chooser" on page 349 for details.

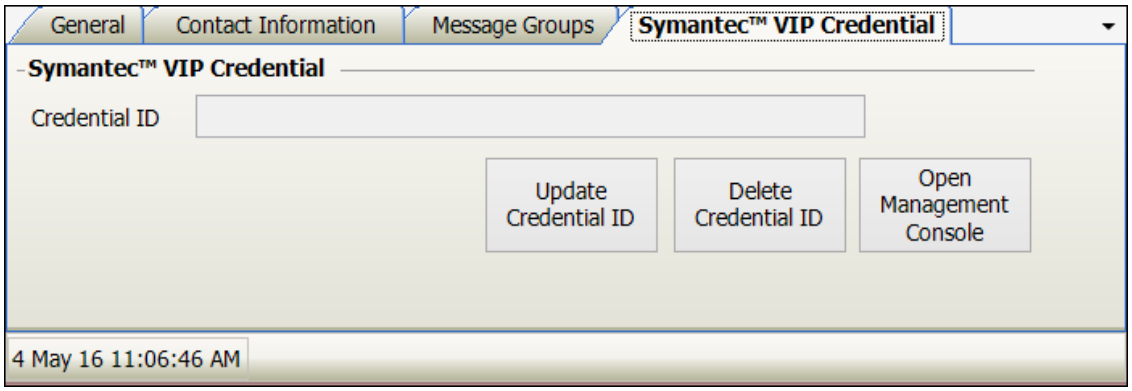
You can also manage Secure Messaging groups via the **Communication > Secure Messaging** option in the workspace tree. See "Configuring Secure Messaging" on page 298.

CSR Users Symantec VIP Credential tab

In addition to a login ID and password, an FI can require that CSRs provide a VIP token code. See "CSR VIP token codes" on page 78 for details.

Note: CSRs can be temporarily locked out if too many unsuccessful login attempts occur.

Symantec VIP Credential tab



Symantec VIP Credential tab options

Option	Description
Credential ID	The Credential ID associated with the CSR User. For a physical Symantec VIP token, this ID appears on a sticker on the back of the token. In the VIP Access mobile app, the Credential ID appears on the main page of the app.
Update Credential ID	Opens the Symantec VIP Credential ID window to provide a new or updated Credential ID issued by Symantec.
Delete Credential ID	Clears the Credential ID tab; authorization will not occur.
Open Management Console	Provides access to the Symantec VIP Manager application where you can manage VIP credentials for CSR Users.

CSR Users tasks

This section describes standard tasks for CSR Users, including:

- "Adding a CSR User" on page 30
- "Editing a CSR User" on page 31
- "Assigning CSR Users to CSR Roles" on page 31
- "Changing the Admin password" on page 31
- "Enrolling CSR Users in Secure Messaging groups" on page 32
- "Deleting a CSR User" on page 32

Tip: The CSR Role to which you are assigned must have the *ADMINISTRATION: Manage CSR Users* right enabled to perform these tasks.

Adding a CSR User

To add a new CSR User

1. In the workspace tree, click **Administration > CSR Users**. (The New CSR page can also be accessed from the shortcut menu on any CSR option, such as CSR User Lockouts.)
2. When the CSR Users workspace appears, right-click anywhere in the list and choose **New CSR** to display the New CSR page.
3. In the New CSR page, complete the information in the General tab.

   Note: Login ID and Password are required values, and the password must adhere to the CSR Password Policy displayed on the tab.

4. Click **Save**.
5. Switch to the Contact Information tab and enter values in the fields provided.
6. Click **Save And Close**.

Editing a CSR User

To edit a CSR User

1. In the workspace tree, click **Administration > CSR Users**.
2. In the CSR Users workspace, select the CSR User record you want to edit, right-click and select **Edit CSR User**.
3. In the CSR page, make the necessary changes to the CSR record.
4. In the toolbar, click **Save**.

Assigning CSR Users to CSR Roles

To assign a CSR User to a CSR Role

1. In the workspace tree, click **Administration > CSR Users**.
2. In the CSR Users workspace, locate and double-click the CSR User record you want to assign to a CSR Role.
3. In the **General** tab, select the **Role** from the drop-down list.
4. In the toolbar, click **Save.**

Changing the Admin password

Admin password refers to the password that a CSR User uses to log into Q2central. If you search for and select a CSR User record on the CSR User page, you can right-click to access a shortcut menu that includes a **Change Admin Password** option.

Note the following details about changing a CSR User password:

- After you change the password, you must provide it directly to the CSR; no automated message is sent.
- The Logon Status for the CSR User must be set to *Normal*, as displayed on the General tab of the CSR page.

To change the Admin (CSR User's) password

1. In the workspace tree, click **Administration > CSR Users**.
2. In the CSR Users list, select the CSR User row, right-click and select **Change Admin Password**.
3. On the Change Password page, type the new password twice and click **OK**.
4. Click **OK** on the Change Password confirmation page.

Enrolling CSR Users in Secure Messaging groups

As described in "Configuring Secure Messaging" on page 298, a Secure Messaging group is a set of FI staff who receive messages sent by online banking end users. You can control the CSR Users that have access to different types of secure messages in the CSR User list, as described in this section.

Note: To manage Secure Messaging for CSR Users, you must be assigned a CSR Role with the *ADMINISTRATION: Message Group Members* right enabled.

To enroll a CSR User in a Secure Messaging group

1. In the workspace tree, click **Administration > CSR Users**.
2. In the CSR Users workspace, locate the CSR User record, right-click and select **Edit CSR User**.
3. In the Message Groups tab, click in the **Enrolled** column to enroll that CSR User in the Secure Messaging group.

Deleting a CSR User

You can delete a CSR User if you are assigned to a CSR Role that has the *ADMINISTRATION: Manage CSR Users* right enabled.

Tip: For security purposes, be sure to delete CSR User records for people that are no longer employed at the FI.

To delete a CSR User

1. In the workspace tree, click **Administration > CSR Users**.
2. In the CSR Users list, right-click the CSR User record and click **Delete CSR**.
3. Click **Yes** on the Confirm Deletion window that appears.

Note: Details about the CSR User's actions remain in system history with the original login ID. However, the login ID is disabled and a delete date is added to the CSR User record.

CHAPTER 3: CSR NOTIFICATIONS

Monitor the activities within Q2centraland online banking using CSR Notifications. This feature provides up-to-the-minute alerts of events that occur in Q2 applications.

The Home page that appears when you first log into Q2central is another way to track tasks that need to be performed.

This chapter includes the following sections:

- "CSR Notifications overview" on page 33
- "CSR Notifications reference" on page 38
- "CSR Notification tasks" on page 42

CSR Notifications overview

The Manage CSR Notifications page lets FI staff add, edit, or delete notifications for almost any auditable event in the system (that is, any event that results in a change to the database). Notifications are sent to the email address provided in this feature and are not necessarily the same as the address maintained on the Contact Information tab of the CSR record. This allows you to set up notifications for email alias groups.

CSR Notifications may be set up for events that need to be processed in a timely way, such as domestic and international wires. Additionally, setting up notifications for failed attempts to authorize transactions can help with balancing accounts at day's end.



Tip: It may not prove worthwhile to set up a notification for some audit events that are routine activities.

The Q2central Home page is another way that CSRs can see tasks that need to be performed. It includes several widgets—graphic representations of data that change dynamically—that provide shortcuts to different pages, such as the New Messaging and Locked Logins pages.

Recommended CSR Notifications

The following list of CSR Notifications may prove useful for your FI. Because each FI has unique needs, we suggest that you review this list to determine if these CSR Notifications are suitable for your FI before enabling them.

Note: This list is provided for reference only. Based on your FI's specific needs, you may decide to enable additional CSR Notifications.

API category

Notification	Trigger event
Create Micro Deposit	When an end user adds an external account in online banking, a micro deposit is sent to validate the external account. To be notified immediately when this process begins, enable this notification.

Authentication category

Notification	Trigger event
Login Risk Fraud Analytics/Wedge Call Failed	One or more transactions were not processed in time by Q2 Sentinel (formerly called *Risk and Fraud Analytics*) so they were placed in the Draft Transactions folder. In the Q2platform, the *Wedge* provides a connection for services such as Bill Pay, as well as custom forms created for an FI.
Max Access Code Failure Per Day Threshold Exceeded	A secure access code (SAC) exceeds the maximum number of SAC failures allowed per calendar day; the default value is 100. This notification is useful for security monitoring.

CSR Administration category

Notification	Trigger event
Add an administrator	A new CSR User is created in Q2central.
Delete an administrator	A CSR User is deleted in Q2central.
Delete a user	A CSR User deletes an online banking User in Q2central.
Delete a user logon	A CSR User deletes a login ID in Q2central.
Delete an online user through Q2online (self service)	A Business or Corporate Banking end user with rights to the Manage Users feature deletes a User in online banking.
Service Charge Calculation Files Generated	The Process Monthly Fees action is executed. This notification may be useful to inform management that the process occurred for the current month.
Create a Csr Assist Login	A CSR User attempts to use the CSR Assist functionality in Q2central. This notification is useful for system administrators or auditors.
Transaction Limit Exceeded	A Generated Transaction limit is exceeded. This can occur when limits such as amount per day, amount per transaction, and transactions per day are exceeded. An FI can use this data to take a proactive approach to customer service.

Customer category

Notification	Trigger event
Activate User	The Activate Users option is selected for a User record that was previously disabled.
Disable All Users	The Disable All Users option is selected for a Customer record.

Group category

Notification	Trigger event
Create a new Group	A Group is created in Q2central. This notification may be useful for a system administrator.
Delete a Group	A Group is deleted in Q2central.
Set a Group	A CSR User changes Group attributes, or the Group assigned to a Customer in Q2central.

Marketing Message category

Notification	Trigger event
Delete Campaign	A CSR deletes a marketing campaign in Q2central. This notification may be useful for management.
Update Campaign	A CSR User modifies a marketing campaign in Q2central.

Messaging category

Notification	Trigger Event
Send broadcast message	A message is distributed to all online banking Customers.
Send a secure message to all users in a Group	A CSR sends a secure message to a Group.

Roles category

Notification	Trigger event
Update administrator role properties	Rights are changed on the CSR Role page.

System Administration category

Notification	Trigger event
Create Service Charge Plan	A CSR User creates a Fee Plan. This notification may be useful for managers or a system administrator.
Delete Service Charge Plan	A CSR User deletes a Fee Plan.
Set Transaction Holidays	A CSR User updates the Bank Holidays in Q2central.
Update a password policy	A CSR User updates the Password Policy for end users in Q2central.
Update an admin password policy	FI staff updates the Password Policy for CSRs logging into Q2central.
Update hours	A CSR User modifies a Bank Holiday in Q2central.
Update Service Charge Plan	A CSR User updates an existing Fee Plan.
Update Service Charge Plan Customer List	A CSR User updates the Customers linked to an existing Fee Plan.

Transactions category

Notification	Trigger event
Authorize Domestic Wire	An end user approves a domestic wire. This notification is useful for FI staff that process international wires.
Authorize International Wire	An end user approves an international wire. This notification is useful for FI staff that process international wires.
Authorize Stop Payment	An end user approves a Stop Payment request. This time-sensitive notification can be useful if an FI is not configured for real-time Stop Payment requests.
Decide Suspect Transaction	A CSR either accepts or declines a suspect transaction processed by Sentinel.

Transactions category (cont'd)

Notification	Trigger event
Risk Fraud Analytics Failure	Sentinel cannot process a transaction due to bad data or a network issue.
Risk Fraud Analytics Suspect	Sentinel scoring determines that a transaction is suspicious. If Sentinel is in Active Mode, the transaction is placed on hold.
Risk Fraud Analytics Suspect with Access Code	Sentinel scoring determines that a transaction performed using a SAC is suspicious.
Risk Fraud Analytics Suspect with Token	Sentinel scoring determines that a transaction that included a Symantec VIP token code is suspicious.
Risk Fraud Analytics Wedge Call Failed	Sentinel did not have sufficient information to score one or more transactions due to a wedge call failure that created anomalous server activity. Sentinel will place the transaction(s) in the Other Transactions state. This is a timing issue; the next attempt to approve the transaction is usually successful without any additional effort.

CSR Notifications reference

This section describes several ways that FI staff can ensure that CSRs are notified about outstanding tasks:

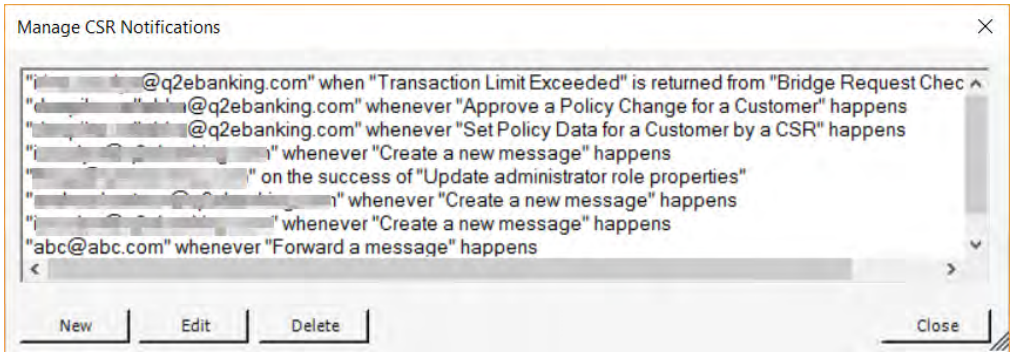
- Use the Manage CSR Notifications page, accessible via the **Administration > CSR Notifications** option in the workspace tree, to manage system-generated notifications for CSRs.
- Configure the Q2central Home page that shows CSRs how they are tracking collectively in several administrative areas.

Manage CSR Notifications page

You can use the Manage CSR Notifications page to manage notifications that can be sent to FI staff for almost any audit event. For example, the system can generate an automated message whenever a Corporate Banking Customer changes a Company Policy.

Notifications can be sent to the same email address on the Contact Information tab of a CSR User's record, or you can direct notifications to an alias email address shared by multiple CSRs.

Manage CSR Notifications page



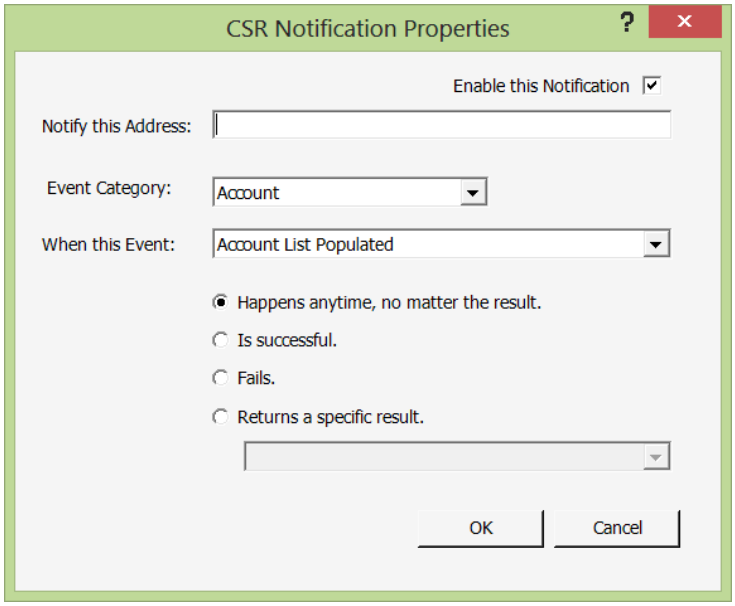
Manage CSR Notifications options

Option	Description
CSR Notification Summary	The summary of the notification in the structure of the recipient email, along with the event.
New	Opens the CSR Notification Properties page where you can create a new CSR Notification.
Edit	Opens the CSR Notification Properties page, where you can edit an existing CSR Notification.
Delete	Permanently removes a CSR Notification from the system.
Close	Closes the page and cancels the action.

CSR Notification Properties page

Use the CSR Notification Properties page to set up an automated notification to be sent to you when the event you specify occurs.

CSR Notification Properties page



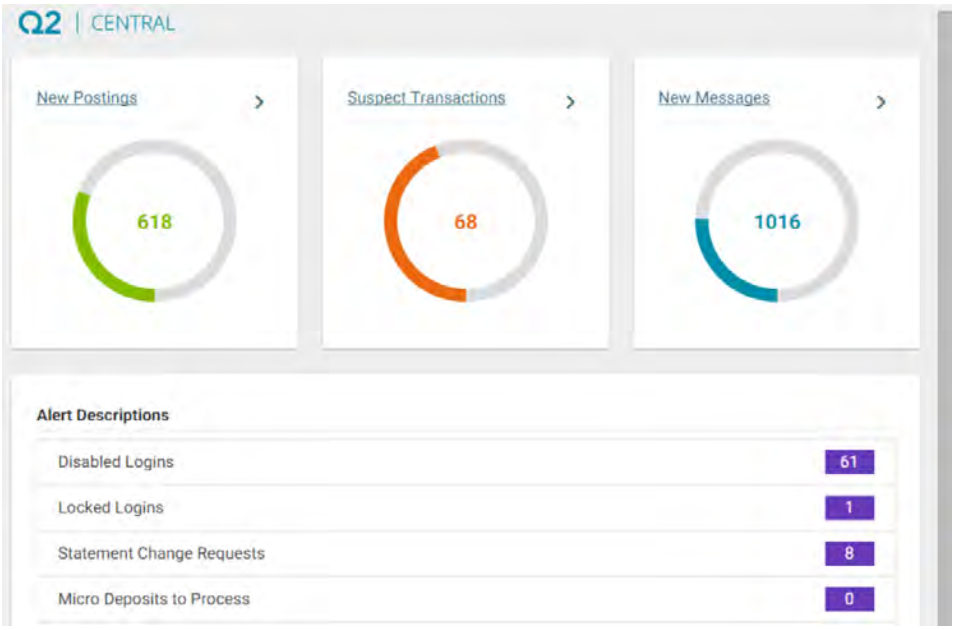
CSR Notification Properties page options

Option	Description
Enable this Notification	Activates the notification.
Notify this Address	The CSR email address.
Event Category	The category of the event that triggers the CSR Notification.
When this Event	The event that triggers the CSR Notification.
Outcome	The event that is the final trigger to send the CSR Notification. Options include: • Happens anytime, no matter the result. • Is successful. • Fails. • Returns a specific result.

Home page

The Home page is the first page that appears after you log into Q2central. It includes several widgets—graphic representations of data that change dynamically—so CSRs can quickly see which tasks are outstanding. This visual display shows CSRs, at a glance, how they are tracking collectively in several administrative areas.

Home page



Widgets on the Home page are also hyperlinks to other areas of Q2central. Click a widget on the Home page to quickly access the Q2central page where a task is performed. For example, click the New Postings widget to access the To Process page and display wire transactions.

Note: Only widgets that you have permission to use appear. For example, if the CSR Role to which you are assigned does not have rights to manage logins, the Locked Logins widget will not appear on the Home page.

FI staff with administrative privileges can customize the Home page. See "Configuring widgets on the Home page" on page 42.

CSR Notification tasks

This section includes some of the most commonly used tasks for CSR Notifications, including:

- "Configuring widgets on the Home page" on page 42
- "Adding a CSR Notification" on page 43
- "Editing a CSR Notification" on page 44
- "Deleting a CSR Notification" on page 45

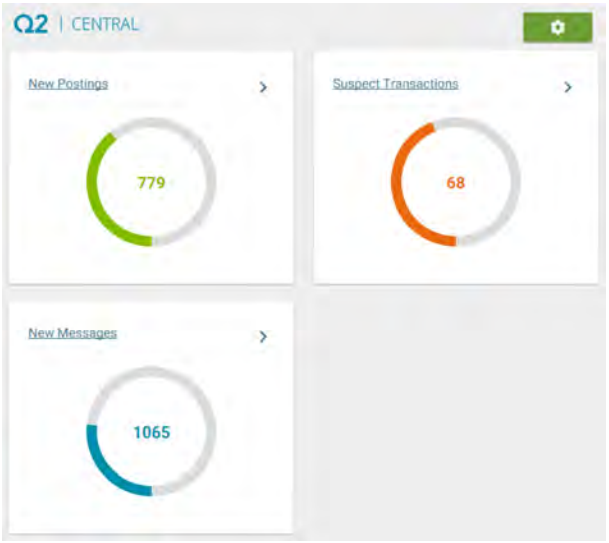
For a full list of CSR Notifications, see the *Q2central Reference Lists* document.

Configuring widgets on the Home page

For each widget on the Home page, FI staff with administrative privileges in Q2central can set the number that will serve as the total against which CSRs measure their progress. For example, one FI may consider 15 suspect transactions to be a high number that warrants immediate attention, while another FI may consider 30 to be a critical threshold.

When a widget's circle reaches the total, the number continues incrementing and the circle remains complete until the number of items drops below the critical mark.

Home page



Note: CSRs only see widgets for tasks that they can perform, based on their CSR Role. For example, if a CSR Role does include rights to manage logins, CSRs assigned to that role will not see the Locked Logins widget.

To configure widgets on the Home page

1. Click the Configure icon () at the top of the Home page.

   Note: The Configure icon only appears if your CSR Role has the *ADMINISTRATION: Change Global Splashboard Settings* right enabled.

2. Enter a **Display Maximum** between 0 and 9,999 for each circular graph.
3. Click **Save**.

Adding a CSR Notification

Add CSR Notifications to notify your FI staff of system events as they occur.

To add a CSR Notification

1. In the workspace tree, click **Administration > CSR Notifications**. The Manage CSR Notifications page appears.
2. In the Manage CSR Notifications page, click **New**.
   The CSR Notification Properties page appears.
3. In the **CSR Notification Properties** page, complete the following:
   a. Click the **Enable this Notification** check box.
   b. In the **Notify this Address** field, enter a valid email address.

      Note: This may not be the same email address on the Contact Information tab of the CSR record.

      Tip: Separate multiple email addresses with a semi-colon.

   c. Select an **Event Category**.
   d. In the **When this Event** drop-down list, select the event associated with the selected Event Category.



Note: For a complete list of available events, see the *Q2central Reference Lists* document.

e. Select one of the following outcomes:
   - **Happens anytime, no matter the result**
   - **Is successful**
   - **Fails**
   - **Returns a specific result**

4. Click **OK**.

Editing a CSR Notification

To edit a CSR Notification

1. In the workspace tree, click **Administration > CSR Notifications**.
2. When the Manage CSR Notifications page appears, locate and select the notification you want to edit.
3. Click **Edit** or double-click the notification.
4. On the CSR Notification Properties page, edit the fields, as necessary:
   a. In **Notify this Address** field, enter a valid email address.



Note: This is not necessarily the same email address provided on the Contact Information tab of the CSR User record.

   b. Select an **Event Category**.
   c. In the **When this Event** drop-down list, select the event associated with the selected Event Category.



Note: For a complete list of available events, see the *Q2central Reference Lists* document.

   d. Select one of the following outcomes:
      - **Happens anytime, no matter the result**
      - **Is successful**
      - **Fails**
      - **Returns a specific result**



Note: For most events, "Happens anytime, no matter the result" is suitable.

5. Click the **Enable this Notification** check box and click **OK**.

Deleting a CSR Notification

To delete a CSR Notification

1. In the workspace tree, click **Administration > CSR Notifications**.
   The Manage CSR Notifications page displays all current notifications, listed alphabetically by the email address of the FI staff being notified.
2. Locate and select the notification.
3. Click **Delete**.
4. Confirm the deletion by clicking **Yes**, and then click **Close**.

CHAPTER 4: GROUP ACCESS MAPPING

The optional Group Access Mapping feature enables FI staff to control how much access CSRs have to Customer, User, and Login ID records that belong to specific Groups.

This chapter includes the following sections:

- "Group Access Mapping overview" on page 46
- "Group Access Mapping reference" on page 49
- "Group Access Mapping tasks" on page 51

Group Access Mapping overview

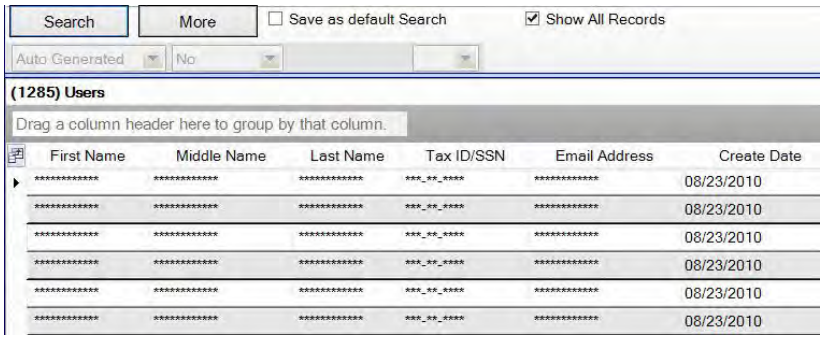
You can use Group Access Mapping to define the level of access that CSRs have to records, based on the parent Group to which records belong.

This feature provides the following benefits:

- Enables an FI to establish and manage CSR Teams with varying levels of access to Customer, User, and Login ID records to meet your FI's diverse data needs.
- Shields sensitive data such as accounts for FI board members.

Some CSRs can have full access to a Group's child records and some can have view-only access, depending on the CSR Team to which they belong. CSRs on a team with minimal rights cannot see identifying details about a Group's child records because details will be masked—letters and numbers appear as symbols, as shown in the following illustration.

Masked search results (example)



Tip: If a CSR needs assistance with a masked record, the CSR can right-click a record to display CSRs with full access. See "Using the Show CSRs with Full Rights option" on page 55.

Note: Even if a record is masked, it will appear in relevant search results, as well as Q2central reports.

Understanding Group Access Mapping rights

With Group Access Mapping, you can create CSR Teams with different levels of access to records that belong to different Groups. Those rights extend through each Group's child records (Customers, Users, and Logins), allowing or restricting CSRs from viewing and/or changing data depending on the CSR Team to which they belong.

The following table outlines available rights for Group Access Mapping and the access that each right provides:

Group Access Mapping rights

Right	View record details	Edit records	Reset passwords	Unlock Login IDs	Use CSR Assist
Full	Yes	Yes	Yes	Yes	Yes
View + Unlock	Yes	No	Yes	Yes	No
View	Yes	No	No	No	No
Minimal	No	No	No	No	No

Note: If your FI uses the Corporate Banking product, Group Access Mapping will not prevent CSRs whose CSR Role has the *Manage Treasury* right enabled from accessing the Policy Dashboard in edit mode. To block CSRs from editing Customer Policies, make sure their CSR Role has *Manage Treasury* disabled.

CSR Team examples

As you configure Group Access Mapping, you can create CSR Teams with different rights to meet your FI's diverse needs. This section describes two examples of CSR teams:

- View-only mode
- Private-data-by-group mode

View-only mode

A CSR Team with view-only rights to records can be helpful for auditors that need to access records but do not need to change records or see identifying data about Users.

The two levels of View access include:

- **View**: CSRs can view but cannot edit Customer, User, and Login records. This is a good option for visiting auditors.
- **View + Unlock**: CSRs can view Customer, User, and Login records, plus reset passwords and unlock login IDs. This is a good option for CSRs at call centers that only perform low-level tasks such as resetting passwords and unlocking login IDs.

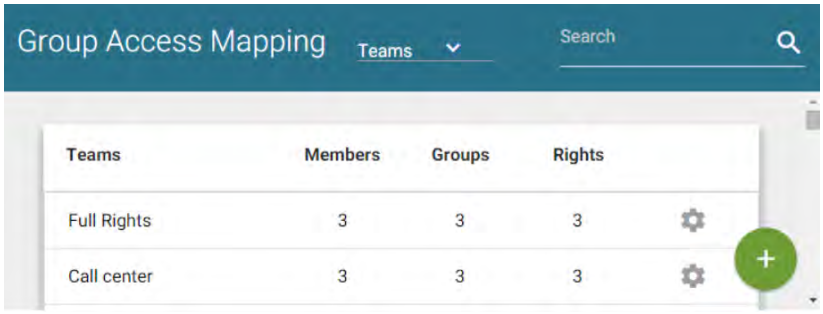
Private-data-by-group mode

You can also create Groups of Customers to which a limited subset of CSRs have full access. This is useful for restricting access to data about coworkers, FI executives, celebrities, high-value Customers, etc. This mode can also be used if certain CSRs are dedicated to a particular business segment or are assigned to specific Customers.

Group Access Mapping reference

This section describes how the Group Access Mapping page changes based on the value selected in the drop-down list at the top of the page.

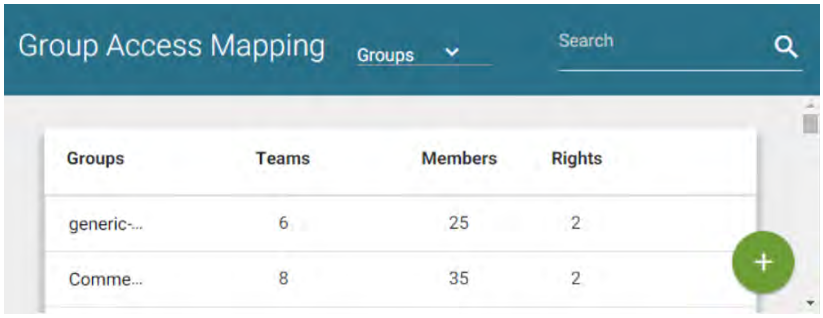
Group Access Mapping page (Teams)



If *Teams* is selected, data on the page appears as follows:

- The Teams column lists all existing CSR Teams.
- The Members column shows how many CSRs are part of the team. If a team has only one CSR, the CSR login ID appears.
- The Groups column shows how many Groups for which a team can access records. If a team can access only one Group's records, the Group name appears.
- The Rights column shows how many distinct rights exist for the Group. Click a value to display a list of rights and the Groups that have each right. If only one right is held for a Group, that right appears.
- Click the gear icon ( ) to edit CSRs and/or Groups for a team.
- Click the Add icon ( ) to create a new CSR Team.

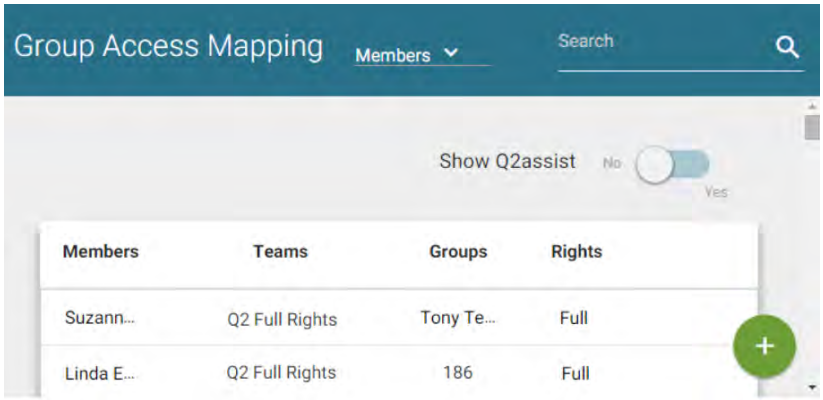
Group Access Mapping page (Groups)



If *Groups* is selected, data appears as follows:

- The Groups column displays all Groups at your FI.
- The Teams column shows how many teams have enhanced rights (that is, either View, View + Unlock, or Full) to the Group; hover over the number to display a list of teams. If no teams have rights for a Group, a red triangle appears. If only one team has enhanced rights, the team name appears.
- The Members column shows how many CSRs have rights to records in the Group; hover over a number to display a list of teams. If no CSRs have rights to a Group, a red triangle appears. If only one CSR has rights, that CSR login ID appears.
- The Rights column shows how many distinct rights exist for a Group, with full rights listed first; hover over a number to display all rights. If no team has rights for a Group, a 0 (zero) appears. If only one distinct right is held, the right appears.

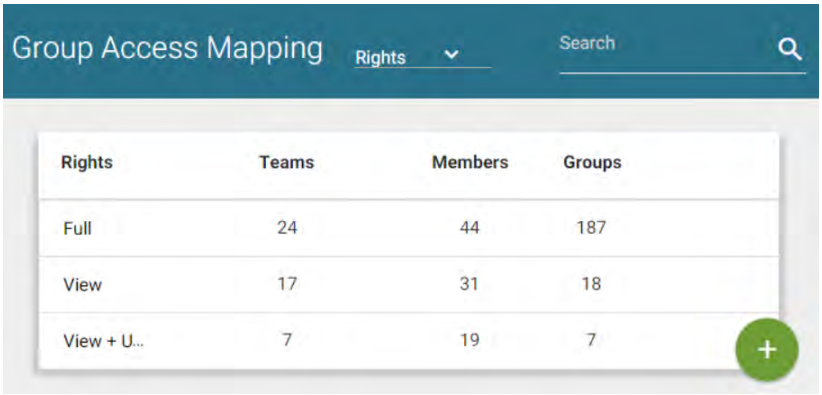
Group Access Mapping page (Members)



If *Members* is selected, data appears as follows:

- The Members column lists CSRs that belong to a CSR Team.
- The Team column shows the team to which a CSR belongs.
- The Groups column shows the number of Groups to which a CSR has access. If a CSR can access records in only one Group, the Group name appears.
- The Rights column indicates the type of rights a CSR has in the Groups to which the CSR belongs. If a CSR has multiple types of rights in different Groups, click the value to display Groups and associated rights.

Group Access Mapping page (Rights)



If *Rights* is selected, data appears as follows:

- The Rights column displays a list of available permissions.
- The Teams column shows the number of teams with a right. If only one team has a specific right, the team name appears.
- The Members column lists CSRs with a specific right. If only one CSR has a right, the CSR Login ID appears.
- The Groups column shows the number of Groups with a specific right. If only one Group has a right, the Group name appears.

The following fields also appear on the Group Access Mapping page:

- Enter search criteria and click the Search icon to find a CSR Team, Group, Member, or Right, depending on the value selected at the top of the page.
- Click the Add icon to create a CSR Team. Type the name in the window that appears and click **Save**.

Group Access Mapping tasks

This section includes some of the most commonly-used tasks for Group Access Mapping. It includes the following topics:

- "Preparing for Group Access Mapping" on page 52
- "Adding a CSR Team" on page 54
- "Editing a CSR Team" on page 54
- "Deleting a CSR Team" on page 55
- "Using the Show CSRs with Full Rights option" on page 55

Preparing for Group Access Mapping

Review this section before setting up Group Access Mapping by adjusting CSR Roles and then creating and assigning rights to CSR Teams. It contains tips and important details that will prevent loss of CSR access to records.

Developing a CSR Team strategy

We recommend that you create a strategy for CSR Teams before enabling Group Access Mapping. Consider how many CSR Teams you need, the access each CSR Team should have, and which CSRs to assign to each CSR Team.



Note: Each CSR User can have one CSR Role and belong to only one CSR Team.

For example, you can assign CSRs at a call center to a CSR Team with View + Unlock rights if their job duties include low-level tasks such as resetting passwords and unlocking Login IDs. Another group of trusted CSRs can be added to a team with Full rights for a Group that includes accounts for FI board members.

Upgrading to Group Access Mapping

This section describes how to set up Group Access Mapping. Preferably, this will occur over a weekend or after hours when less people use Q2central.



Caution: Enabling Group Access Mapping will render all records masked until CSR Teams are set up. We recommend that you start by creating a single CSR Team with Full rights to all Groups to match current functionality and add all CSRs to that team. As you create specialized teams, you can gradually move CSRs to those teams.

The following steps are intended for FI staff that belong to a CSR Role with administrative rights, such as CSR-L5. After Q2 updates the *EnableGroupAccessMapping* system property in the database, all CSRs will have minimal access to Customer, User, and Login records across all Groups until they are assigned to a CSR Team with enhanced rights.

To set up Group Access Mapping

1. Click **Administration > CSR Roles** and adjust the CSR Role to which you belong by enabling the *ADMINISTRATION: Manage teams in Group Access Mapping* right on the CSR Role > General tab. See "Editing a CSR Role" on page 21.
2. Log out and then log back into Q2central to refresh the rights associated with your CSR Role.
3. Click **Administration > Group Access Mapping** to access the Group Mapping page.
4. Create a single CSR Team with Full rights to all Groups that includes yourself and other trusted FI staff, such as supervisors. (See "Adding a CSR Team" on page 54.) This will ensure that several CSRs have full rights to all records, across all Groups.

   Caution: Limit membership in the CSR Team that has rights to configure Group Access Mapping to prevent unauthorized staff from changing their own access.

5. Add more CSR Teams, as necessary. For example, add an auditor team that includes View rights, and a team for call center CSRs that includes View + Unlock rights. See "CSR Team examples" on page 48.

   Tip: Another option is to provide Full access to all CSRs when Group Access Mapping is first enabled, and then add CSR teams with more restricted access later.

6. Access Customer, User, and Login records to verify that you, as a CSR User with full access to all Group records, can see all record details.
7. Set up a test CSR User or ask a CSR with minimal rights to access records in a Group for which records should appear masked to ensure that Group Access Mapping is active.
8. Notify CSRs that Group Access Mapping is enabled and CSR Teams with specific rights to different Group records exist, so some records may appear masked.

   Tip: Let CSRs know that if they need assistance with a masked record, they can right-click the record and select **Show CSRs with Full Rights**.

Adding a CSR Team

Note: CSR Users and Groups must exist prior to linking them to a CSR Team. You cannot create them on the Group Access Mapping page. Also, each CSR can belong to only one CSR Team.

To add a CSR Team

1. In the workspace tree, click **Administration > Group Access Mapping**.
2. Select *Teams* in the drop-down listbox at the top of the Group Access Mapping page.
3. Click the Add icon ( ).
4. In the Add Team window, type a **Team Name** and click **Save**.
5. To add CSRs to a team:
   a. Click the Add Member icon ( ).
   b. (Optional) In the dialog box that appears, slide the **Show Q2assist** option to *Yes* to display CSRs with access to Q2assist.
   c. Select the check box next to each CSR to add to the team.
   d. Click **Done**.
6. To provide the CSR Team with access to records in one or more Groups:
   a. Click the Add Member icon ( ).
   b. In the window that appears, select the level of rights that you want the CSR Team to have for each Group.
   c. Click **Done**.
7. Click the Save icon ( ).

Editing a CSR Team

To edit a CSR Team

1. On the Group Access Mapping page, enter the CSR Team name in the **Search** field.
2. Click the Configure icon ( ) on the row of the CSR Team.
3. In the window that appears, make any necessary changes.
4. Click the Save icon ( ).

Deleting a CSR Team

Caution: When you delete a team, CSRs on the team will have minimal rights to the system. Move CSRs to other teams before deleting a team. Also, make sure that no Groups are left without CSRs that can manage records in them.

To delete a CSR Team

1. On the Group Access Mapping page, enter the CSR Team name in the **Search** field.
2. Click the Configure icon ( ) next to the CSR Team.
3. In the window that appears, click the Delete icon ( ).

Using the Show CSRs with Full Rights option

The Group Access Mapping page can be accessed by FI staff with rights to use that feature, but CSRs without those rights may need to know which colleagues can help an end user whose record is masked.

After selecting a record on a Q2central page, CSRs can right-click and select **Show CSRs with Full Rights** on the shortcut menu to display CSRs with full access to the record.

Note: If you click **Show CSRs with Full Rights** and the message "There are no members with full access" appears, notify the online banking system administrator at your FI. Each Group should have at least one CSR that can access its records.

CHAPTER 5: AUDITING

Q2central Auditing allows you to monitor activities in Q2 applications, as performed by both FI staff and end users. Not only can auditing provide you with important security-related data from within the FI, it also allows you to see trends in end-user behavior.

This chapter includes the following sections for working with the Q2central Auditing feature:

- "Auditing overview" on page 56
- "Auditing reference" on page 56
- "Auditing tasks" on page 57

Auditing overview

The Auditing feature provides information about usage of Q2 products by FI staff and end users. You can also use it to build ad hoc reports.

This feature shows a stream of events that may be searched for troubleshooting purposes. Some events may be appropriate for FI staff alerts; however not all events displayed on the event log require a response by all FI staff. Rather than browsing the list, Q2 suggests you use it for specific searches as described here.

You can set up CSR Notifications for events that need to be processed in a timely way, such as domestic and international wires. Setting up notifications for failed transaction authorization attempts can also help with balancing accounts at the day's end. See "CSR Notifications overview" on page 33.

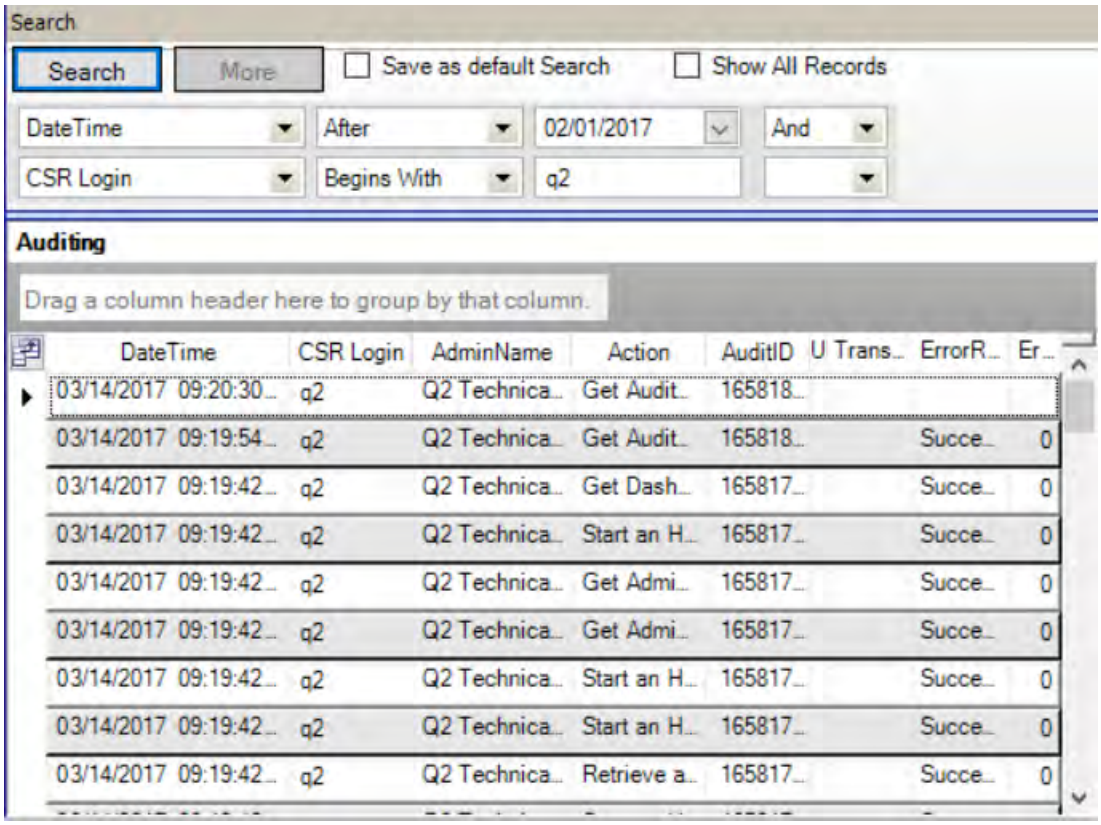
You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

Auditing reference

The Auditing feature, accessible via the **Administration > Auditing** option in the workspace tree, relies on the searching and filtering capabilities of Q2central to gather data to create detailed reports about activity at your FI. Reports can then be exported to an MS Excel file or printed.

Tip: By default, results are sorted using the same filter you used last time. After running queries, you can sort results again to remove unintended filters for next time.

Auditing page



Auditing tasks

This section includes tasks to create some of the common reports you may find helpful when preparing auditing information, including:

- "Retrieving a Customer IP address with action types" on page 58
- "Verifying User creation" on page 58
- "Viewing end-user activities" on page 59
- "Viewing security-related actions by CSRs" on page 59

Retrieving a Customer IP address with action types

This section describes how to retrieve a Customer IP address based on actions that Users linked to the Customer perform in online banking.

To retrieve a Customer IP address with action types

1. In the workspace tree, click **Administration > Auditing.**
2. Click the Field Chooser icon ( ) in the upper-left corner of the Auditing page and select these options:
   - Action
   - ClientAddress
   - CustomerName
   - DateTime
3. Close the Field Chooser.
4. In the toolbar, click **Refresh**.
5. At the top of the Search area, set the first filter box to *Action*.
6. Set the second filter box to *Contains*.
7. Set the third filter box to the type of action you want to display. For example, to view actions that affected end users, type `User`.
8. Click **Search** to display the results.
9. In the search results, click the Action column header to sort the results by action.
10. (Optional) Double-click a record to display the Audited Event Details window.
11. Re-run the report for each action type of interest.

Verifying User creation

Use the Audit Summary Report to generate information about User records created in Q2central.

To verify User creation

1. In the workspace tree, click **Administration > Auditing.**
2. Click the Field Chooser icon ( ) and select these options:
   - Action
   - UserLogin
3. Close the Field Chooser.
4. In the toolbar, click **Refresh**.
5. At the top of the Search area, set the first filter box to *Action*.
6. Set the second filter box to *Begins With*.

7. Set the third filter box to the type the action you want to display. For example, to view all actions related to adding Users, type `Add a User`.
8. Set the filter boxes at the top of the page to *UserLogin* and *Begins With*.
9. In the third box, type the login ID of the User record that was created. If the login ID is not known, search for the Date and Time, if known.
10. Click **Search** to display matching login IDs.
11. (Optional) Double-click a record to display the Audited Event Details window.

Viewing end-user activities

To view activities affecting a specific end user

1. In the workspace tree, click **Administration > Auditing.**
2. Use the Field Chooser to select these options:
   - Action
   - CSRLogin
   - CustomerName
   - DateTime
   - User Login
3. Close the Field Chooser.
4. In the toolbar, click **Refresh**.
5. At the top of the Search area, set the first filter box to *Action*.
6. Set the second filter box to *Contains*.
7. Set the third filter box to the type of action you want to display. For example, to view all actions that affected end users, type `User`.
8. Click **Search** to display the results.
9. Click the Action column header to sort results by action.
10. Re-run the report for each action type of interest.
11. (Optional) Double-click a record to display the Audited Event Details window.

Viewing security-related actions by CSRs

To view security-related actions by CSRs (for audits or daily monitoring)

1. In the workspace tree, click **Administration > Auditing.**
2. In the upper-left corner of the Auditing page, click the Field Chooser icon and select the following:
   - Action
   - CSR Login
   - CustomerName
   - DateTime

3. Close the Field Chooser.
4. In the toolbar, click **Refresh**.
5. At the top of the Search area, set the first filter box to *Action.*
6. Set the second filter box to *Contains*.
7. Set the third filter box to the type of action you want to display. For example, to view all actions that affected end users, type `User`.
8. Click **Search** to display the results.
9. Click the Action column header to sort the results by action.
10. Re-run the report for each action type of interest.
11. (Optional) Double-click a record to display the Audited Event Details window.



Tip: Consider directing FI staff to provide daily backup documentation for all security-related actions.



Note: If a report includes an encrypted character string (for example, 5edc4a9f-2c85...) where a login ID should appear, this indicates that the login occurred via a CSR using CSR Assist.

CHAPTER 6: PASSWORD AND LOGIN POLICIES

You can establish the guidelines that your FI staff and end users must adhere to when accessing Q2central, online banking, and Q2voice. These policies help ensure that the system is accessed only by those that have established their identity and conform to those rules.

This chapter includes the following sections for creating and maintaining password and login policies in Q2central:

- "Password policies overview" on page 61
- "Password Policy reference" on page 61
- "Password Policy tasks" on page 66

Password policies overview

With Q2central, you can establish different password policies for different types of users you have, including Q2central, Q2online, Q2mobility Apps, and Q2voice.

You can also create a login policy for each channel (for example, mobile vs. desktop) that controls the number of failed login attempts allowed before a specified action (for example, a temporary lockout) occurs. For secure access codes (SACs), you can specify the length of SACs, as well as how long a SAC is valid before it expires.

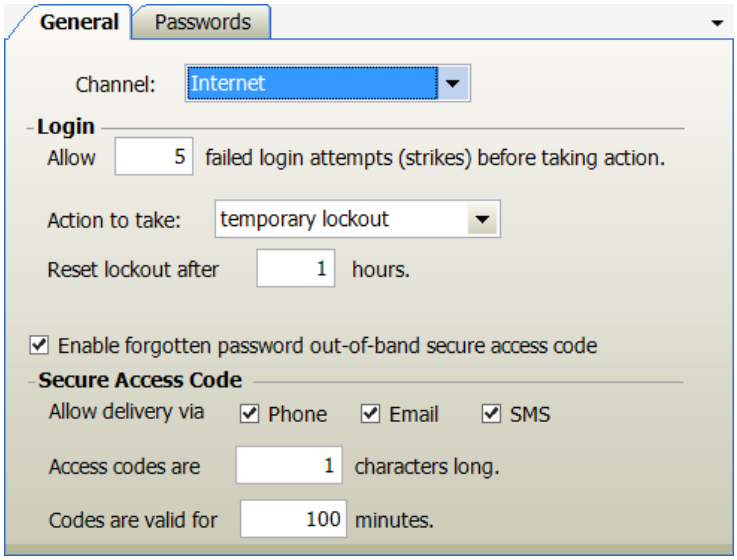
Password Policy reference

The Password Policy page contains a General tab where you can establish login requirements and a Passwords tab where you can specify password requirements.

Password Policy General tab

The Password Policy page allows you to set access security rules for various channels. On the General tab, you establish login requirements.

Password Policy General tab



Password Policy General tab options

Option	Description
Channel	The channel for which you are creating a policy. • Back Office: Q2central • Internet: Q2online and Q2mobility Apps • Voice: Q2voice
Login	
Allow _ login attempts (strikes) before taking action	The number of failed login attempts allowed before taking the specified action.
Action to take	The outcome applied to a user's login record if the number of failed login attempts is exceeded. • *Temporary lockout*: A user can attempt to log in again with the same credentials after a certain time period elapses • *Disable login*: A user cannot log in without FI assistance

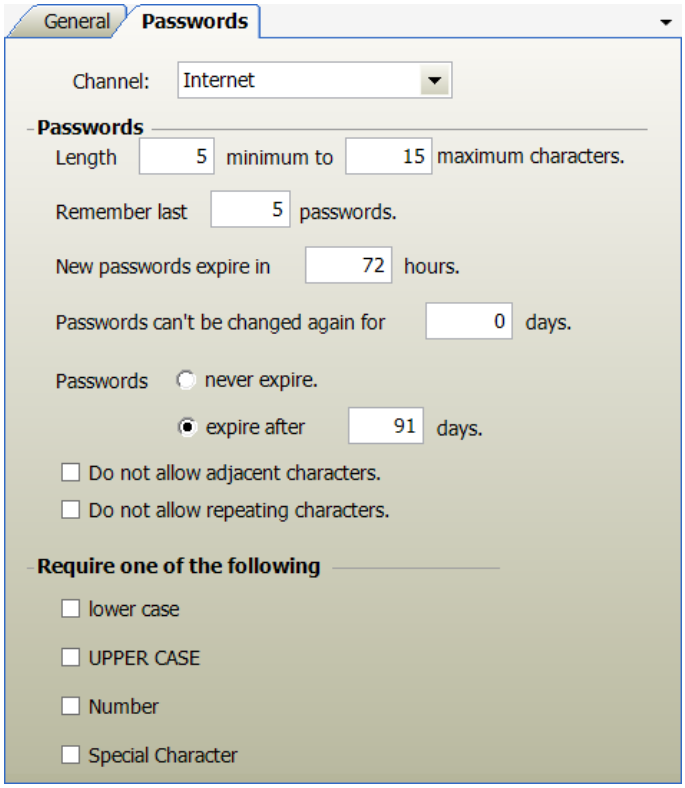
Password Policy General tab options (cont'd)

Option	Description
Reset lockout after _ hours.	The number of hours that must pass before the account lockout is reset. **Note:** This only applies if *Temporary lockout* was selected as the action to take.
Enable forgotten password out-of-band secure access code	Allows online banking end users to request automatic generation of new passwords by clicking **Forgot My Password** on the Login page.
Secure access code	
Allow delivery via • Phone • Email • SMS	The method for delivering the secure access code (SAC) to the end user.
Access codes are _ characters long.	The number of characters in the SAC.
Codes are valid for _ minutes	The number of minutes after which a SAC will be considered invalid.

Password Policy Passwords tab

The Password Policy page allows you to set access security rules for various channels. On the Passwords tab, you establish password requirements.

Password Policy Passwords tab



Password Policy Password tab options

Option	Description
Channel	The channel for which you are creating a policy. • Back Office: Q2central • Internet: Q2online and Q2mobility Apps • Voice: Q2voice
Passwords	
Length _ minimum	The minimum number of characters allowed for the password.

Password Policy Password tab options (cont'd)

Option	Description
to _ maximum characters.	The maximum number of characters allowed for the password, up to 99 characters.
Remember last _ passwords.	The number of unique passwords an end user must create without reusing previous passwords. For example, if value is5, and an end user's favorite password is "Password1", the end user must provide five new passwords before the system accepts "Password1" again for this end user.
New passwords expire in _ hours	The number of hours that can elapse after FI staff provide a login without the end user needing to log in. **Tip:** Allow extra time when users first start using Q2 applications to avoid extra support calls.
Passwords can't be changed again for_ days.	The number of days an end user must wait before requesting a new password. This discourages end users from quickly cycling through the number of passwords in the **Remember last** box in an attempt to regain an old password.
Passwords never expire after _ days.	Options for selecting passwords to never expire, or that expire after a set number of days. This includes setting the number of days that pass before the password expires. **Note:** When configuring Groups and Users, the *Authentication: Never expire end user passwords* setting on the Group and Features tab can override this setting.
Do not allow adjacent characters	Prevents end users from selecting passwords that use characters that are next to each other on the keyboard, such as "asdf" or "1234".

Password Policy Password tab options (cont'd)

Option	Description
Do not allow repeating characters	Prevents end users from selecting passwords with more than one occurrence of the same character, such as "5555" or "yellow".
Require one of the following	
• Lower case • Upper case • Number • Special character (for example, `~!@#$%^&*()_+-={}|[]:";'<>?,./\)	The requirements for the password.

Password Policy tasks

Setting up password policies is a two-step process. First, the login policy is established and then the password requirements are created.

This section includes two of the most common tasks for working with Password Policies, including:

- "Adding a login policy for a channel" on page 67
- "Adding a password policy for a channel" on page 68

Adding a login policy for a channel

To add a login policy for a channel

1. In the workspace tree, click **Administration > Password Policy**.
2. On the Password Policy page, complete the fields on the General tab.
    a. Select the **Channel** for which you are adding a policy.
    b. In **Allow**, enter the number of failed login attempts allowed.
    c. In **Action to take**, choose the outcome if the number of failed login attempts is exceeded. Options are:
        - *Temporary lockout*: The User can log in again with the same credentials after a certain time period elapses
        - *Disable login*: The User cannot log in without FI assistance
    d. For temporary lockouts, enter the number of hours to wait before resetting the lockout. Users remain locked out until they attempt to log in again. If Users can log in on the first attempt, their login status returns to normal. If they do not enter a valid password after one attempt (regardless of the amount of failed login attempts specified in the policy), they remain locked out for the specified time period again, and the last-failed date is updated.
    e. Select **Enable forgotten password out-of-band secure access code** if your FI allows Users to generate new passwords via the **Forgot My Password** link on the Login page. Then provide the following:
        i. In **Allow delivery via**, select *Phone*, *Email*, and/or *SMS* to select how the secure access code (SAC) is delivered to the end user. Targets are configured on the **Administration > User** page.
        ii. In **Access codes are**, enter the number of characters of each SAC.
        iii. In **Codes are valid for**, enter the number of minutes that can elapse before an unused SAC expires.
    f. Click **Save**.

Adding a password policy for a channel

Note: If you change an existing password policy, the policy only applies to passwords established for new login IDs.

To add a password policy for a channel

1. In the workspace tree, click **Administration > Password Policy**.
2. On the Password Policy **General** tab, complete these fields:
   a. Select the **Channel** for which you are adding a password policy.
   b. In the **Length** fields, enter the minimum and maximum number of characters allowed.
   c. In the **Remember last** field, specify how many unique passwords a user must create without reusing previous passwords.
   d. In the **New passwords expire in** field, enter how many hours can elapse after FI staff provide a password without the user needing to log in.
   e. In the **Passwords can't be changed again for** field, enter the number of days a user must wait before requesting a new password. This discourages users from cycling through the number of unique passwords required to restore an old password.
   f. Select **Passwords never expire** or **Passwords expire after**, and then enter the number of days when passwords will expire.
   g. Select the **Do not allow adjacent characters** check box to block passwords with adjacent keyboard characters , such as "asdf" or "1234".
   h. Select the **Do not allow repeating characters** check box to block passwords with adjacent instances of the same character, such as "5555" or "yellow".
   i. In the **Require one of the following** area, select any combination of:
      - Lower case
      - UPPER CASE
      - Number
      - Special Character (such as `~!@#$%^&*()_+-={}|[]:";'<>?,./\)
   j. Click **Save**.

CHAPTER 7: BANK HOLIDAYS

With Q2central, you can establish dedicated holidays for your financial institution by defining when the processing of selected transaction types will stop and when it will resume.

For example, your FI may decide to allow transactions that do not require processing on a particular day (such as Check Reorders) to continue but halt transactions that are time-sensitive such as ACH and wire transactions. Your FI may also wish to accept Funds Transfers if the core operates in real-time.

This chapter includes the following sections:

- "Bank Holidays overview" on page 69
- "Bank Holidays reference" on page 69
- "Bank Holidays tasks" on page 72

Bank Holidays overview

The Bank Holidays feature in Q2central allows you to specify the days on which each branch of your FI is closed. This prevents scheduling of transaction processing for the transaction types you specify.

End users are also prevented from scheduling effective dates that are impossible based on your calendar. The system determines the next valid default processing date for transactions that require them, and then uses the holiday schedule to determine invalid dates (such as weekends) and cutoff times.

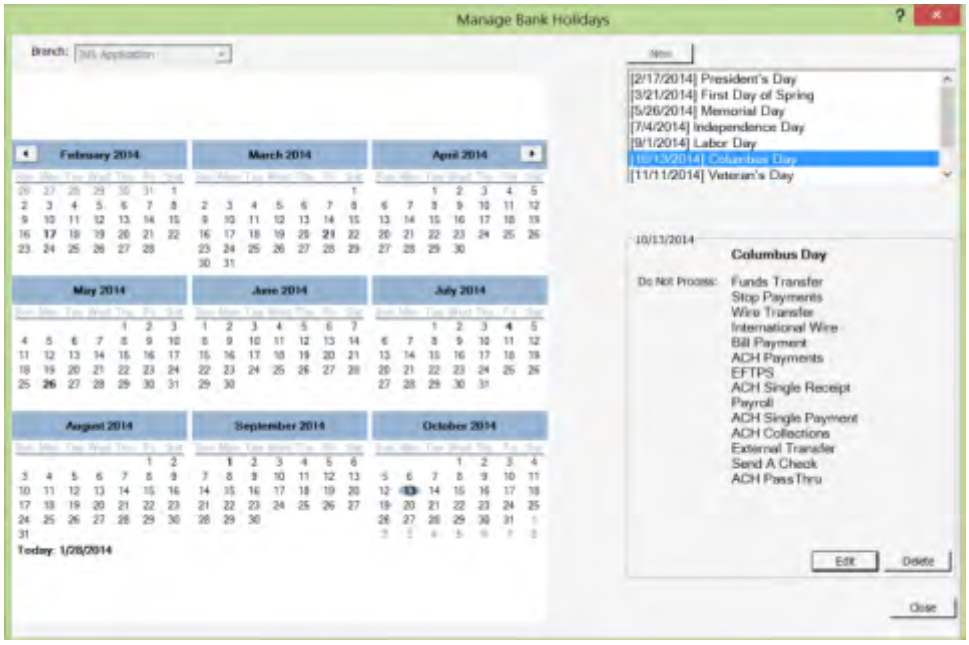
Bank Holidays reference

The Bank Holidays feature consists of two pages: Manage Bank Holidays and Edit Bank Holiday.

Manage Bank Holidays page

The Manage Bank Holidays page provides a high-level view of your FI's designated bank holidays and the transaction types designated for processing.

Manage Bank Holidays page



Manage Bank Holiday page options

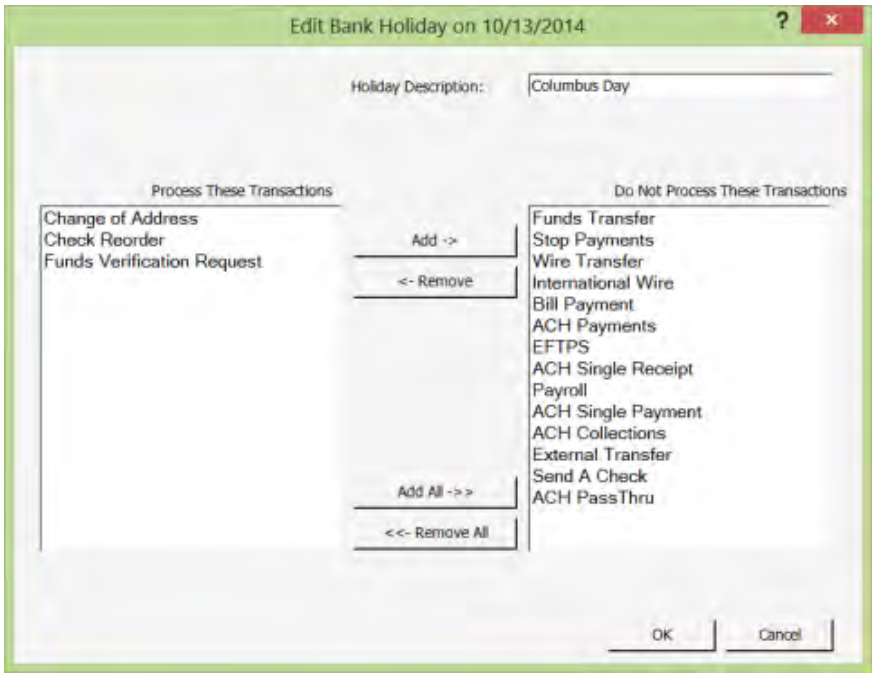
Option	Description
Branch	The branch designation for this set of bank holidays (if applicable).
Calendar	The current calendar.
Scheduled Holidays	Lists the currently-scheduled holidays.
Holiday Details	Provides details about the holiday that is currently selected in the Scheduled Holidays list.
Edit	Click to edit the selected scheduled holiday.
Delete	Click to delete the selected scheduled holiday.

Edit Bank Holiday page

The Edit Bank Holiday page allows you to define which transaction types will and will not be processed on a day your FI designated as a bank holiday.

Note: You cannot change the date of an existing holiday record. To change a date, delete a holiday and add a new one on the correct day.

Edit Bank Holiday page



Edit Bank Holiday page options

Option	Description
Holiday Description	The description for this holiday.
Process These Transactions	The list of transaction types to be processed on the bank holiday.
Add ->	Moves a transaction type from the Process These Transactions list to the Do Not Process These Transactions list.

Edit Bank Holiday page options (cont'd)

Option	Description
<- Remove	Moves a transaction type from the Do Not Process These Transactions list to the Process These Transactions list.
Add All ->>	Moves all transaction types from the Process These Transactions list to the Do Not Process These Transactions list.
<<- Remove All	Moves all transaction types from the Do Not Process These Transactions list to the Process These Transactions list.
Do Not Process These Transactions	The list of transaction types that should not be processed on the scheduled bank holiday.

Bank Holidays tasks

This section contains the most commonly performed tasks when managing Bank Holidays, including:

- "Adding Bank Holidays" on page 72
- "Editing Bank Holidays" on page 73
- "Defining processing for Bank Holidays" on page 74
- "Deleting Bank Holidays" on page 74

Adding Bank Holidays

Add holidays to prevent specific transaction processing when a branch is closed.

To add a bank holiday

1. In the workspace tree, click **Administration > Bank Holidays**.
   The Manage Bank Holidays page displays a calendar and any currently defined bank holidays.
2. In the calendar, select a date and click **New**.
   The Edit Bank Holiday page appears and contains two list boxes: Process These Transactions and Do Not Process These Transactions.
3. Using the **Add ->**, **<- Remove**, **Add All ->>**, and **<<- Remove All** buttons, choose transaction types that should be processed on the bank holiday

and transaction types that should not be processed on the bank holiday.
4. When finished, click **OK**.



Caution: Q2 recommends adding holidays at least one year in advance. Adding holidays on short notice removes processing dates that may already be selected for some transactions. Transactions with invalid processing dates may fail, depending on the transaction type.

Editing Bank Holidays

To edit a bank holiday

1. In the workspace tree, click **Administration > Bank Holidays**.
   The Manage Bank Holidays page appears, listing the currently defined bank holidays in the upper right corner.
2. Click a holiday to display details such as the holiday date, description, and transaction types designated as Do Not Process.
3. With the holiday selected, click **Edit**. The Edit Bank Holiday page appears and contains two list boxes: Process These Transactions and Do Not Process These Transactions.
4. Using the **Add ->**, **<- Remove**, **Add All ->>**, and **<<- Remove All** buttons, choose transaction types that should be processed on the bank holiday and transaction types that should not be processed on the bank holiday.
5. When all selections are made, click **OK**.



Note: You may only edit bank holidays that occur in the future.

Defining processing for Bank Holidays

To define processing for a Bank Holiday

1. In the workspace tree, click **Administration > Bank Holidays**.
   The Manage Bank Holidays page appears, listing the currently defined holidays in the upper right corner.
2. Click a holiday in the list to display its date, description, and all transaction types designated as Do Not Process.
3. With the holiday selected, click **Edit**. The Edit Bank Holiday page display two list boxes: Process These Transactions and Do Not Process These Transactions.
4. Change the Holiday Description, if needed.
5. In the **Process These Transactions** list, verify that the transaction selected can be processed on this day when your FI is closed.
   - To prevent processing of an item listed in the **Process These Transactions** list, select it and click **Add ->** to move it to the **Do Not Process These Transactions** list.
   - To allow processing of an item listed in the Do Not Process These Transactions list, select it and click **<- Remove** to move it to the **Process These Transactions** list.
6. When all selections are made, click **OK**.



Note: Avoid blocking ACH and wire transactions on Bank Holidays, since not processing them can cause problems. Stop Payments and Change of Address typically do not require processing on a particular day, so they can be allowed. Continue accepting funds transfers if your FI core operates in real time.

Deleting Bank Holidays

To delete a Bank Holiday

1. In the workspace tree, click **Administration > Bank Holidays**.
   The Manage Bank Holidays page displays existing holidays.
2. Select the holiday you want to delete.
3. Click **Delete**.
4. When prompted to confirm the deletion, click **Yes**.
5. Click **Close** on the confirmation window that appears.

CHAPTER 8: SECURITY FEATURES IN Q2CENTRAL

Security features are built into the Q2platform and many can be accessed via the Q2central workspace tree. Other features are configured during implementation. Many security features are described throughout this document, as listed here.

Access security

- "CSR Roles overview" on page 19
- "CSR Notifications overview" on page 33
- "Group Access Mapping" on page 46
- "Password Policy General tab" on page 61
- "Security codes" on page 76
- "Challenge questions" on page 81
- "Multi-factor authentication" on page 80
- "Session expiration timers" on page 81
- "User management definitions and relationships" on page 87
- "User Account Management tab" on page 224

Transaction security

- "Authorizing suspect transactions" on page 78
- "Multi-factor authentication" on page 80
- "Q2 Sentinel reports" on page 82
- "User Secure Access tab" on page 222
- "User Symantec VIP Credential tab" on page 221

Transaction security (limits)

- "Group General tab" on page 135
- "Group ACH tab" on page 170
- "Customer Rights tab" on page 196
- "Customer ACH tab" on page 198
- "User Rights tab" on page 229
- "Corporate Banking Policies and Users" on page 93

In addition, the Q2platform offers the ability to require Dual Action for transactions; end-user security and transaction alerts (maintained by end users); disclaimers (maintained outside of Q2central); and secure messaging, among other features. We also maintain partnerships with trusted third-party security vendors including Trusteer and Symantec.

Here are some recommended ways to bolster the security of Q2central:

- Avoid installing Q2central on a device that is allowed to leave the physical premises of your FI. If a CSR User accesses Q2central on a laptop computer, the device should remain on site.
- Implement IP whitelisting so that Q2central is only accessible by FI-controlled, FI-expected IP addresses. Contact Q2 for details.
- Disable logins for CSR Users that are no longer employed at the FI.
- Be conservative about assigning any unnecessary rights to CSR Users.

Security codes

FI staff and end users encounter various security codes in the system, as described in this section, including:

- "Secure access codes" on page 76
- "Symantec VIP token codes" on page 77
- "Authorizing suspect transactions" on page 78
- "Mobile authorization codes" on page 79

Secure access codes

A secure access code (SAC) is a randomly generated code sent to an end user via phone, text, or email. The user may be required to provide a SAC in the following situations:

- At initial login. Depending on how the system is configured, a user may be prompted to enter two successive SACs the first time the user accesses online banking.
- To register a device, if multi-factor authentication (MFA) is in place.
- During subsequent logins, if a browser or device is not registered.
- During transaction approvals, if transactions are of a certain type and amount that require extra authorization.
- If your FI purchased Q2 Patrol, a user may be prompted for a SAC if a potentially fraudulent online session is detected.

To set up SAC targets, use the "User Secure Access tab" on page 222. To require SACs for transactions, set options on the "Customer Rights tab" on page 196 or "User Rights tab" on page 229.

Symantec VIP token codes

The cloud-based Symantec Validation and ID Protection (VIP) service blocks unauthorized access to networks and applications while preventing access by malicious, unauthorized attackers. This extra layer of security can be helpful for end users that are more susceptible to fraud, transact large amounts of money, and/or authorize transactions.

The VIP service generates VIP token codes that are six digits long, accessible via a physical VIP token (also called a *fob*) or the VIP Access mobile app. Each code is valid for one-time use and expires if not utilized within a preset period of time or upon issuance of another code.

Each physical VIP token has a unique serial number, called a *credential ID*, which is usually located on a bar code on the back of the token. In the VIP Access mobile app, the credential ID appears at the top of the app window.

Your FI can determine the transaction types and amount limits for monetary transactions that require VIP token codes. Corporate users with administrative privileges can also configure requirements.

Depending on how the system is configured, a user may need to provide one or two VIP token codes in the following situations:

- To log into online banking for the very first time.
- To log into online banking for all subsequent sessions.
- To register a new browser or device.
- To complete transactions, based on the transaction type and amount involved.
- If a potentially fraudulent online session is detected by Q2 Patrol, if your FI purchased that product

FI staff can also be required to use VIP token codes, as described in the *Q2central Administration Guide*.

Configuring VIP token code requirements for end users

After determining which users can benefit from VIP token codes, FI staff can specify transaction types and limits on the following Q2central pages:

- Group > General tab
- Customer > Rights tab
- User > Rights tab

Corporate users with administrative privileges can also configure VIP token code requirements in Company Policies and User Roles, as described in the *Business and Corporate Banking User Guide*.

CSR VIP token codes

Your FI can add an extra layer of security by requiring CSRs to provide a VIP token code derived from either a physical Symantec VIP token or the VIP Access app when logging into Q2central. To request this functionality, contact your Q2 Relationship Manager (RM) or Q2 Customer Support and ask them to update the *EnableAdminToken* system property in the database.

After CSR VIP token codes are enabled, follow these steps to set up CSRs to use them:

1. On the **Administration > CSR Roles** page, enable the *ADMINISTRATION: Require Token During BackOffice Login* right for each CSR Role that you want to require VIP token codes. See "Editing a CSR Role" on page 21.
2. Create a Credential ID for each CSR User that will use VIP token codes. See "Editing a CSR User" on page 31 and "CSR Users Symantec VIP Credential tab" on page 29.

Refer to the *Q2central Administration Guide* for details.

Note the following details about VIP token codes for CSRs:

- CSRs logging into Q2central for the first time with a temporary password will be prompted to supply two successive VIP token codes.
- CSRs can be locked out if too many unsuccessful attempts to provide a VIP token code occur. See "CSR VIP token codes" on page 78.

Authorizing suspect transactions

If your FI purchased Q2 Sentinel and that product is in Active mode, a security feature called CSR Suspect Transaction Validation can be enabled for suspect transactions that are placed on hold.

If this feature is enabled, CSRs can authorize on-hold suspect transactions on the **Case Management > Case Notes** page only after an end user provides:

- A secure access code (SAC), or
- A VIP token code derived from a physical VIP token or the VIP Access app.

The type of code required depends on the Customer record, as detailed in the following two scenarios.

If a SAC is required to authorize a transaction and a CSR selects the Authorize Transaction check box, the CSR is prompted to:

1. Contact the end user to verify details about the transaction.
2. Select an existing SAC target.
3. Send a new SAC to the end user.
4. Ask the user for the SAC.
5. Enter the SAC.
6. Click **Submit**.

If a token code is required to authorize a transaction and a CSR selects the Authorize Transaction check box, then the CSR is prompted to:

1. Contact the end user to verify details about the transaction.
2. Ask the user to generate a new token code. If this is the user's first time providing a code, two successive codes may be required.
3. Enter the token code(s).
4. Click **Submit**.

In either case, the Reason value on the Case Notes page may automatically default to End User Approval and the transaction status will change to Authorized when a valid code is provided. Otherwise, the transaction remains in the Suspect Transactions queue with an On Hold status.

Mobile authorization codes

A *mobile authorization code* (MAC) is a secure code that users can enter to approve commercial transactions via telephone. Intended for Business and Corporate end users of Q2mobility Apps, mobile authorization must first be enabled by FI staff See "Group Features tab" on page 143 and "Customer Features tab" on page 200.

After the feature is enabled, a user can navigate to **Settings > Mobile Authorization** in online banking to configure the MAC and select the transactions for which it will be used.

A MAC can be used:

- To approve a transaction initiated via a mobile device.
- To approve a transaction when using a mobile device rather than Q2online.

Multi-factor authentication

Multi-factor authentication (MFA) helps your FI to meet audit requirements for out-of-band authentication by delivering a credential in a channel other than the one in which an end user is performing transactions. MFA protects end users and the FI from situations where credentials may be compromised.

If your FI uses MFA, you can require all Users that belong to a specific Group to supply a SAC or VIP token code (collectively known as "security codes") when users are:

- Logging into online banking
- Approving transactions
- Working in a session that has been identified as potentially fraudulent, if your FI uses the Q2 Patrol product.

As described in "Security codes" on page 76, a SAC can be delivered via email, text, or phone message. VIP token codes can be acquired via a physical VIP Security Token or the VIP Access mobile app.

The MFA process used in Q2online and Q2mobility Apps may permit some end users to register their browsers or devices. On a registered browser or device, the system may not prompt end users for a new VIP token code each time they log in, depending on how the system is configured.

Q2 offers the following suggestions regarding MFA:

- Business Banking, Corporate Banking, high-risk, or high-stakes end users should not register their browsers, but be required to always log in with a new VIP token code instead.
- Users who perform ACH or Wire transactions, including External Transfers, should be required to supply a security code each time they log in.
- FIs should not use MFA during Go Live—the period when an online banking system is first being used. After providing a security code the first time they access the system, end users must provide a security code a second time to register their computer. This can confuse end users and increase call volume. Instead, enable MFA after the majority of users have accessed the new system and then use a Marketing Message or a System Notification to notify users about the change.

To learn about MFA-related controls for Groups, see "Group Features tab" on page 143.

Challenge questions

Challenge questions, such as "What town were you born in?" are another authentication method that is provided for backward compatibility with older versions of Q2 products.

Caution: Q2 does not recommend the use of challenge questions because they do not provide out-of-band authentication for logins or transactions. Challenge questions may be used for fraudulent activity if a user's computer or mobile device is compromised.

To set up challenge questions, see "Group Features tab" on page 143 and enable the *Authentication challenge code: Allow one-time access via challenge code* feature.

Note: Consumer Banking Users cannot register a browser or device with a challenge question.

Session expiration timers

Session timeouts that occur within Q2central, Q2assist, Q2online, and Q2mobility Apps are managed through two settings: Session Inactivity and Session Life. These settings are not configured within Q2central but are determined and set at the time of implementation.

The following table describes various session timeout settings.

Session timeout settings

Setting	Description
Session Inactivity	The amount of time that elapses without activity that impacts the server (such as approving a transaction) before an end user is automatically logged out of an application. A message will prompt the end user to click **OK** or risk being logged out. **Note:** Q2central users do not receive a warning or an option to remain logged in. They are logged out automatically.

Session timeout settings (cont'd)

Setting	Description
Session Life	The maximum amount of time that a session is allowed to be active, regardless of activity levels. When this time is reached, the session expires, requiring the end user to log in again. **Note:** If this time expires, the end user is required to provide a login ID and password. This is a new session, and the end user sees the default landing page after successfully logging in.

For example, suppose your FI sets Session Inactivity to 10 minutes and Session Life to 30 minutes. If a user does not perform an action after 5 minutes but before 10 minutes, a message will warn the user to click **OK** or risk being automatically logged out. If the user does not respond after 1 minute, the session is terminated. If 30 minutes elapse without activity, the session ends. The next time the end user logs in, the Account Overview page appears.

The system knows when an end-user session was terminated by any of these methods or by the end user logging out.

If an end user navigates to another site from within an active online banking session, Q2online and Q2mobility Apps do not consider the session terminated. In this case, if the session is still within the session settings, the user may click the browser's Back button and return to the online banking session. If this is an issue with your FI, Q2 recommends that any external link from within the online banking session be created to automatically launch a separate window if the link is clicked.

Q2 Sentinel reports

Q2 Sentinel is a product (formerly called *Risk and Fraud Analytics*), that was designed to meet and exceed compliance standards for detecting and protecting end users and your FI from fraud. Sentinel monitors for suspicious characteristics of transactions that remove funds from your FI; may place them on hold; and gives FI staff the opportunity to verify the transactions' authenticity with end users.

Sentinel incorporates a behavioral classification model built from an end user's activity history. Each end user's profile evolves over time as Sentinel adapts to changing behaviors. Sentinel also applies policy-based classification to some transaction types.

FI staff can use Q2central to view a detailed list of all on-hold suspicious transactions. Q2central also provides a link to a detailed transaction information report for transactions identified as suspect. This report provides an overview of the suspect transaction information with links to detailed graphs showing how the current transaction compares to historical transaction data.

If you have Sentinel installed, the following aspects of Q2central reports are different:

- The custom User Activity Report (if installed) displays Scoring information for each end user in addition to the regular audit items in the report.
- Transaction status lists include On Hold as a status (if your Sentinel implementation is in Active Mode).

End user security controls

It can be helpful for FI staff to understand security features that end users interact with directly, some of which they can configure on their own, such as general alerts for low balances.

Note: The name and location of the following links may vary if your FI asked Q2 to change them during implementation.

End user security controls

Control	Description
Change Password	End users access this by choosing **Security** in the Preferences menu in online banking.
Change Login ID	End users access this by choosing **Security** in the Preferences menu if your FI is configured to allow it.
Update secure delivery information	Appears only after end users register their browser.

End user security controls (cont'd)

Control	Description
Set up security alerts	Security alerts notify end users regarding events in their online profile or accounts, such as changes to password or security options. See "End user alerts overview" on page 345.
Set up general alerts	End users can configure alerts to receive notifications about low balances or when transactions post for amounts outside of designated thresholds. See "End user alerts overview" on page 345.

Chapter 9: Merchant Services for Q2voice

This option is used only by FIs that purchased Merchant Services as a supplemental feature to Q2voice.

To use Merchant Services, local merchants must be set up by your FI as Q2voice Customers, Users and Logins. The merchants log in to Q2voice with their login names and passwords and can enter any account numbers they wish.

You can limit the number of verifications by setting a limit for the Merchant Verification transaction type (if listed) at the Group or Customer level. See the *Q2central Administration Guide* for more information.



Note: Merchant Services is not part of the standard Q2voice offering; it is a separately purchased feature.

Section II - User Management - end user configuration

This section provides detailed information about the features in the User Management menu. These features enable FI staff to manage all aspects of end-user records—Fee Plans, Groups, Customers, Users, and Logins.

Fee Plan management is not part of records management, but is included in the User Management menu because many FIs that use account analysis choose to take fee plans into account when creating Business and Corporate Banking Groups. Fee Plans are applied at a Group level.

Chapter 10: Understanding User Management

This chapter describes the hierarchical nature of relationships between Groups, Customers, Users, and their Logins within the construct of Q2central's User Management feature.



Note: Although many Business Banking concepts regarding user management also apply to the Corporate Banking product, be sure to read "Corporate Banking Policies and Users" on page 93 if your FI uses Corporate Banking. In addition to rights and features, Corporate Banking includes User Roles with varying levels of entitlements, as well as Group Policies, Customer Policies, and Company Policies.

User management definitions and relationships

Q2central's end-user management is based on a tiered model. Most limits you apply to a level affect the levels below it, providing your FI with control and access security. Levels are as follows:

User Management levels

Level	Description
Groups	Groups are FI-determined categories that allow you to organize Users in ways that are meaningful to your business. Groups are where the first layer of rights and limits are assigned. Groups are made up of your Customers.

User Management levels (cont'd)

Level	Description
Customers	Customer records describe the set of Users that are associated with a particular set of accounts. Every Customer record belongs to only one Group record. Customers are established as either *Commercial* or *Business/Corporate*. If *Business/Corporate* is selected, then: • The Customer > General tab will include a Tax ID field. • Online banking functionality may vary. For example, certain transaction types apply only to Business Banking and Corporate Banking that will not appear to Household Users that utilize the Consumer version of online banking.
Users	Users are the records that describe a person. Every User record belongs to exactly one Customer record. Customers, especially in the case of Business and Corporate Banking, often contain multiple Users.
Logins	Logins are the unique identifiers each person uses to access the system. Each Login ID is associated with exactly one User.

Groups

In Q2central, Groups provide the foundation for User Management. Groups are made up of Customers, which are in turn, made up of Users and Login IDs. Rights and limits are designated at each of these levels. This section provides a high-level overview of Groups in regard to User Management.

When you create Groups, consider the following:

- Which features should be available to Customers in the Group?
- What ACH and other transactional limits apply to Customers in the Group?

At a minimum, some FIs choose to create the following Groups based on similar end-user needs:

- Consumer Banking Group
- Business Banking Group
- ACH Business Banking Group
- Corporate Banking Group (if your FI purchased that product)

Group Access Mapping

Group Access Mapping allows an FI to define the level of access that CSRs have to records in Q2central.For example, system administrators can assign CSRs view-only access to records in some or all Groups. This feature is particularly useful to provide view-only access to FI staff that need to view records but do not need to edit records (auditors or executives, for example). To learn more, see "Group Access Mapping" on page 46.

Group rights and limits

When creating Groups, the point is to set highest permissions and feature access at the Group level to minimize the time spent to set up Customers and Users. Rights and limits set at the Group level are *inherited*, or passed down, to all Customers assigned to that Group, and then to Users assigned to those Customers.



Note: For Business and Corporate Banking, there are exceptions to how Group rights and features are inherited at the Customer and User levels. For example, Dual Action can be enabled at the Customer and User level, regardless of the Group setting. There are also exceptions for Business and Corporate Banking features that warrant extra security such as Multi-Wires. See "Feature right exceptions" on page 107.

Customers

Customers are created as either Household or Commercial Customers on the General tab of the Customer window. Commercial users can belong to either Business or Corporate Banking Groups. The Customer Type impacts options that are available to Customers in online banking.

Household Customers are typically Consumer Banking users, and often (although not always) consist of a single user. For example, several members of a family can belong to a single Customer. Commercial Customers typically consist of multiple users that use the Business or Corporate Banking product.

Customer information file (CIFs) or member numbers, commonly used in the banking industry are associated at the Customer level in Q2central. Fee Plans can also be applied to certain Customers.

Customer rights and limits

By default, the rights and limits set on Customers are inherited from the settings in their assigned Group. Permissions and limits may be denied or altered (respectively) at the Customer level.

For most features, Customers cannot have more permissions than were granted at the Group level. There are exceptions to that premise, as described in "Group rights and limits" on page 89.

Users

In Consumer Banking, everyone is an individual end user. The person's User record is almost identical to the Customer record.

User rights and limits

Most permissions and limitations set at the Customer level are inherited by default by all Users in the Customer record. Permission may be further denied at the User level. In general, Users cannot have more permissions than were granted at the Customer level. See "Group rights and limits" on page 89 for exceptions.

Differences between User and Customer records become more apparent when there are multiple Users associated with a commercial Customer. For example, one User may have full access to originate transactions, and another User within the same Customer may have view-only rights to account activity.

Login IDs

If a User's Login ID becomes locked or disabled, that end user is unable to access the system until they gain assistance from the FI.

Secure access code targets are *assigned* at the User level and *delivered* to the Login ID.

Login ID rights and limits

There are no rights or limits assigned to login IDs. Passwords in the system are assigned at the Login ID level.

Examples of Customers in Groups

For Consumer Banking Customers, the Customer record normally describes an individual in charge of his or her personal accounts. This is typically a one-to-one relationship where the Customer record and User record are for the same individual and there are no other Users associated with that Customer. In the case of an individual, the Customer record overlaps almost entirely with the person's User record.

For Business Banking Customers, the Customer record describes the entity that is the company or organization. User records and login IDs for a commercial Customer may belong to the owner, director, or lead staff member in such an organization.

For Corporate Banking Customers, the Customer record describes the company or organization. Generally, Corporate Banking is used by Customers with complex business needs, such as a large number of employees that need varying levels of access to accounts and transactions. User records and login IDs for a Corporate Banking Customer may belong to the finance department or an accounting group.

Consumer Banking Group example

Jane Smith is an individual end user at the FI. Ms. Smith is both the User and the Customer in this example. Her User record has one login ID, jsmith, which is used to access Q2online and Q2mobility Apps. She has one account, checking 101, and her CIF number is 123456789. She has full access (deposit, view, and withdrawal) to that account.

Business Banking Group example

Acme Builders has accounts at the FI that includes one Customer record and has two Users. The owner, Jack Johnson, is a User with two login IDs: jjohnson (used to access Q2online) and 22222 (used to access Q2voice).

The bookkeeper, Dorothy Davis, is another user. She has one login ID, ddavis (used to access Q2online). Both Jack Johnson and Dorothy Davis have full access (deposit, view, and withdrawal) to all of Acme Builders' accounts.

If the FI chooses, a main User (most likely, Jack) can be set up as an administrative User with rights to control or remove access of the other Users.

Corporate Banking Group example

Dupree Enterprises is a company with 200 employees that has accounts at the FI. Dupree Builders is the Customer record with 11 users. Rashad Adams leads the accounting department and has two login IDs: radams (used to access Q2online) and 44444 (used to access Q2voice). Both Rashad and his executive assistant, Joseph Lamas, have full access (deposit, view, and withdraw) to all Dupree Enterprises accounts.

The remaining 9 users include 1 Payables manager, 1 Payables administrative assistant, 2 Payables clerks, 1 Receivables manager, 1 Receivables administrator, 2 Receivables clerks, plus 1 controller. Each has her or his own login ID.

Chapter 11: Corporate Banking Policies and Users

The Corporate Banking product is intended for Customers who have commercial accounts and complex banking needs such as high transaction volumes and a large number of employees. It offers more control over who does what, to which accounts, and when. These extended permissions are known as *entitlements*.

This chapter includes the following sections:

- "Corporate Banking overview" on page 93
- "Corporate Banking Policies" on page 98
- "Corporate Banking User Roles" on page 115

Tip: If your FI does not use Corporate Banking, you can skip this chapter.

Corporate Banking overview

Corporate is for companies with high transaction volumes and a large number of employees that require more complex entitlement structures. Corporate includes features that help you manage entitlements, provide reports for your end users, and validate routing transit numbers (RTN).

Corporate features

Features	Description
Enhanced entitlements	Control entitlements for the Company Policy and User Roles.
Information reporting	Customize, schedule, and print reports in different formats. Standard reports include: • Account Activity Report • ACH Activity Report • Cash Position Report • Company Entitlements Report • Outgoing Wires Report • Transaction Report • User Activity Report

Corporate features (cont'd)

Features	Description
RTN validation	Perform RTN validation (RTN lookup) by entering either an American Banker Association (ABA) routing number or FI name into the Recipient Account Record ABA field and have matching entries returned. This service reduces ABA routing number errors, complies with NACHA requirements for commercially-reasonable screening, and reduces costs associated with returned items.
Multi-Transfer	Includes the ability to create multiple internal funds transfers from one screen and save the set of transfers as a template. End users can select a single processing date or different processing dates for all of the transfers. However, a single Batch ID will be associated to each set of transfers to streamline approval and reconciliation.
Multi-Wire Origination	Includes the ability for end users to execute multiple domestic or international wire transactions from one screen and save the resulting set of wire transactions as a template. End users can select a single or different effective date for all of the transactions; however, a single batch ID will be associated for each wire to streamline approval and reconciliation.
Batch Wire Uploads	Includes the ability to import a comma separated (CSV) file including multiple domestic or international wires, replacing the need to manually key in wires. Uploaded wires will be represented as single transactions in the Activity Center. However, a single batch ID will be associated for each wire to streamline approval and reconciliation. Only files containing the mandatory Fedwire and SWIFT fields will be supported and this service does not include the ability to create a wire outside of the CTR format.
Recipient Upload from Batch Payments	Provides the ability to upload a NACHA file containing recipient information to create new recipient records, as well as update existing recipient records when end users are uploading ACH batch payments (ACH payments, collections, and payroll).

Corporate features (cont'd)

Features	Description
Incoming/Outgoing Wire Activity	Provides the ability for end users to access and view transaction details associated with incoming or outgoing domestic and international wire transactions. Connectivity to a real-time wire processor is required. The available data and timeliness of the data shown will be dependent on the integration made available by the third party service wire system.
Incoming Wire Alerts	Provides the ability for end users to set up incoming domestic and international wire alerts within Corporate Banking. Connectivity to a real-time wire processor is required. The available data and timeliness of data shown will be dependent on the integration made available by the third-party wire system.
Account Labels	Provides the ability for a User to add labels to accounts within the Company Policy page where the labels can be associated with entitlements and information reporting, resulting in increased efficiency and productivity.
Dual Action by Transaction Type	Some financial transactions require Dual Action approval by a different end user than the one who created it, even if the drafter has approval rights. This action is driven by dollar amount and can be set at the Group level; that setting applies at the Customer and User Role level as well.
Commercial Dashboard	Allows FIs with access to a large volume of accounts to organize accounts, view different balances, and access quick links and widgets in a User-defined view to increase information visibility and productivity with online banking.

Note: Corporate entitlements, reporting, and RTN validation are only available for Corporate users.

Differences between Business and Corporate Banking

In Business, you define what you can do with your transactions. In Corporate, you define what you can do and how you manage transactions. Since Corporate is part of UUX, users will employ the same payment workflows and template workflow they use in Business. The Corporate entitlement structure allows the separation of duties and the ability to designate specific account numbers to specific transactions such as ACH Payroll.

Corporate Banking is the best solution for companies that need to:

- Have entitlements (account level, time of day, etc.) by transaction type
- Manage users with different levels of responsibility
- Generate reports with transaction information
- Validate ABA routing numbers

These capabilities make Corporate Banking a more efficient and powerful choice for large Business Banking users with a large number of transactions.

Entitlements help different users handle transactions, while users can generate reports that contain specific financial data. Corporate users can also validate the ABA routing number in recipient records for use in ACH or Wire payments, which will reduce errors and returns. Below is a comparison of Business and Corporate features and entitlement options:

Corporate and Business functions

Functionality	Business	Corporate
User Management	X	X
Transaction Types	X	X
Account Numbers permitted to Transaction Types		X
Approval Limits	X	X
Draft Limits		X
User Roles		X
Company Policy		X
Activity Center	X	X
RTN Validation		X

Corporate and Business functions (cont'd)

Functionality	Business	Corporate
Dual Action for financial transactions	X	X
Multiple Approvals of financial transactions		X
Dual Action of non-financial actions (such as editing a User Role)		X
Information Reporting		X
Permission, Limits, and View Rights for User Roles		X
Third-party service application (also known as SSO) access based on User Roles	X	X
Entitlements (such as IP addresses and subsidiaries, etc.) tied to specific Account Numbers in Policy Rules		X

Understanding Dual Action

Dual Action (also known as *Dual Approval*) requires a transaction to be approved by a different end user from the one who created it, even if the drafter has approval rights. Some changes require Dual Action before they go into effect. These changes are categorized under non-financial and financial transactions.

Dual Action for non-financial transactions

After an administrative end user makes non-financial changes in the User Roles, Company Policy, or Users pages, another User must need to approve or reject them. Users impacted by approved changes will not be affected until they log off and log back into online banking.

Examples of non-financial changes that can be approved or rejected include:

- Editing account access rights
- Changing a User's assigned User Role
- Activating a User
- Changing a Company Policy



Tip: An approver cannot make a change, approve it, and then use the new rule in the same session. The next time the approver logs in, the changes will take effect.

Dual Action for financial transactions

Some financial transactions require Dual Action approval by a different end user than the one who created it, even if the drafter has approval rights. This action is driven by dollar amount and can be set at the Group level; that setting applies at the Customer and User Role level as well.

Each setting cascades down through each level. When you set the Dual Action amount at the Customer level, you cannot exceed the amount set at the Group level. When you set the Dual Action amount at the User Role level, you cannot exceed the amount at the Customer level.

If an end user attempts to approve an amount, at any level, that exceeds the set Dual Action amount, the Approve button will be dimmed and the user will be stopped from approving the transaction. However, the user can still draft the transaction.

Corporate Banking Policies

Q2central's Corporate Banking capabilities allow you to create and manage Group and Customer Policies that control:

- The **transactions** that Customers assigned to each Group can perform, and how those transactions can be performed. (For example, ACH Payments may only be allowed during normal work hours.) Each transaction type can have its own set of Draft, Approve, Cancel, and View rights, as well as limits. These attributes are known as *entitlements*.
- **Account permissions** that control who can view, deposit, or withdraw funds from an account.
- The **Features** (for example, Manage Templates) that are available to Customers assigned to each Group Policy.
- Whether or not **Dual Action** is required for non-financial transactions, such as changes to User Roles.

When a Corporate Customer is added to a Group, a Customer Policy is automatically generated that inherits the transaction types and resulting entitlements and features from the Group Policy. FI staff can then configure the Customer Policy to best suit its business needs.

For each Customer Policy, an FI can also create a variety of User Roles to which end users can be assigned. Each User Role has a different combination of entitlements, account permissions, and features. User Roles can be created individually, or default User Role templates can be used and then modified, as necessary. For example, Payables-related User Role templates include Admin, Payables Admin, Payables Clerk, and Payables Manager.

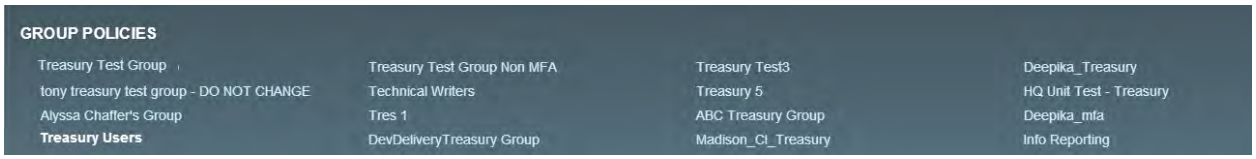
The lowest policy level—the Company Policy—inherits entitlements, Features, account details, and User Roles from the Customer Policy, which can then be tailored by Corporate Banking end users associated with a User Role that has Manage Company Policy rights.

This section outlines the options available for the various policies that make up Corporate Banking. The Corporate Banking-related options can also be managed from the User Management section of the Q2central workspace tree, in the respective Groups, Customers, and Users options. See "Managing Users" on page 213 for details.

Group Policies list

To display existing Group Policies, click the Corporate Banking option in the User Management section of the Q2central workspace tree. The Group Policies window appears and displays all Groups created via the User Management section of the workspace tree (**User Management > Groups**) for which Corporate Banking is enabled.

Group Policies list



To edit an existing Group Policy

1. Click the Group Policy in the Group Policies list. The Group Policy name appears in the bottom of the Group Policies window, along with any Customers that are children of the parent Group Policy.

2. Click the **Edit** ( ) icon next to the name of the selected Group Policy. The Group Policy window appears.
3. To change the entitlements for a Group Policy, see "Configuring Allowed Actions for transaction types" on page 101 and "Configuring Approval Limits for transaction types" on page 104.
4. To change the features available to Customers assigned to the Group Policy, see to "Editing Group Policy features" on page 106.

> **Note:** When closing a policy record while other policy records are open, wait briefly for the policy record to close before attempting to work with another policy record.

Group Policy

The Group Policy is the overarching set of entitlements and features that will be inherited by all Customer Policies for Customers that are children of the parent Group. The Group Policy has the greatest set of rights and features and cannot be less than what is available to the child Customer Policy associated with it.

This functionality is similar to the non-Corporate Banking functionality in Q2central's User Management. To learn more, see "Understanding User Management" on page 87.

> **Note:** For Business and Corporate Banking, there are exceptions to how Group rights and features are inherited at the Customer and User levels. For example, Dual Action can be enabled at the Customer and User level, regardless of the Group setting. There are also exceptions for Business and Corporate Banking features that warrant extra security such as Multi-Wires. See "Feature right exceptions" on page 107.

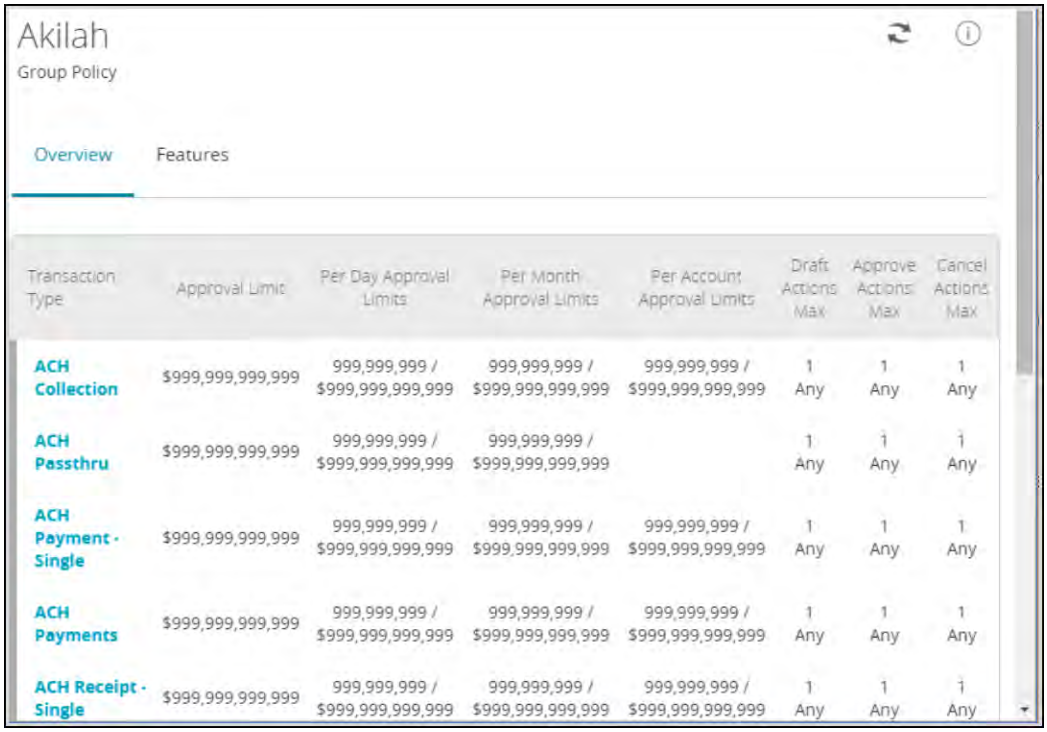
This section includes the following topics:

- "Group Policy Overview tab" on page 101
- "Group Policy Features tab" on page 106
- "Customer Policy" on page 113
- "Company Policy" on page 114

Group Policy Overview tab

After selecting a specific policy on the Group Policies window and clicking the **Edit** (✎) icon, the Group Policy window appears. The Overview tab indicates which transaction types are active for the Group Policy plus the related entitlements, as shown next. Click the **Refresh** (↻) icon at the top of the page to update displayed data.

Group Policy Overview tab



Transaction Type	Approval Limit	Per Day Approval Limits	Per Month Approval Limits	Per Account Approval Limits	Draft Actions Max	Approve Actions Max	Cancel Actions Max
ACH Collection	$999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	1 Any	1 Any	1 Any
ACH Passthru	$999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999		1 Any	1 Any	1 Any
ACH Payment - Single	$999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	1 Any	1 Any	1 Any
ACH Payments	$999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	1 Any	1 Any	1 Any
ACH Receipt - Single	$999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	999,999,999 / $999,999,999,999	1 Any	1 Any	1 Any

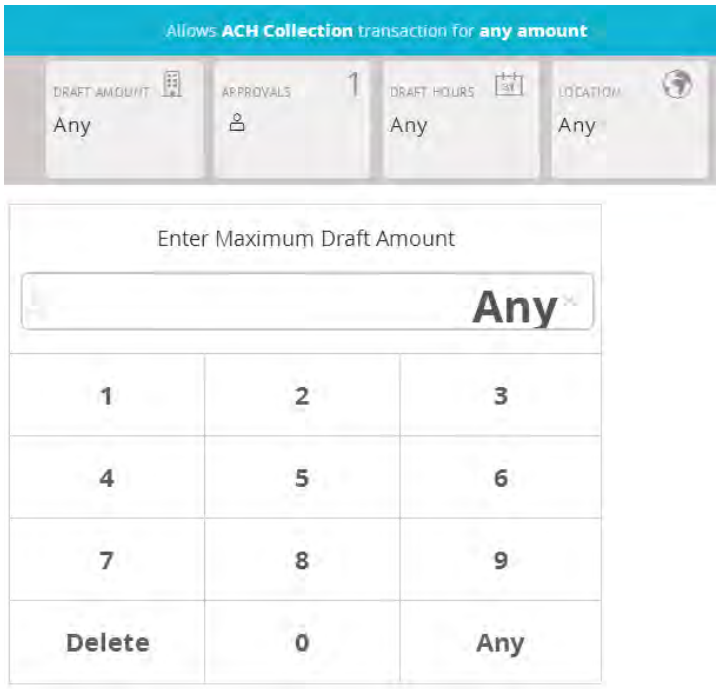
Note: Group transaction types are determined and maintained by FI staff in Q2central. This information is never seen by the end user.

Configuring Allowed Actions for transaction types

You can configure the entitlements for a Group Policy by specifying Allowed Actions for each transaction type and setting limits. These entitlements will be inherited by all Customer Policies linked to the Group Policy.

Note: After creating a new Allowed Action, you must enable it to activate it.

Group Policy Allowed Actions



To configure Allowed Actions for a transaction type

1. In the User Management section of the Q2central workspace tree, click **Corporate**. The Group Policies page appears.
2. Click the Group Policy you want to edit, and then click the **Edit** (✎) icon. The Group Policy page appears.
3. On the Overview tab, click the **Transaction Type** for which you are creating an Allowed Action. The Allowed Actions tab for the selected transaction type appears with the current restrictions.
4. Click **Add New Allowed Action**. The Policy Rules page for the selected transaction type appears.
5. Specify values for the options that appear. After changing an option, click **OK** to return to the Policy Rules page and make any other necessary changes.
6. Click **Save** to return to the Group Policy page. The summary appears above the new Allowed Action.

Note: When closing a policy record while other policy records are open, wait briefly for the record to close before attempting to work with another record.

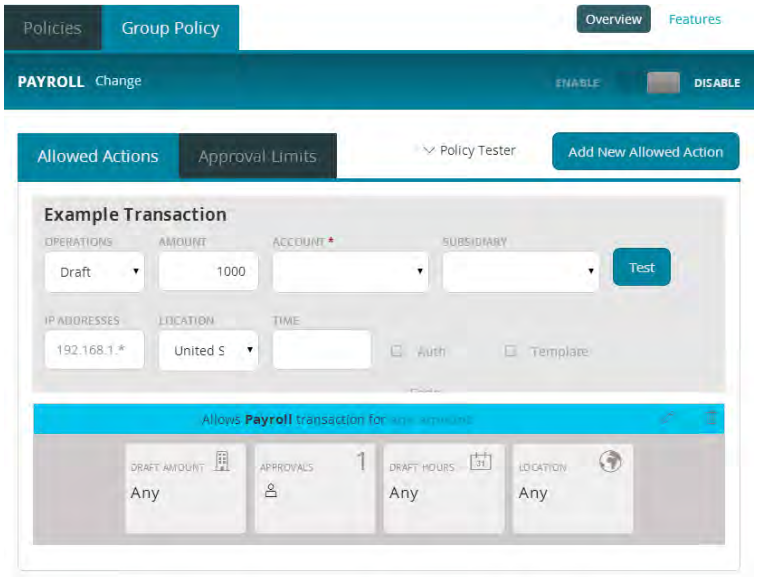
7. Click or tap **Enable** to activate the Allowed Action.

Tip: To create additional Allowed Actions, click **Add New Allowed Action** and repeat the steps above.

Using the Policy Tester for a Group Policy

Use the Policy Tester to assess potential Allowed Action edits before making permanent changes.

Sample transaction in the Policy Tester



To use the Policy Tester

1. Click **User Management > Corporate** in the workspace tree. The Group Policies page appears.
2. Click or tap the Group Policy you want to edit, and then click the **Edit** ( ) icon. The Group Policy page appears.
3. Click the **Transaction Type** for which you want to test a policy. The Allowed Actions tab appears.

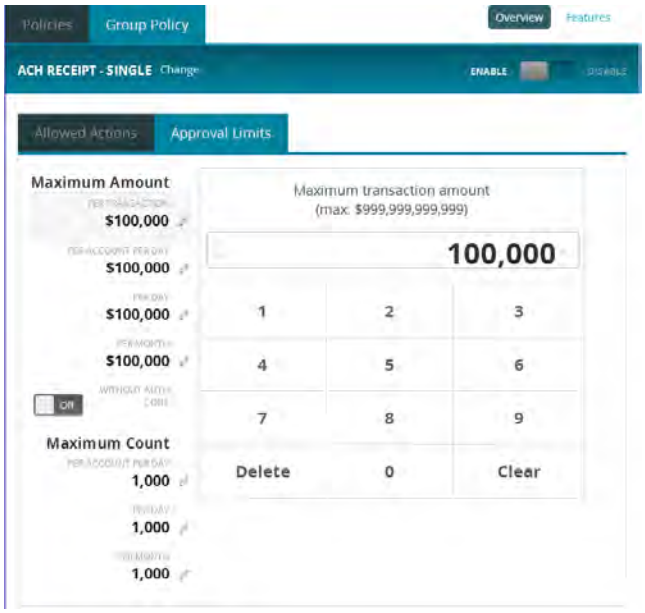
4. Click the Allowed Action row that you want to test.
5. Click **Policy Tester**. The Example Transaction fields appear with fields that are specific to the transaction type, which may include:
   - **Operations**
   - **Amount**
   - **Account**
   - **Subsidiaries**
   - **IP Addresses**
   - **Location**
   - **Time**
6. (Optional) Select **Template** to create a template.
7. Click or tap **Test**. The Policy Results appear and indicate if the FI settings will allow or deny the transaction.

Configuring Approval Limits for transaction types

This section describes how to configure Approval Limits for transaction types that are active for a Group Policy that will be inherited by all Customer Policies linked to the Group Policy.

> **Caution:** The default amounts for transaction type Approval Limits are set at the maximum allowed values. Be sure to adjust these limits, as necessary, for each Group Policy.

Group Policy Approval Limits



To configure Approval Limits for a transaction type

1. In the User Management section of the Q2central workspace tree, click **Corporate**. The Group Policies page appears.
2. Click the Group Policy you want to edit, and then click the **Edit** (✎) icon. The Group Policy page for the selected Group appears.
3. On the Overview tab, click the **Transaction Type** for which you are configuring an Approval Limit. The Allowed Actions tab for the selected transaction type appears with the current restrictions.
4. Click the Approval Limits tab to display the current limits for the transaction type.
5. For the following fields, click the **Edit** (✎) icon and adjust the amounts, as necessary.
   - **Per Transaction**
   - **Per Account Per Day**
   - **Per Day**
   - **Per Month**
6. Enable **Without Auth Code**, as necessary. When this option is enabled, a field appears where you can enter the limit for transactions that can be performed without providing a security token. Any transaction over that amount will require a security token.

   Note: The limit for transactions that can be performed without providing a security token established in the Group Policy will impact all Customer Policies linked to the Group Policy. For example, if **Without Auth Code** is enabled at the Group level for ACH Collection transactions over $1,000,000, the limit for related child Customer Policies will be $1,000,000 or less.

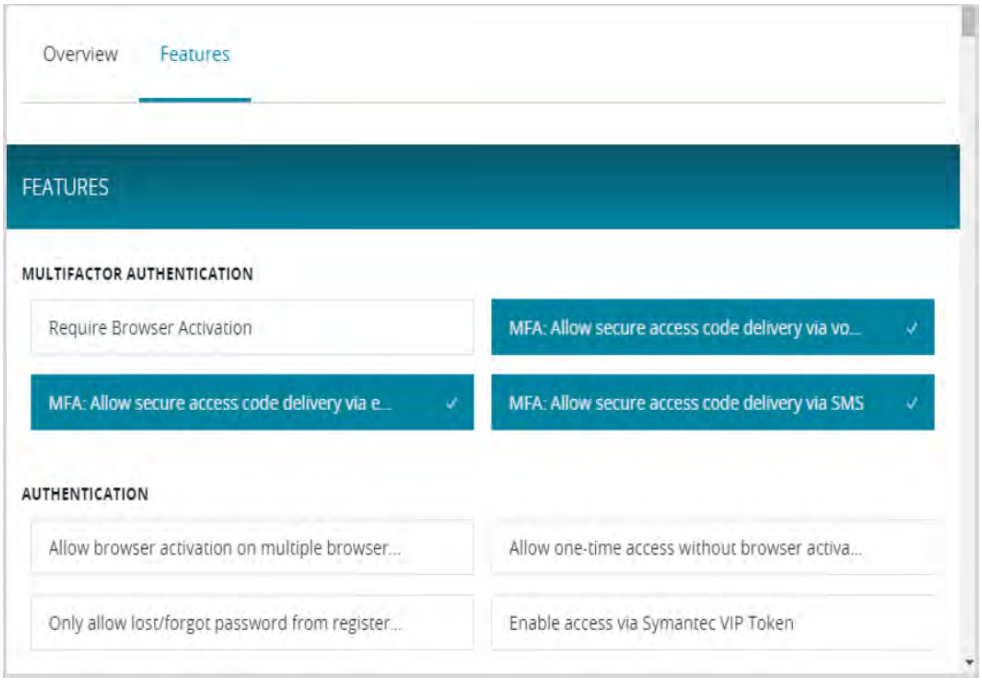
7. For each of the following fields, click the **Edit** (✎) icon and adjust the Maximum Count values, as necessary.
   - **Per Account Per Day**
   - **Per Day**
   - **Per Month**
8. Click **Save** to save the changes and return to the Group Policy page.

Note: When closing a policy record while other policy records are open, wait briefly for the policy record to close before attempting to work with another policy record.

Group Policy Features tab

View or edit the selected Group Policy by clicking the Edit ( ) icon. Click the Features tab to display the enabled options associated with the Group Policy. Click the **Refresh** ( ) icon at the top of the page to refresh data.

Group Policy Features tab



Note: The Group Policy and related Group Features are maintained by FI staff. This level of management is never seen by the end user.

Editing Group Policy features

To edit the features that are available for a Group Policy

1. In the User Management section of the Q2central workspace tree, click **Corporate**. The Group Policies page appears.
2. Click the Group Policy you want to edit, and then click the **Edit** ( ) icon. The Group Policy page appears.
3. Click the **Features** tab to see a list of available features.

4. Click the desired **Features** to enable and disable them. The feature categories will vary depending on your configuration and may include:
    - Multifactor Authentication
    - Mobile
    - Corporate
    - ACH
    - Authentication
    - Link out (to third-party offerings such as Bill Pay)
    - Quick Action
    - Rights
    - Other Services



Note: When closing a policy record while other policy records are open, wait briefly for the policy record to close before attempting to work with another policy record.

Feature right exceptions

The standard Q2central User Management hierarchy dictates that feature rights (such as the ability to add Users) set at the Group level are inherited down to the Customer and User levels automatically. The goal is to set the highest rights at the Group level to minimize time spent to set up Customers and Users.

Starting in Q2central 4.3.0.5004, there are exceptions regarding how rights are inherited for Business and Corporate Banking features that warrant extra security, including:

- CentrixETMS Group (This feature validates the payee on a check image against the payee name that a User included in an issued check file.)
- Commercial Dashboard
- Enable Multi-Transfer
- Enable Multi-Wire
- ACH: Allow one day credit ACH payments
- ACH: Allow one day credit ACH payroll batches
- Enable Same Day ACH

This functionality is useful in situations such as when an FI wants to pause specific functionality, such as Multi-Wires. For example, if a fraud investigation is underway, the FI can pause all Multi-Wires until the investigation is complete.

When the FI enables that feature again for the Group Policy, the ability to use the feature is also restored for Customer Policies, Company Policies and User Roles linked to the Group Policy that rights to the feature to begin with.

The following table describes where Group feature rights are configured, along with the lower levels that inherit them.

Configuring Group feature rights

Group type	Wherefeature rights are configured	Levels that inherit Group feature rights
Business	Group > Features tab	Customer User
Corporate	Group > Policy Dashboard	Customer Policy Company Policy User Roles

Expected feature right exception behavior in Business Banking

This section describes how features with right exceptions behave in Business Banking Groups. Expected behavior varies, depending on whether administrative staff is:

- Enabling features with right exceptions for the first time, or
- Disabling features with right exceptions.

Expected behavior when enabling feature rights for the first time

This section describes how settings for features with right exceptions cascade into lower levels when FI staff configure rights for the first time.

The following table includes these symbols:

 = Disabled

 = Enabled

 = Not available because right is disabled at a higher level

Cascading behavior for features with right exceptions

Scenario	Group level	Customer level	User level
1			
2			
3			
4			

Depending on the scenario, expected behavior for features with right exceptions is as follows:

- **Scenario 1:** The feature is disabled at the Group level—the default setting for all features, initially. Rights are not available at the Customer or User level.
- **Scenario 2:** FI staff enables a feature at the Group level and clicks **Save**. The feature is disabled at the Customer level, but is actionable (that is, it can be enabled). It is not available at the User level.
- **Scenario 3:**FI staff enables a feature at the Customer level and clicks **Save**. The feature is disabled at the User level, but is actionable.
- **Scenario 4:**FI staff enables a feature at the User level and clicks **Save**. The feature is available to the User.

Expected behavior when disabling feature rights

This section describes how features with right exceptions behave when they are disabled at the Group level. Features with right exceptions (see"Feature right exceptions" on page 107) can be disabled at the Group, Customer, or User levels to block Users at lower levels from using them. When a disabled feature is enabled again, the system uses its records of Users with access to the feature so it can restore those rights when the feature is enabled again.

Using the earlier Multi-Wire example, this means that if an FI enables Multi-Wires after a fraud investigation, all Users that originally had rights to process Multi-Wires will have their rights restored without the FI needing to restore each User's right individually.

The following table illustrates how features with right exceptions behave when they are disabled, assuming that rights were previously enabled at all levels. It includes the following symbols:

 = Disabled

 = Enabled

 = Disabled and not currently active at a higher rights level

 = Previously enabled but not currently active at a higher levels

Expected behavior for features with rights exceptions

Scenario	Group level	Customer level	User level
1			
2			
3			
4			

The expected behavior for feature right exceptions in Business Banking is as follows for the scenarios listed in the table:

- **Scenario 1:** A feature is enabled at the Group, Customer, and User level.
- **Scenario 2:** A feature is disabled at the Group level. The feature is present and actionable (that is, it can be enabled or disabled) at the Customer level, but present and inactive at the User level.
- **Scenario 3:** A feature is enabled at the Group level. The feature is disabled at the Customer level, but actionable. It appears but is not actionable at the User level.

  Note: If a feature was enabled and later a subsequently higher tier is disabled, the feature is automatically enabled when the higher tier is enabled again.

- **Scenario 4:** A feature is enabled at the Group and Customer levels, but disabled at the User level. The feature is actionable for individual Users.

> **Note:** If a feature was enabled and later a subsequently higher tier is disabled, the feature is automatically enabled when the higher tier is enabled again.

Expected feature right exception behavior in Corporate Banking

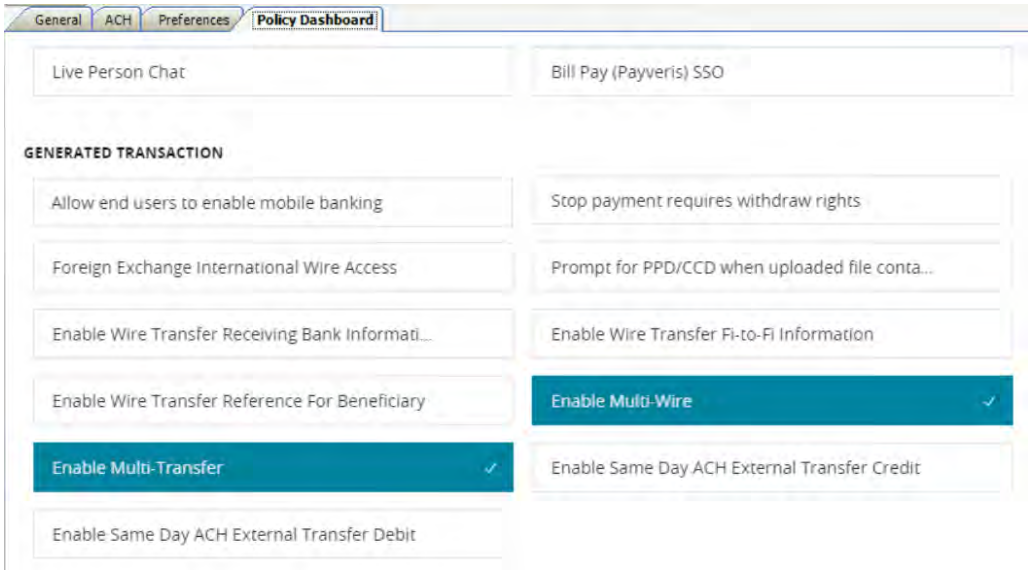
This section describes how features with right exceptions (see "Feature right exceptions" on page 107) behave in Corporate Banking.

For Corporate Groups, FI staff configures features on the Policy Dashboard tab of the Group page. Enabled features appear dark blue with a check mark; disabled features are white.

In the following figure, the following rights are enabled:

- Enable Multi-Transfer
- Enable Multi-Wire

Enabling features (Group Policy > Features tab)



At the next level down from the Group Policy—the Customer Policy—only features enabled for the Group Policy appear as available options, as shown in the following figure.

Enabling features (Customer Policy > Features tab)



The same is true for the Company Policy; only features enabled in the Customer Policy appear as available options in child Company Policies. Those same features, if still enabled, trickle down from the Company Policy to the list of available features for User Roles.

The following table shows how settings for features with right exceptions cascade in Corporate Banking.

- ☐ = Disabled, but can be enabled
- ■ = Enabled
- N/A = Is not available. If a feature is disabled at a higher level, it will not appear at lower levels.

Expected behavior for features with rights exceptions

Group Policy	Customer Policy	Company Policy	User Role
☐	N/A	N/A	N/A
■	☐	N/A	N/A
■	■	☐	N/A
■	■	■	☐

Customer Policy

The Customer Policy is an extension of the overarching Group Policy. After a Customer is assigned to a Group Policy, a Customer Policy is automatically generated that inherits the transaction types and resulting entitlements and features from the Group Policy. FI staff can configure the Customer Policy to best suit the business needs of the Customer.

In addition to Transaction Type rights and Features, the Customer Policy includes account rights (View, Deposit, and Withdraw), as well as User Roles to which users can be assigned.

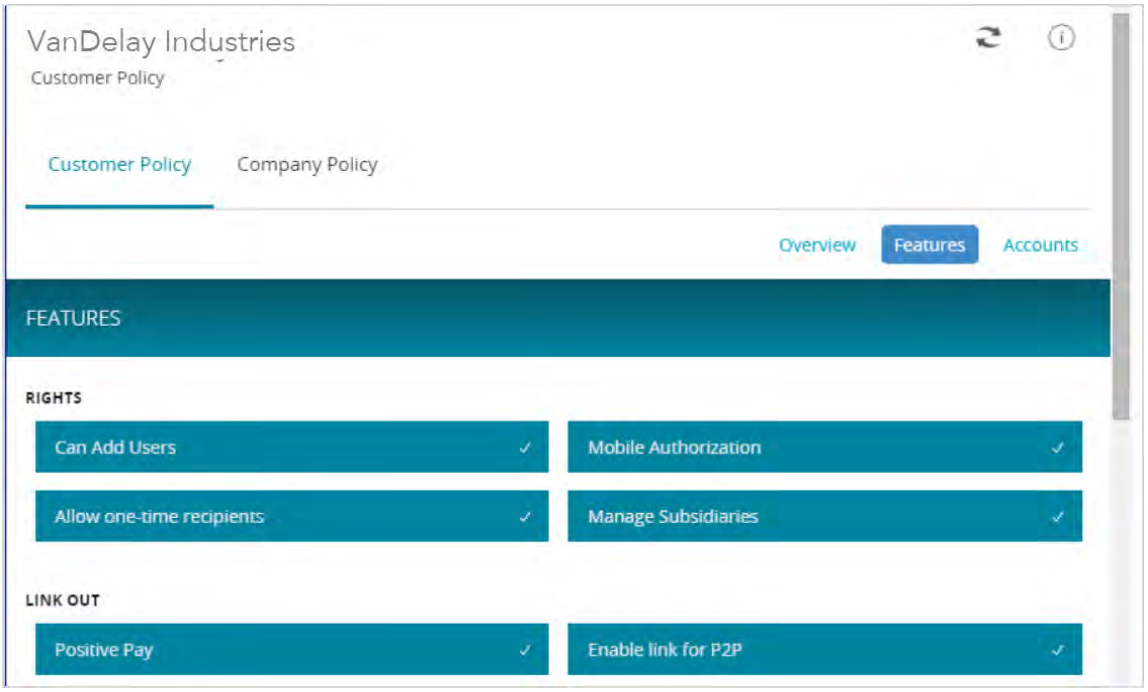
Note the following details about Customer Policies:

- Although Corporate Banking Users can display Customer Policies, they cannot edit them. Only Users associated with a User Role that has *Manage Company Policy* rights can update a Customer Policy.
- The Customer Policy cannot have greater rights or features than the parent Group Policy to which it is associated, and the Company Policy cannot have greater rights or features than the parent Customer Policy.
- The Accounts available in the Customer Policy are determined by the Accounts assigned to the Customer in the Account Management tab in User Management. (To access that tab, click **User Management > Customers**, select a Customer record and switch to the Account Management tab in the window that appears.)

Customer Policy page

The Customer Policy page includes the same tabs as the Group Policy page: Overview, Features, and Accounts. Click the **Refresh** ( ) icon at the top of the page to refresh data.

Customer Policy page



Company Policy

A Company Policy is a resulting extension of the Customer Policy that, initially, provides the same Transaction Type rights/limits (that is, entitlements), Features, Accounts, and User Roles as the parent Customer Policy.

As a user moves through the payment workflow in online banking, the system checks the User Role and limits at the User level until the work flow reaches the Review & Submit tab. At that point, the system checks the User Role and limits at the Company, Customer, and Group levels. Waiting until the completion of a transaction to check higher levels supports changes made to rights and limits between the time a transaction is drafted and the time it is actually submitted.

Note the following details about Company Policies:

- Typically, a Company Policy is managed by end users associated with a User Role that has Manage Company Policy rights. The only way that FI staff can modify the Company Policy is to log in as a Customer via CSR Assist. For details, see "Using CSR Assist" on page 261.
- The Company Policy can be edited, but not deleted. Administrative end users with Manage Company Policy rights can edit the Company Policy to configure transaction types and limits. Administrators can only make the

Company Policy more restrictive than what the FI has set in the Customer Policy in Q2central. There are some exceptions for high-risk features such as Multi-Transfers. See"Feature right exceptions" on page 107.

Corporate Banking User Roles

Q2central's Corporate Banking capabilities allow you to create User Roles that determine the rights and access allowed by each end user of Corporate Banking.

This section outlines options for managing Corporate Banking end users and actions allowed by each User Role. Roles can be fine-tuned to ensure that users can access only the data they need. Corporate Banking rights can also be managed from the User Management section in Q2central in the respective Groups, Customers, and Users options.See "Managing Users" on page 213.

User Roles

For each Customer Policy, you can configure User Roles that control the following attributes for users that will be assigned to each role:

- The transaction types that can be performed, along with view/deposit, and withdraw permissions as well as limits.
- The Features (for example, Manage Templates) that are available to users.
- View, deposit, and withdraw privileges for individual accounts.

These attributes will be inherited by any Company Policies that are created based on the Customer Policy.

Working with User Role templates

Each Customer Policy includes a set of default User Role templates that you can use "as is" or customize and rename, as necessary.



Note: If default templates do not appear on the User Roles page, click **Generate Templates**.

Default User Role templates

Name	Description
Admin Role	Provides access to all features, accounts, and enabled transaction types with full amount (per FI policy) for draft, approve, and cancel transaction rights. This role also has the maximum Role Approval Limits per Company Policy and the ability to view all User Role transaction activity.
Payables Admin	Provides access to non-User or Company Policy-related features, all accounts, and enabled payables General Transaction (GT) transaction types, including: • ACH Single Payment • ACH Payments • ACH Payroll • ACH PassThru • Domestic Wire • International Wire The Payables Admin Role also has the maximum Role Approval Limits per Company Policy and the ability to view all User Roles transaction activity.
Receivables Admin	Provides access to non-User or Company Policy-related features, all accounts, and the enabled receivables GT transaction types listed below with full allowed amount (per FI policy) for draft, approve, and cancel transaction rights. • ACH Single Payment • ACH Collections • ACH PassThru The Receivables Admin Role also has the maximum Role Approval Limits per Company Policy and the ability to view all User Roles transaction activity.

Default User Role templates (cont'd)

Name	Description
Payables/ Receivable Admin	Provides access to non-User or Company Policy-related features, all accounts, and enabled payables/receivables GT transaction types, with full amount (per FI policy) for draft, approve, and cancel transaction rights, including: • ACH Single Payment • ACH Payments • ACH Payroll • ACH PassThru • Domestic Wire • International Wire • ACH Collections The Payables/ Receivables Admin Role also has the maximum Role Approval Limits per the Company Policy and the ability to view all User Roles transaction activity.
Payables Manager	Provides access to the Manage Recipients and Manage Subsidiaries features, all accounts and the following enabled payable GT transaction types with 50% of the allowed amount (per FI policy) for draft, approve, cancel transaction rights. • ACH Single Payment • ACH Payments • ACH Payroll • ACH PassThru • Domestic Wire • International Wire The Payable Manager Role also has 50% of the Role Approval Limits per the Company Policy and the ability to view all User Roles transaction activity.

Default User Role templates (cont'd)

Name	Description
Receivables Manager	Provides access to the Manage Recipients and Manage Subsidiaries features, all accounts, and the following enabled receivables GT transaction types (with 50% of the allowed amount (per Bank policy) for draft, approve, and cancel transaction rights. • ACH Single Receipt • ACH Collections • ACH PassThru The Receivables Manager Role also has 50% of the Role Approval Limits per Company Policy and the ability to view all User Roles transaction activity.
Payables Clerk	Blocks access to features, but provides access to all accounts, and access to the following enabled payables GT transaction types with 25% of the allowed amount (per FI policy) for the draft, approve, and cancel transaction rights • ACH Single Payment • ACH Payments • ACH Payroll • ACH PassThru • Domestic Wire • International Wire The Payables Clerk also has 25% of the Role Approval Limits per Company Policy and the ability to view their own User Role transaction activity.

Default User Role templates (cont'd)

Name	Description
Receivables Clerk	Blocks access to features, but provides access to all accounts, and access to the following enabled payables GT transaction types with 25% of the allowed amount (per Bank policy) for the draft, approve, and cancel transaction rights. • ACH Single Receipt • ACH Collections • ACH PassThru The Payables Clerk also has 25% of the Role Approval Limits per Company Policy and the ability to view their own User Role transaction activity.
View Only	Blocks access to features, but provides access to all accounts, and access to view all GT transaction types, including ACH Single Receipt and ACH Collections.

After selecting a User Role, you can make changes for each transaction type.

User Role page example



This page includes the following tabs:

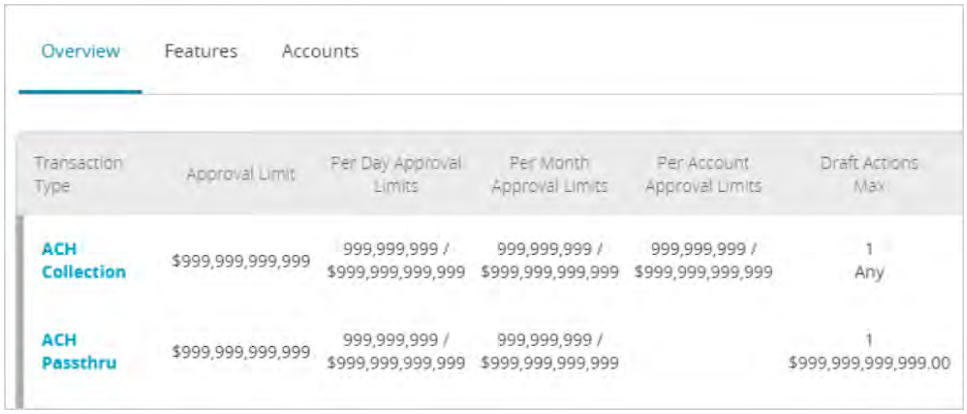
User Role tabs

Tab	Description
Overview	Displays a list of transaction types. Each enabled transaction type must have at least one action. Transaction details include: • Transaction Type • Limit • Per Day • Per Month • Per Account • Draft/DR Actions • Approve Actions • Cancel Actions • View
Features	Displays a list of entitlements and third-party services enabled for the User Role. Examples include: • Entitlements: Manage users, company policy, and templates • SSOs: Link out to third parties • Mobile: Mobile Capture • Other: Statement Image These features will vary depending on your financial institution's configuration.
Accounts	Displays a list of accounts and access rights. Access rights include: • View – View balance and history for the account on the Home page, on the Account Details page, and in reports. • Deposit – Deposit funds into the account. • Withdraw – Withdraw funds from the account.

Transaction types

Each User Role has different entitlements for each transaction type.

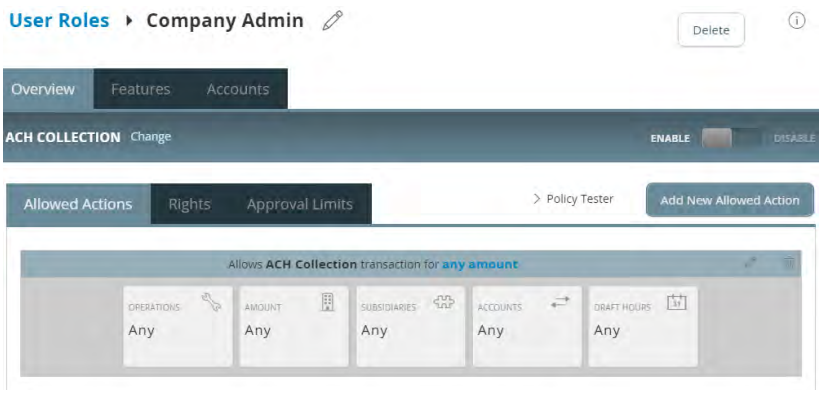
User Role transaction types



You can create a new User Role, copy existing User Roles, or copy Role Templates (if enabled) to create new ones. Edit a role by changing the policy features (Allowed Actions, limits, and policy tester). A sentence summarizes the changes so other users can see the results of the new action.

In the following example, the User Role supports drafting, canceling, and approving ACH Collections of any amount, at any time for any account.

User Policy entitlements example



For each transaction, users can change the following policy features:

User Role transaction type features

Features	Description
Allowed Actions	Change the following details for an Allowed Action: • Operations • Draft Amount • Subsidiaries • Accounts • Draft Hours After making changes, a summary of the proposed action appears.
Rights	Control whether the user can view online activity. Users can view one of the following: • All activity for the company • The activity of everyone with the same role • The user's activity • No activity

User Role transaction type features (cont'd)

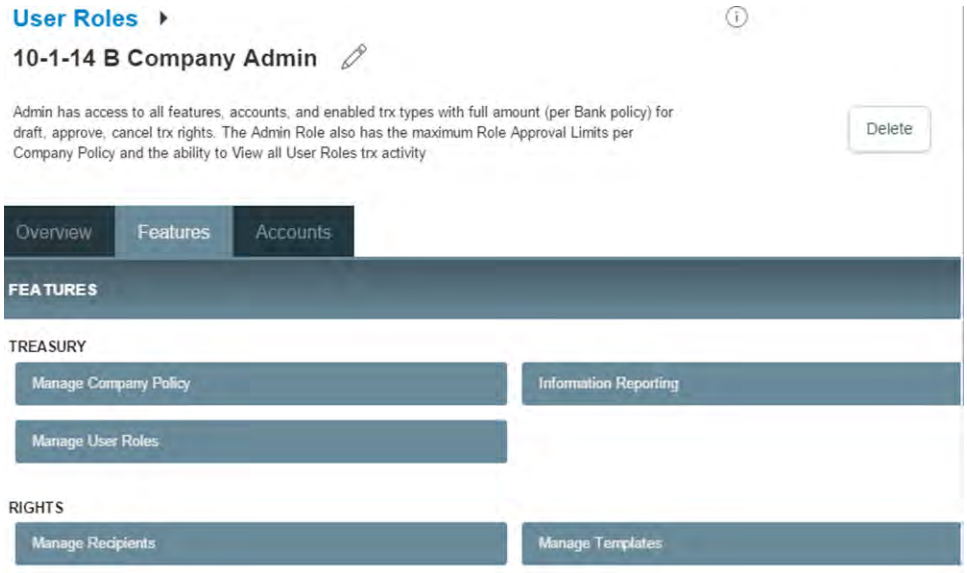
Features	Description
Limits	Set limits on the maximum transaction amounts by editing the following details: • Per transaction • Per account per day • Per day • Per month Set limits on the maximum number of transactions (also known as maximum count) by editing these values: • Per account per day • Per day • Per month
Policy Tester	Check whether changes to an action follow the Company and User Role Policies. The tester either allows or denies the changes for each policy. If the transaction is denied, that means the transaction didn't match the Allowed Actions for that policy.

Note: If digits appear in red on the Overview tab, this indicates that the limits have exceeded limits set at a higher level (for example, the Customer level vs. the Group level). This conflict may occur if the Group is changed for a Customer.

User Role Features

The Features tab on the User Role Policy page lists the features assigned to a specific user.

Features tab example



Depending on your configuration, the features may include some or all of the following:

Feature options

Option	Allows you to
Manage Templates	Create, edit, and delete templates for any transaction type.
Manage Recipients	Create, edit, and delete recipients.
Manage Subsidiaries	Create, edit, and delete subsidiaries.
Manage Users	Add and delete end users.
Statement Image	View statement images.

Feature options (cont'd)

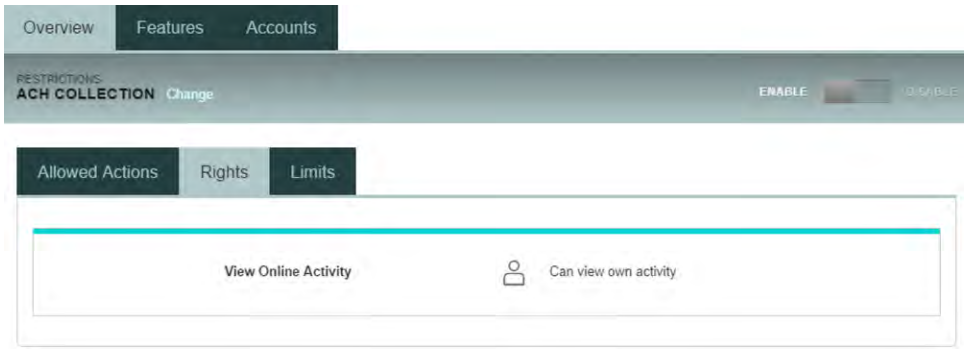
Option	Allows you to
Mobile Capture	Use Q2mobility Apps to deposit checks.
Manage Company Policy	Edit the Company Policy.
Manage User Roles	Create, edit, and delete User Roles.
Information Reporting	Generate Corporate Banking reports, as described in the *Business and Corporate Banking User Guide*.

Note: Depending on your configuration, User Role templates may appear on the Features tab. Use the templates of existing roles to create new User Roles.

Rights

Setting on the Rights tab determine how much transaction activity that end users linked to a User Role can see.

Rights tab



Unlike the Allowed Actions for a Customer Policy, the Allowed Actions for User Roles do not include IP addresses and Location features.

Depending on how a User Role is configured, users assigned to that User Role can view:

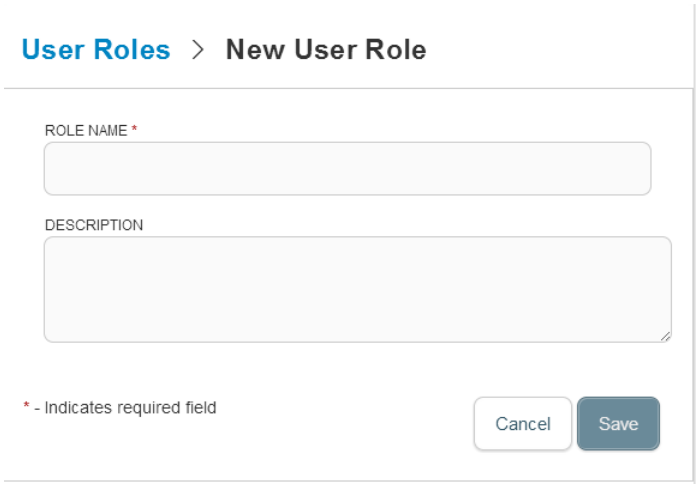
- The user's own activity
- The activity of everyone with the same role
- All activity for users throughout the company
- No activity

Creating a User Role

Use the User Roles tab in the Customer Policy window to create User Roles with different combinations of Corporate Banking entitlements, account permissions, and features. You can create a new User Role from scratch, copy an existing User Role, or copy a default User Role Template and then customize it.

After creating a User Role, you can assign individual Users to the User Role on the User General tab.

New User Role page



To create a User Role

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are adding a User Role. The Group Policies page appears.
3. Click the Customer for which you are adding a User Role. The Customer Policy page appears.
4. On the User Roles tab, click **Generate Templates** to display a list of default User Role templates if they do not already appear.

5. Click **Create Role**. The New User Role page appears.
6. Enter a **Role Name**.
7. (Optional) Enter a **Description**.
8. Click **Save**. A message confirms the policy changes.
9. Click **Close** to return to the User Roles tab.

To create a User Role based on an existing role

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are adding a User Role. The Group Policies page appears.
3. Click the Customer for which you are adding a User Role. The Customer Policy page appears.
4. On the User Roles tab, select the existing role with which you want to create a new User Role.
5. Click the **Copy** icon ( ) next to the role that you want to copy. The New User Role page appears.
6. Change **Role Name**, as necessary.
7. (Optional) Change the **Description**, if necessary.
8. Click **Save**.The Policy Saved page confirms the policy changes.
9. Click **Close**. The User Role page appears.

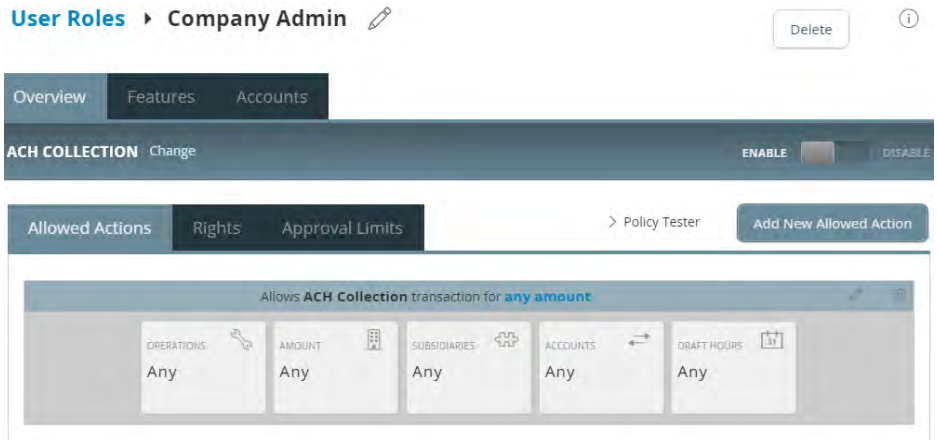
To create a User Role based on a default User Role template

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are adding a User Role. The Group Policies page appears.
3. Click the Customer for which you are adding a User Role. The Customer Policy page appears.
4. On the User Role tab, click **Generate Templates** to display a list of default User Role templates if they do not already appear.
5. Click the **Copy** icon ( ) next to the User Role template from which you want to create a new User Role. The New User Role page appears.
6. Enter a **Role Name**.
7. (Optional) Change the **Description**, if necessary.
8. Click **Save**. The Policy Saved page confirms the policy changes.
9. Click **Close**. The User Role page appears.

Editing Allowed Actions for a User Role

You can edit how a User Role interacts with a transaction type by editing the Allowed Actions.

User Role Allowed Actions



To edit the Allowed Actions for a User Role

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role.
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab and click the **Edit** icon (✎) next to the User Role you want to edit.
5. On the Overview tab, click the name of the **Transaction Type** for which you are creating an Allowed Action. The Allowed Actions tab for the selected transaction type appears with the current restrictions.
6. Create additional actions by clicking **Add New Allowed Action**. The Policy Rules page for the selected transaction type appears.
7. Add an Allowed Action by specifying values for the options that appear, which vary according to transaction type. After changing an option, click **OK** to return to the Policy Rules page and make any other necessary changes.
8. Click or tap **Policy Rules** to save the changes and return to the Customer Policy page. The summary appears above the new Allowed Action.
9. Click or tap **Save**.

Deleting a User Role

When the User Role is deleted, the user will move into an unassigned role status and will not have access to accounts.

> **Caution:** Deletion is permanent, so use caution before deleting a User Role.

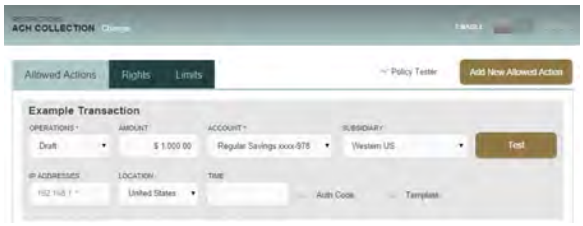
To delete a User Role

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are deleting a User Role. The Group Policies page appears.
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab and click the **Delete** icon (🗑) next to the User Role you want to edit.
5. When the confirmation message appears, click **Delete**. The "Policy Deleted" message appears.

Using the Policy Tester for a User Role

Use the Policy Tester to assess potential Allowed Action edits before making permanent changes.

Sample transaction in the Policy Tester



To use the Policy Tester

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role. The Group Policies page appears.

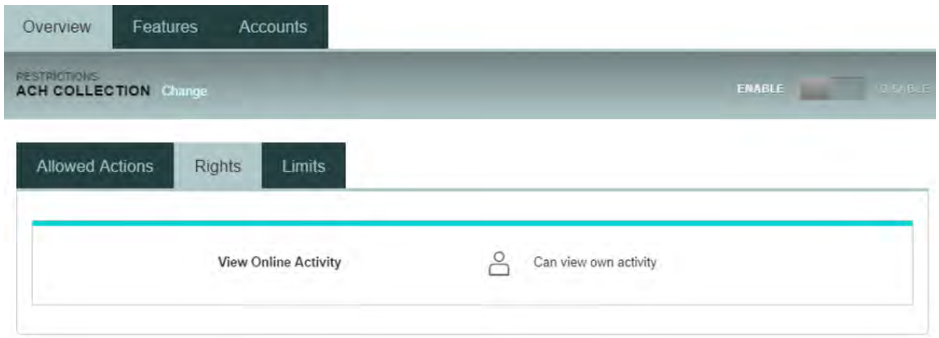
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab and click the **Edit** icon ( ) next to the User Role you want to edit. The User Roles page appears, displaying the transaction types on the Overview tab.
5. Click or tap the **Transaction Type** for which you want to use the Policy Tester. The Allowed Actions tab appears.
6. Click or tap **Policy Tester** and edit the options that appear, which vary according to the selected transaction type.
7. Click or tap **Test**. The Policy Results appear and indicate whether the User Role and FI settings will allow or deny the transaction.

Note: The FI may turn off the Subsidiaries, Draft Hours, IP Address, Location, and other features.

Editing viewing rights for a User Role

This section describes how to edit the rights for a User Role for a particular transaction type.

Rights tab



To edit viewing rights for a User Role

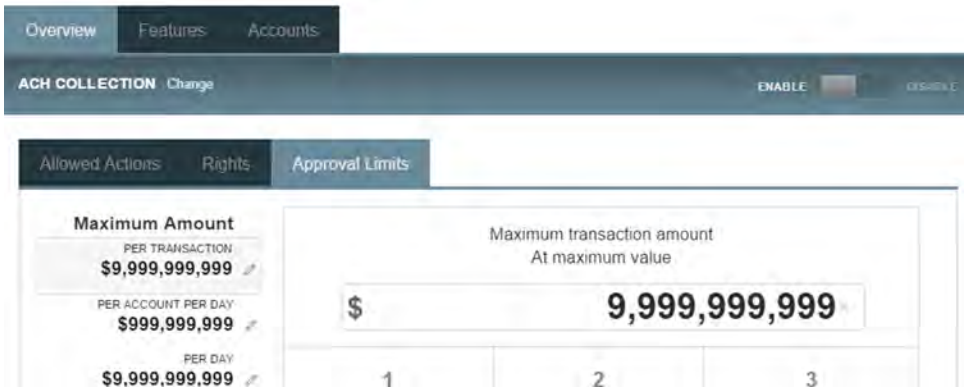
1. In the workspace tree, click **User Management > Treasury**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role. The Group Policies page appears.
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.

4. Switch to the User Roles tab and click the **Edit** icon (✎) next to the User Role you want to edit.
5. On the Overview tab, click the name of the **Transaction Type** for which you are editing rights. The Allowed Actions tab for the selected transaction type appears.
6. Click or tap the **Rights** tab and select a viewing right.
7. Click **Save**.

Editing limits for a User Role

This section describes how to edit the limits for a User Role that are associated with a transaction type.

Limits for User Roles



To edit limits for a User Role

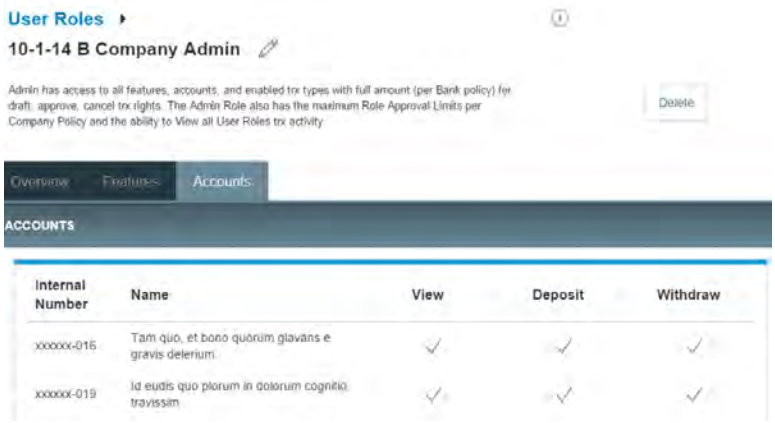
1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role. The Group Policies page appears.
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab and click the **Edit** icon (✎) next to the User Role you want to edit. The selected User Role appears.
5. On the Overview tab, click the name of the **Transaction Type** for which you are creating an Allowed Action. The Allowed Actions tab for the selected transaction type appears.
6. Click or tap the **Limits** tab to see a list of limits. The limits will vary depending on your configuration.

7. Edit limits on the maximum transaction amounts by editing the following values:
   - **Per transaction**
   - **Per account per day**
   - **Per day**
   - **Per month**
8. Edit limits on the maximum count (that is, the maximum number of transactions) by editing the following values:
   - **Per account per day**
   - **Per day**
   - **Per month**
9. Click **Save**.

Editing User Role accounts

This section describes how to change the accounts that Users associated with a particular User Role can access, as configured on the User Role Accounts page.

User Role Accounts page



To edit User Role accounts

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role. The Group Policies page appears.
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab and click the **Edit** icon (✎) next to the User Role you want to edit. The selected User Role appears.
5. Click the **Accounts** tab to see a list of accounts.

6. Edit one or more of the following access rights by clicking the icon to allow or deny access to an account:
    - **View**: View balance and history for the account on the Home page, on the Account Details page, and in reports.
    - **Deposit:** Deposit funds into the account. (Applies to ACH Receipt and ACH Collections transactions.)
    - **Withdraw**: Withdraw funds from the account. (Applies to the ACH Single Payment, ACH Payment, Payroll, Domestic Wire, and International Wire transactions.)
7. Click **Save**. The Policy Saved message appears to confirm the changes.
8. Click or tap **Close** to return to the Accounts page.

If the *Dual Action required for Nonfinancial Actions* option is enabled in the Customer Policy, the status of the User Role will be *Pending* until another user approves changes made to the User Role. The next time the user logs in, the changes will take effect. See "Dual Action for non-financial transactions" on page 97.

Editing User Role features

To edit the features that are available for a User Role

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role. The Group Policies page appears.
3. Click the Customer for which you are editing a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab and click the **Edit** icon () next to the User Role you want to edit. The selected User Role appears.
5. Click the **Features** tab to see a list of features.
6. Click the desired **Features** for the User Role. Available options will vary depending on your FI's system configuration and may include:
    - Rights
    - Link out (for example, if your FI offers an SSO such as Positive Pay)
    - Mobile
    - Transactions
    - Generated Transactions

Searching for a User Role

Enter information related to a role in the search bar to search for User Roles.

Search bar



To search for a User Role

1. In the workspace tree, click **User Management > Corporate**. The Group Policy page appears.
2. Select the Group Policy that includes the Customer Policy for which you are editing a User Role. The Group Policies page appears.
3. Click the Customer for which you are searching for a User Role. The Customer Policy page appears.
4. Switch to the User Roles tab.
5. In the search bar, enter text such as the role name and click the **Search** icon ( ). The search results appear.

CHAPTER 12: DEFINING GROUPS

In Q2central, Groups provide the foundation for User Management. Groups are made up of Customers, which are, in turn, made up of Users and Logins. Rights and limits are designated at each of these levels.

This chapter discusses the conceptual aspect of Groups in User Management, detailed reference material for each tab on the Group window, and step-by-step procedures for completing tasks while working with Groups in Q2central.

This chapter includes the following sections:

- "Group overview" on page 135
- "Group reference" on page 135
- "Group tasks" on page 178

Group overview

The Groups option lists the Groups that have been established at your FI. For more information about how Groups relate to Customers and Users, see "User management definitions and relationships" on page 87.

Group reference

The Group window in Q2central provides a means to add, view, or edit information about a specified Group. In the Group record, transactions and limits are defined, as well as features, rights, and preferences. The following sections provide a detailed reference for each of the tabs in the Group window.

If you purchased Corporate Banking, references to Corporate Banking-specific settings are also included.

Group General tab



Tip: If you selected a Corporate Banking Group record in the workspace, this tab only includes the Group Name. Use the ACH tab and Policy Dashboard tabs to configure rights and limits instead.

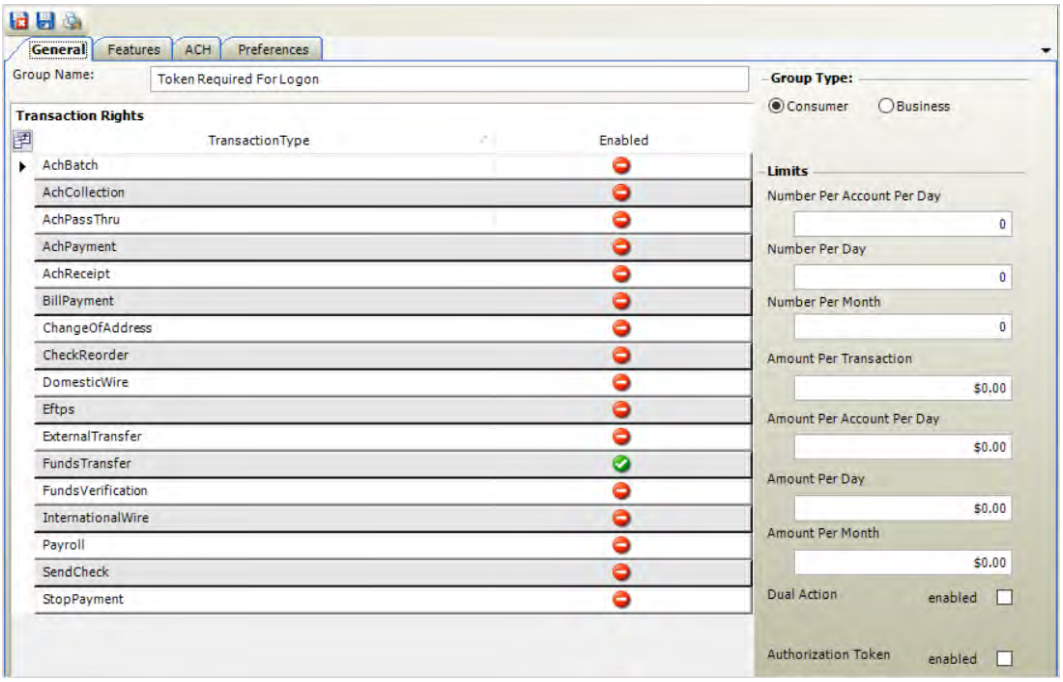
The Group General tab displays the Group name and type, plus a list of rights (that is, permissions), and associated limits for a selected Group. These settings are the foundation for Group settings that may then be applied to Customer, User, and Login ID records in online banking.

To access the Group General tab, click **User Management > Groups**, search for a Group, and then double-click the Group record. The Group name, enabled or disabled transaction types, and limits for each transaction type appear.

Note the following details about the Group General tab:

- When setting rights and limits, it's good practice to save work periodically.
- Advise end users that changed settings take effect only after they log out of online banking, and then log back in.

Group General tab



Group General tab options

Option	Description
Group Name	The name should be descriptive enough so that FI staff can make an informed selection when placing Customers in Groups.

Group General tab options (cont'd)

Option	Description
Group Type	Select *Consumer* or *Business*. This value will be used to gain a count of Groups, both for FI purposes and for Trusteer® implementation, if applicable. It is also used in ACH and Wire transactions if a Customer opts not to set up separate Subsidiaries. This option defaults to *Consumer*initially, but if an FI user selects a different option for a new Group, that value is saved as the new default value for that FI user later. The count of end users in a Consumer or commercial Group is not visible inQ2central.
Transaction Rights pane	
Transaction Type	A list of available transaction types, as configured during the implementation of online banking.
Enabled/Disabled	Click the icon to enable/disable each transaction type that Customers and Users in this Group may perform.
Limits pane	
Options vary depending on the Transaction Right selected.	Provide a value other than 0 for each field. Otherwise, Users in this Group cannot perform the associated transaction type. • Number per Account per Day • Number per Day • Number per Month • Amount per Transaction • Amount per Account per Day • Amount per Day • Amount per Month Limits can be lowered (but cannot be raised) at the Customer and User levels. For details, see the *Q2central Transaction Processing Guide*.
Dual Action	Enable this option to require that two Users within each Customer record approve transactions. This option can be disabled at the Customer or User level, if necessary. See"Understanding Dual Action" on page 97.

Group General tab options (cont'd)

Option	Description
Authorization Token	Select the enabled check box to require that a Symantec token code or secure access code (SAC) be provided when an end user approves a transaction. This right can be disabled at the Customer or User level, if necessary.



Tip: Save your settings before proceeding to another tab or closing the window.

Understanding Dual Action

You can enable Dual Action (formerly called *Dual Approval*) for transaction types to require that at least two Users approve a transaction before it is considered authorized. The transaction must be approved by a different User from the one who created it, even if the drafter has approval rights.

Note the following details about Dual Action:

- When Dual Action is set at the Group level, the Dual Action amount is enforced all the way down to the User level.
- To make Dual Action more restrictive, do so at the Customer level first and then the User level. The key is that the User must be more restrictive than the Customer and the Customer setting more restrictive than the Group.
- To the opposite effect, Dual Action can be enabled at the individual User level without the need to enable it at the Customer or Group level. The same is true at the Customer level, but all of the Customer's Users will have the Customer setting applied.
- Dual Action can also be enabled for non-financial transactions such as Editing account access rights.
- Only CSRs can enable Dual Action for Business Banking Users. For Corporate Banking Customers, a User with administrative privileges can configure Dual Action in the Company Policy and/or User Role.

Group Transaction Rights list

The following table lists available Transaction Rights for a Group, as defined on the General tab.

Transaction Rights and Limits reference

Transaction Right	Description
ACH Batch	A commercial batch payment that send funds to multiple recipients through the ACH Network.
ACH Collection	A commercial batch payment of several debits to the recipients' accounts and one large credit to the user's account.
ACH PassThru	A commercial payment that allows users to import a single pre-formatted file that contains multiple batches.
ACH Payment	A commercial batch payment of one large debit to the user's account and several credits into the recipients' accounts.
ACH Single Payment	A commercial payment of a single credit to a single recipient's account and a debit to the user's account.
ACH Single Receipt	A commercial payment of a debit to a single recipient's account and a credit to the user's account.
Bill Payment	Allows users to access a Bill Pay vendor's site to manage their bills.
Change of Address	Allows users to submit a request to change their address of account on the core. This usually is a transaction that must be manually processed unless an FI has a special link out to the core that allows the transaction to occur in real-time. End users can access this transaction type via the Services menu in online banking.
Check Reorder	Provides users access to the check vendor's site to reorder checks via the Navigation menu in online banking. (This can also be a form submitted to the FI for manual processing.)
Domestic Wire	Allows users to send a wire transfer to a recipient in the United States.
EFTPS	A commercial payment that allows users to pay their taxes using online banking.

Transaction Rights and Limits reference (cont'd)

Transaction Right	Description
External Transfer	Allows users to transfer money between the internal accounts and external accounts they own and have access to in online banking. End users access this transaction type by clicking **Services** on the Navigation menu in online banking.
Funds Transfer	Allows users to transfer money between the internal accounts they own and have access to in online banking.
Funds Verification Request	FI staff can create Customer, User, and Login records for merchants in a Group with this right enabled. Merchants can then log into Q2voice and enter account numbers to verify funds. To limit the number of verifications, set a limit for the Merchant Verification transaction type (if listed) at the Group or Customer level. **Note:** This option is used only by FIs that purchased Merchant Services as a supplemental feature to Q2voice.
International Wire	Allows Users to process an international wire.
Payroll	A commercial batch payment of several credits to multiple recipient accounts and one large debit to the User's account to pay employees.
Send Check	Allows Users to request a paper cashier or teller for a designated payee or end user. Users can access this transaction type by clicking **Services** on the Navigation menu in online banking. Although this is a manual process, the transaction will appear in Activity Center.

Transaction Rights and Limits reference (cont'd)

Transaction Right	Description
Stop Payment	Allows Users to request a stop payment for an individual check or a series of checks that have not yet been presented for payment. The stop payment may be processed manually or in real time, depending on the core. **Note:** In addition to View rights for an account, a User may need Withdrawal rights to perform a stop payment, depending on how the *Require withdrawal rights on account to perform stop payment* option is configured on the Group > Features tab. See "Default Group features" on page 144.

Group Transaction Limits list

The following table outlines the Transaction Limits available for Q2central Group Transaction Rights. For detailed information and recommendations about transaction limits, refer to the *Q2central Transaction Processing Guide*.

Note: If you change an existing Group limit later and the new value exceeds the Customer limit, the Customer limit is updated to match the Group limit automatically.

Group Transaction Rights Limits

Limit	Description
Number Per Account Per Day	The number of times a User is allowed to originate this type of change to one account during a given day.
Number Per Day	The number of times a User is allowed to originate this type of change from all entitled accounts on a given day.

Group Transaction Rights Limits (cont'd)

Limit	Description
Number Per Month	The number of times a User is allowed to originate this type of change from entitled accounts during a given month.
Amount Per Transaction	The maximum dollar amount a User is allowed to include in one transaction of this type. If this value is 0, no transactions can be approved.
Amount Per Account Per Day	The maximum dollar amount a User is allowed to transact from one account in a given day. If this value is 0, no transactions can be approved.
Amount Per Day	The maximum dollar amount a User is allowed to transact of this transaction type from all entitled accounts in one day. If this is value is 0, no transactions can be approved.
Amount Per Month	The maximum dollar amount a User is allowed to transact of this transaction type from all entitled accounts in one month.
Dual Action	Requires that two Users approve the transaction. See "Understanding Dual Action" on page 97 for details.
Authorization Token	Requires that a secure access code (SAC) or a VIP token code be provided to complete the transaction.

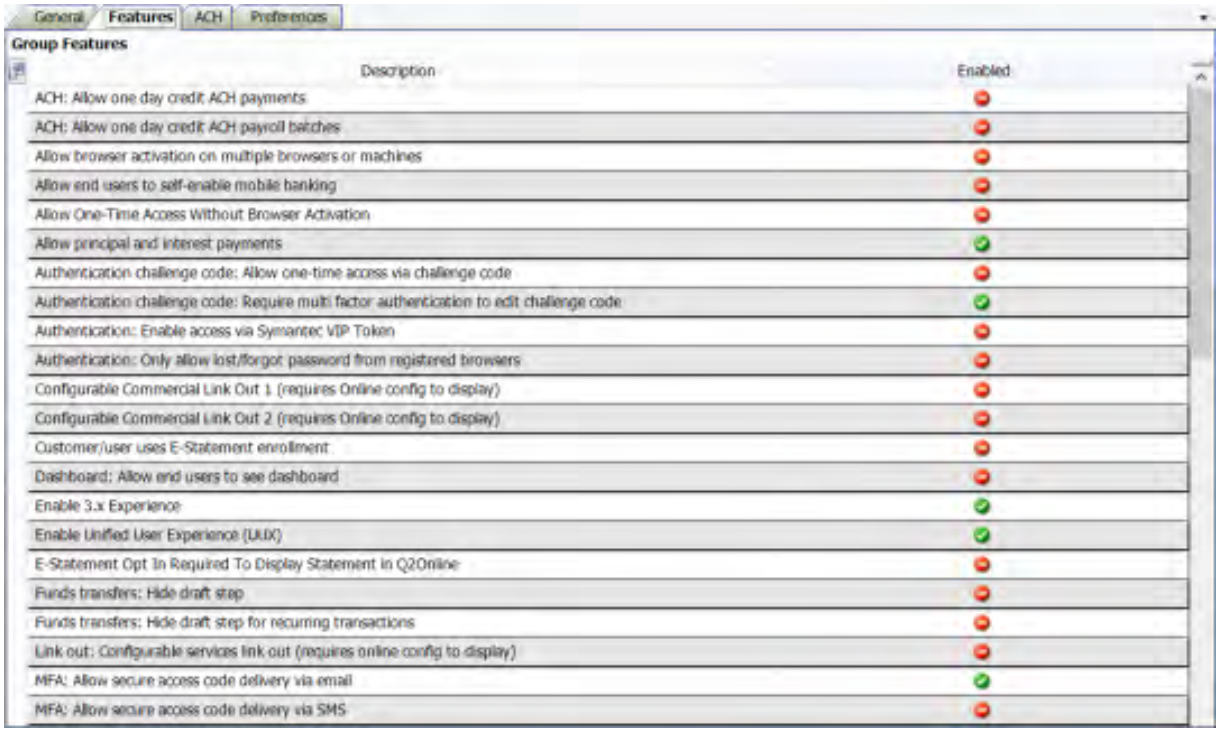
Group Features tab

The Group Features tab displays a list of features that can be enabled for a selected Group. A *feature* is a capability that can be performed in online banking, such as logging in with Touch Authentication or making commercial payments.

Note the following details about the Features tab:

- This tab will not appear if you selected a Corporate Group record in the Q2central workspace. Use the Policy Dashboard tab that appears for Corporate Groups instead. See "Group Policy Dashboard tab overview (Corporate Banking)" on page 176.
- Features listed vary, depending on which capabilities and add-ons (for example, Live Person Chat) your FI offers.

Group Features tab



Default Group features

The following table details the default features available for Groups in Q2central. Custom features may also be enabled during implementation or via a support request. See "Custom Group features" on page 155.

Group Features list

Group Feature	Description
ACH: Allow one-day credit ACH payments	Allows Business and Corporate Users to submit ACH payments for one-day processing, as opposed to the typical two-day processing. ACH credits are usually submitted two business days before the effective date. FIs that enable this option allow commercial Users to submit an ACH credit whose effective date is the next business day. **Note:** Even if this feature is enabled and a User has permission to submit an ACH payment, files submitted two or more business days before the effective date must be authorized at least two days before the effective date. Otherwise the files will be considered stale-dated and must be resubmitted.
ACH: Allow one-day credit ACH payroll batches	Same as above, but applies to payroll payments (credits).

Group Features list (cont'd)

Group Feature	Description
Allow ACH Company Entry Description Entry	The Company Entry Description field appears in Payment and Template workflows to support NACHA file formats with a Company Entry Description (CED) in the Batch Header record to describe the purpose or intent of a transaction. If this feature is not enabled, the Q2 [Generated] Transaction Type name will appear in this field in outgoing ACH files. Entry formatting must comply with NACHA rules regarding the purpose of the payment, but the ability to add a CED must also comply with the rules for when (REVERSAL) and how (HEALTHCARE) these entries can be made. **Caution:** Be aware of requirements entries, such as Retries. Ensure that ACH agreements contain language regarding how Users must comply with the rules.
Allow one-time recipients	Allows Business or Corporate Users to add a payment recipient without recording recipient details to the database for future use.

Group Features list (cont'd)

Group Feature	Description
Authentication: Allow browser activation on multiple browsers or machines	Allows Users to access online banking via multiple computers or browsers that they activated by providing a SAC or VIP token code. Users will not need to activate a browser again unless their cookies get removed or the browser's settings are reset. If this feature is enabled, Users will see a dialog box after logging into online banking, where they can opt to register a browser or just allow one-time access without registering the browser. **Note:** This feature is used in conjunction with the *Authentication: Require Browser Activation* feature.
Authentication challenge code: Allow one-time access via challenge code	Allows Users to set up a question that must be answered correctly during login, if MFA is enabled. **Note:** Challenge codes are not considered a secure means of user access because they do not provide out-of-band (OOB) authentication. Although not recommended, this capability is provided for backward compatibility with older versions of Q2 products.

Group Features list (cont'd)

Group Feature	Description
Authentication: Allow one-time access without browser activation	Allows Users who provide a secure access code (SAC) to access account information without registering the browser for future use. This setting is the equivalent of treating every computer as if it were a public computer (for example, at a library or airport kiosk). For Groups that originate high-risk transactions, you may wish to enable this feature only and disable all other authentication features. Doing so requires Users to receive a SAC at each login and prevents browser registration. **Note:** This feature is used in conjunction with the *Authentication: Require Browser Activation* feature.
Authentication: Never expire end-user passwords	This security setting overrides any requirement in the FI's Internet Password Policy regarding how Users change passwords (see "Adding a password policy for a channel" on page 68). This feature allows Users to continue using the same password long-term. It is often enabled for low-risk, low-maintenance Groups.

Group Features list (cont'd)

Group Feature	Description
Authentication: Only allow lost/forgot password from registered browsers	Requires browser registration before a User can retrieve a password via the **Forgot Your Password** link. If this feature is not enabled, a User can request that a password reset from an unsecured browser. **Note:** Disabling this feature is not recommended because it may allow unauthorized people to reset a password.
Authentication: Require browser activation	Requires Users to activate their browser (Internet Explorer, Chrome, etc.) before accessing their online banking profile. This feature is associated with multi-factor authorization (MFA) and is recommended, per Federal Financial Institutions Examination Council (FFIEC) guidance. This feature cannot be disabled if the *Authentication: Allow browser activation on multiple browsers or machines* feature is enabled.
Commercial Payments for UUX	Enables Business and Corporate Banking Users to perform commercial payments. This functionality is typically accessible via the Commercial menu, along with options for User Management, Subsidiaries, etc.

Group Features list (cont'd)

Group Feature	Description
Customer/Subsidiaries	Enables and Corporate Banking Users to create and manage subsidiaries in online banking. **Note:** In earlier releases, the ability to manage subsidiaries was only available at the User level. Now FIs can unilaterally turn this feature off at the Group level so that administrative end users cannot see it. Another alternative is to disable this feature for some Customers and Users, while enabling it for others in the same Group.
Enable Wire Transfer Fi To Fi Information	Enables Business and Corporate Banking Users to enter up to six lines (35 characters each per Fedwire spec) in the Review & Submit page for wire payments.
Enable Wire Transfer Receiving Bank	Enables Business and Corporate Banking Users to enter Receiving Bank data in the Recipient Account Detail section for whichever accounts have a Receiving Bank associated with wire payments.
Enable Wire Transfer Reference For Beneficiary	Enables the Reference for Beneficiary field for wire payments.

Group Features list (cont'd)

Group Feature	Description
Funds transfers: Hide draft step	Allows Users to bypass the Draft status when executing funds transfers. Instead, Users are directed to the Activity Center immediately after submitting a transaction, reducing the chance that Users inadvertently leave transactions incomplete. After submission, the record appears as an Authorized or Processed transaction, depending on the processing date.
Funds transfers: Hide draft step for recurring transactions	Allows Users to bypass the Draft status for funds transfers. Instead, they are directed to the Manage Recurring Transactions page immediately after submitting a transaction, reducing the chance that Users inadvertently leave transactions incomplete. After submission, the record appears as an Authorized or Processed transaction, depending on the processing date.  **Note:** The draft step will not be skipped in certain cases (for example if a User has Authorization Token enabled for funds transfers).
Link Out: Configurable commercial link out 1	Allows Users to access a non-SSO application identified in the name, such as commercial Bill Pay software or account aggregation software.  **Note:** This feature is usually renamed during implementation to specify the destination of the link.

Group Features list (cont'd)

Group Feature	Description
Link Out: Configurable commercial link out 2	Allows Users to access a non-SSO application identified in the name, such as commercial Bill Pay software or account aggregation software.  **Note:** This feature is usually renamed during implementation to specify the destination of the link.
Link out: Configurable services link out (requires online config to display)	Allows Users to access a link to a non-SSO application identified in the link name. Consumer Banking examples of link-out applications include Bill Pay and e-statement software.  **Note:** This feature is usually renamed during implementation to specify the destination of the link.
MFA: Allow secure access code delivery via email	Allows Users to receive a SAC by email. SACs are sent to first-time users, during automated Forgot Password retrieval, and as part of MFA when a User registers a new browser or computer, as well as for some sensitive transactions. If not sent by email, SACs may be retrieved through a text or voice message sent to a phone.

Group Features list (cont'd)

Group Feature	Description
MFA: Allow secure access code delivery via voice	Allows Users to receive SACs via a call from Q2voice when needed for login. SACs are sent to first-time users, during automated Forgot Your Password retrieval, and as part of MFA when a User registers a new browser or computer, as well as for some sensitive transactions. Note these details about this option: • Users must have a phone number configured in online banking to select this delivery option. • The FI must own Q2voice to use this feature. • Delivery via text message is not guaranteed. • Delivery to international phone numbers is not supported.
Mobile: Allow Mobile Capture Access	Determines if Q2mobile Remote Deposit Capture (RDC) is automatically enabled for Users after accepting mRDC terms and conditions. If this feature is disabled, FI staff will need to complete the mRDC enrollment process and notify the User afterward.  **Note:** The FI must have an mRDC SSO to support this feature.

Group Features list (cont'd)

Group Feature	Description
New logins are disabled until CSR approves	Requires FI staff to approve new Users in Q2central after a User with administrative entitlements adds a new User in commercial online banking. This is a security measure to prevent fraudsters from creating their own User login records. Both FI staff and the Customer receive a secure message that the disabled record was created.
Other services: Enable other services submission support	Allows end users in this Group to access the service linked to this option during implementation, such as micro deposits, person-to-person, or account-to-account transfers. **Note:** This feature's name is usually customized during implementation to reference a specific service.
Payments: Allow principal and interest payments	Allow Users to specify the amounts they want to pay to principal vs. interest, as appropriate for the payment type.
Payments: Allow principal and interest payments	Allows Users to indicate the principal and interest breakdown when making payments (for example, loan payments). **Note:** If the FI core automatically calculates the breakdown and does not accept User input regarding this data, disable this feature.
Prompt for PPD/CCD When Bad In Uploaded File	Prompts commercial Users to provide a PPD or CCD if an uploaded ACH file is missing a valid SEC code.

Group Features list (cont'd)

Group Feature	Description
Require view rights to account for mobile remote deposit capture	Determines which accounts appear in the Select an Account drop-down list when Users perform an mRDC. If enabled, Users must have View rights to an account, in addition to Deposit rights. If disabled, Users only need View rights.
Require withdrawal rights on account to perform stop payment	Determines which accounts appear in the Select an Account drop-down list when Users perform stop payments. If enabled, commercial Users must have Withdraw rights to an account.
Rights: Enable draft restricted	Allows for one User to set up a draft-restricted User in the Customer record. The draft-restricted User can create transactions and may edit only the dollar amount, effective date, and description of an existing template. All other required data on the draft-restricted template is pre-populated and uneditable for that User.  **Note:** The template executed by a draft-restricted User must have all required criteria (Account, Subsidiary, etc.) saved within the template prior to the draft-restricted User drafting a payment using that template. Draft-restricted Users may also schedule an ACH template or wire template to process as a transaction, and may set a fixed single or recurring payment schedule for the transaction.

Group Features list (cont'd)

Group Feature	Description
SSO: Positive Pay single sign-on	Allows commercial Users to record checks issued for purposes of validating authenticity. The Centrix Solutions Positive Pay service can use the data to identify non-listed checks as suspect.
Statement: Customer/user uses e-statement enrollment	Allows tracking of e-statement opt-in/opt-out in Q2central, if your FI lacks a vendor or core system that tracks this data. The eStatement Users Report is available as a Custom report in Q2central; contact your Q2 Relationship Manager for details.
Statement: E-statement opt in required to display statement in Q2online	Requires Users in this Group to select the e-statement option in online banking to view online statements.
Suppress account memos for landing page	Blocks account memos from being downloaded which may impact initial login times for Users with numerous accounts. This option is enabled by default.

Custom Group features

The following table describes features that can be added to the Group Features list during implementation or via a support request.

For example, if your FI purchased Business and/or Corporate Banking, features related to those products will be enabled during implementation and appear on the Group Features list in Q2central.



Note: This is not a complete list. New features are added regularly for products, features, and services.

Custom Group Features list

Group Feature	Description
Access Incoming/Outgoing Wire Alerts	Determines if Users can configure transaction alerts for incoming and outgoing wires, both domestic and international. **Note:** This feature requires that your FI purchased Corporate Banking.
Authentication challenge code: Allow one-time access via challenge code	Allows Users to set up a "secondary password" after logging in, if MFA is enabled. The system will prompt the User for the challenge code in lieu of a secure access code. However, note that Challenge codes are not considered a secure means of user access because they do not provide out-of-band (OOB) authentication. This capability is provided for backward compatibility with older versions of Q2 products.
Authentication challenge code: Require Multi-factor Authentication to edit challenge code	Allows Users to edit a "secondary password" only within an MFA-authenticated session. **Note:** The *Allow one-time access via challenge code* option must be enabled.

Custom Group Features list (cont'd)

Group Feature	Description
Authentication: Enable Access via Symantec VIP Token	Requires Users to supply a Symantec VIP token codes during login. Tokens for individual Users can be configured on the User > Symantec VIP Credential tab.
CentrixETMS Group	Enables the Centrix Exact transaction management system (TMS) Payee Match module that validates the payee on a check image against the payee name included in an issued check file. This process guards against unauthorized disbursements and fraudulent checks, beyond validating common data such as check number and check amount.
Change Global Splashboard	Enables administrative FI staff to configure widgets on the Home page. See "Home page" on page 41.
Commercial Dashboard	Intended for Business and Corporate Banking users, this feature exposes a navigation menu option called Home Page Preferences that controls what appears on the Home page. For example, some Users may want to see Quick Actions instead of a Facebook feed. **Note:** This feature requires that your FI purchased Corporate Banking.

Custom Group Features list (cont'd)

Group Feature	Description
Enable Multi-Transfer	Determines if Users can process multiple account transfers at one time via the Multi-Account Transfers tab on the Transfers page. **Note:** This feature requires that your FI purchased Corporate Banking.
Enable Multi-Wire	Determines if Business and Corporate Users can process multiple domestic or international wires in a batch on the **Commercial > Payments** page. **Note:** This feature requires that your FI purchased Corporate Banking.
Enable Payveris SSO	Allows Users to access the Payveris Bill Pay SSO.

Custom Group Features list (cont'd)

Group Feature	Description
Enable Same-Day External Transfers Credit	Allows Users to perform external (credit) transfers on the same day, if they occur before the cutoff time. This supports the recent NACHA rule that enables same-day processing of virtually any ACH payment. **Note:** Same-day external (debit) transfers will be supported in a later release.
Enable Wire Upload From Batch	Determines if Business and Corporate Banking Users can upload multiple domestic and international wires via the **Commercial > Payments > Create Payment > Payment from File** workflow. **Note:** This feature requires that your FI purchased Corporate Banking.

Custom Group Features list (cont'd)

Group Feature	Description
Foreign Exchange International Wire Access	Allows Business and Corporate Banking Users to perform real-time international wires that include a foreign exchange rate from which the USD equivalent can be calculated in real-time. **Note:** This feature requires that your FI purchased Corporate Banking.
Information Reporting - *Report name*	Provides Corporate Users with access to various reports in online banking. **Note:** This feature requires that your FI purchased Corporate Banking.

Custom Group Features list (cont'd)

Group Feature	Description
MFA: Allow secure access code delivery via SMS	Allows Users the option of receiving a SAC by text message when needed for login. SACs are sent to first-time Users, during automated Forgot Password retrieval, and as part of MFA when a User registers a new browser or computer, as well as for some sensitive transactions. The User record must include a phone number for device that accepts text to receive SACs this way.  **Note:** The FI must own Q2text (text banking) for this option to take effect. Also, delivery to non-U.S. phone numbers is not guaranteed.
Mobile authorization	Allows a transaction originator to send a mobile alert to another person who has the ability to approve a commercial transaction. The approver can approve the transaction using a PIN, or log in to Q2online to approve the transaction.  **Note:** This functionality does not apply to Q2mobility Apps.

Custom Group Features list (cont'd)

Group Feature	Description
Mobile: Allow Text Banking	Enables Q2text (text banking) on mobile devices for Users. **Note:** The FI must own Q2text for this option to take effect. Also, delivery to non-U.S. phone numbers is not guaranteed.
Navigation: Acculynk P2P	Enables the Acculynk service for person-to-person (P2P) payments, if your FI purchased that product.
OptedInToPersonalized3rdPartyMarketing	Applied at the User level, this feature is enabled by default to block end-user marketing from third-party providers when personal data is used to determine if ads appear.
OptedInToPersonalizedFiMarketing	Applied at the User level, this feature is enabled by default to block end-user marketing from the FI when personal data is used to determine if ads appear.
PFM: Account Aggregation	Enables Consumer (and sometimes Business) Users of the PFM product to link accounts held at other FIs to their online banking profile so that they can see balances and transactions for all accounts in a single view, across all devices.

Custom Group Features list (cont'd)

Group Feature	Description
PFM: Transaction Categorization and Widgets	If enabled, PFM will automatically categorize transactions for linked accounts.Users can change transaction categories, split transactions across multiple categories, create subcategories, and use PFM widgets.
Positive Pay	Enables the Positive Pay form in the navigation menu.
Recipient Upload From Batch	If your FI purchased the Corporate Banking product, this feature determines if Business and Corporate Banking Users can add new recipient records or update existing recipient records when uploading NACHA-compliant ACH files via the **Commercial > Payments > Create Payment > Payment from File** workflow.  **Note:** This feature differs from *Enable Wire Upload* so an FI can allow some Users to add recipients from batch files (for example, procurement or payroll staff) but not other Users (for example, accounting staff).

Custom Group Features list (cont'd)

Group Feature	Description
SSO: Custom application single sign on	Allows Users to access a page for the SSO application identified in the name. **Note:** This feature is usually renamed during implementation for a third-party service integrated with online banking (for example, SSO: Account aggregation single sign-on).
SSO: Live Person Chat	Enables the Live Person Chat service.

Custom Group Features list (cont'd)

Group Feature	Description
Transaction Authorization: Allow secure access code delivery via email	Allows Users in this Group the option of receiving SACs by email when required at the point of transaction authorization. If not sent by email, SACs may be retrieved through a text or voice message sent to a phone.



Note: Q2 recommends disabling SAC delivery by email, particularly for Groups with commercial functionality and/or external transfer capability. Vulnerability to email hacking due to a compromised computer is a primary reason for this recommendation. It is more secure to receive a SAC out-of-band–that is, on a device other than the one to which the User is logging in.

Custom Group Features list (cont'd)

Group Feature	Description
Transaction Authorization: Allow secure access code delivery via SMS	Allows Users in this Group the option of receiving their SACs by text message when required at the point of transaction authorization. Users must have a text-receptive phone number set up in Q2online in order to receive SACs this way. The system uses only the phone number that the User set up as a SAC target–not the one shown in Q2online contact information. **Note:** The FI must own Q2text for this option to take effect.
Transaction Authorization: Allow secure access code delivery via voice	Allows Users in this Group the option of receiving SACs by voice message when required at the point of transaction authorization. Users must have a valid phone number set up in Q2online in order to receive SACs this way. The system uses only the phone number that the User set up as a SAC target–not the one shown in Q2online contact information. **Note:** The FI must own the Q2voice product for this option to take effect.

Custom Group Features list (cont'd)

Group Feature	Description
Transaction Authorization: Enable Transaction Authorization via Secure Access Code	Requires Users in this Group to supply a SAC for specified transaction types. If this is enabled, Users attempting to authorize one of these transactions are required to receive a SAC via email, SMS (text), or voice message and provide it during the authorization session. If the end user is unable to supply the code, the transaction remains in a draft state. Transaction Authorization is recommended for commercial Groups and those with external funds transfer capabilities. **Note:** If both this feature and Transaction Authorization via Symantec Token are enabled, the VIP token code acts as the default authorization method for all end users with a Symantec Credential ID enabled in Q2central. Quick Transfers cannot be completed when a SAC is required.

Custom Group Features list (cont'd)

Group Feature	Description
Transaction Authorization: Enable Transaction Authorization via Symantec VIP Token	Requires Users in this Group to supply a Symantec VIP token code for specified transaction types and to display the Symantec VIP Credential tab on the User record. If this is enabled, Users attempting to authorize one of these transactions are required to supply a Symantec VIP token during the authorization session. If the User cannot supply the token code, the transaction remains in a draft state. Transaction Authorization is recommended for commercial Groups and those with external funds transfer capabilities.  **Note:** If both this feature and Transaction Authorization via Secure Access Code are enabled, the Symantec token acts as the default authorization method for all Users with a Symantec Credential ID enabled in Q2central. See "User Symantec VIP Credential tab" on page 221. Quick Transfers cannot be completed when an Authorization Token is required.

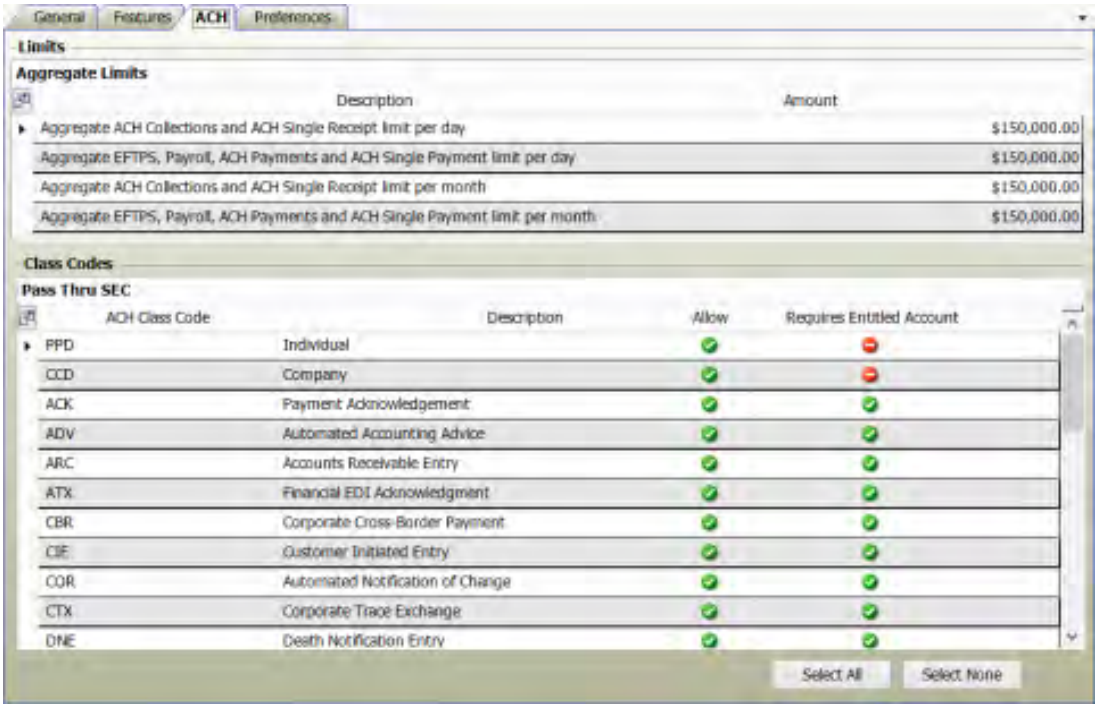
Custom Group Features list (cont'd)

Group Feature	Description
View Wire Activity	If your FI purchased Corporate Banking, this feature determines if Business and Corporate Banking users can access the Wire Activity page to display incoming and outgoing wires, both domestic and international, regardless of their source as long as the wire was processed via the real-time wire processor that is part of the Q2platform.

Group ACH tab

The Group ACH tab displays ACH-related parameters for any Group with ACH capabilities. Skip this tab if a Group cannot originate ACH transactions.

Group ACH tab



Group ACH tab — Aggregate Limits section

Use the Group General tab to set limits for each transaction type for all Customers that are part of the Group. Use the Aggregate Limits section of the Group ACH tab to set limits for accumulated ACH Transactions Types for commercial Customers.

For aggregate limits, the system checks the Customer transaction limit every time a User drafts a transaction, and blocks transactions that would exceed the per-transaction maximum. Users can draft as many transactions as they wish for any available banking date, as long as each transaction's amount does not exceed the Customer per-transaction maximum.

When a transaction is authorized, the system checks the Customer's daily and monthly limits and type-specific limits. It uses the Process Date to compare activity to daily limits; that is, the system prevents authorization of transactions that exceed the limits for the day on which they are to be processed. Until an authorized transaction runs through the Process Wizard, Users can cancel it to make room within the limit balance for a different transaction.

For example, if a transaction is authorized for $100,000 today and the Process Date is two days from now, the aggregate limit is not checked until the Process Date assigned when the transaction was created/authorized.

Note the following details about aggregate limits:

- The system will check limits multiple times, including when a transaction is first drafted and then later when the transaction is authorized.
- Setting aggregate limits is optional, but recommended.
- Limits are specifically tied to a transaction's Process Date; it does not matter what date the transactions are authorized.
- If a value is set to $0.00 in the Aggregate Limits section of the Group ACH tab, it will not affect transaction limits set on the Group General tab.
- To block ACH transactions entirely, set the aggregate limit to $0.00.
- Aggregate limits trump ACH settings on the Group General tab.
- When setting an aggregate limit for a Group, provide a buffer by choosing a limit amount that is comfortably greater than the highest historical aggregate amount by the highest-transacting Customer in the Group.
- Some FIs prefer to set Aggregate Limits at the Customer level only.

For details, see the *Q2central Transaction Processing Guide*.

Aggregate Limits options

Description	Amount
Aggregate ACH Collections and ACH Single Receipt limit per day	In the Amount column, specify the maximum combined daily total that each Customer in this Group may draft for the listed debit types.
Aggregate ACH Collections and ACH Single Receipt limit per month	In the Amount column, specify the maximum combined monthly total that each Customer in this Group may draft for the listed debit types.

Aggregate Limits options (cont'd)

Description	Amount
Aggregate EFTPS, Payroll, ACH Payments and ACH Single Payment limit per day	In the Amount column, specify the maximum combined daily total that each Customer in this Group may draft for the listed credit types.
Aggregate EFTPS, Payroll, ACH Payments and ACH Single Payment limit per month	In the Amount column, specify the maximum combined monthly total that each Customer in this Group may draft for the listed credit types.

Group ACH tab — PassThru SEC section

Use the PassThru SEC section of the Group ACH tab to choose which SEC codes end users in this Group can use in an ACH PassThru file. Skip this section if this Group cannot submit ACH PassThru files.

PassThru SEC columns

Column	Description
ACH Class Code	The SEC codes that have been configured in your FI's database as acceptable in ACH PassThru files.
Description	The description associated with the ACH Class code.
Allow	Enable end users in this Group to submit ACH PassThru files containing this SEC code (optional).

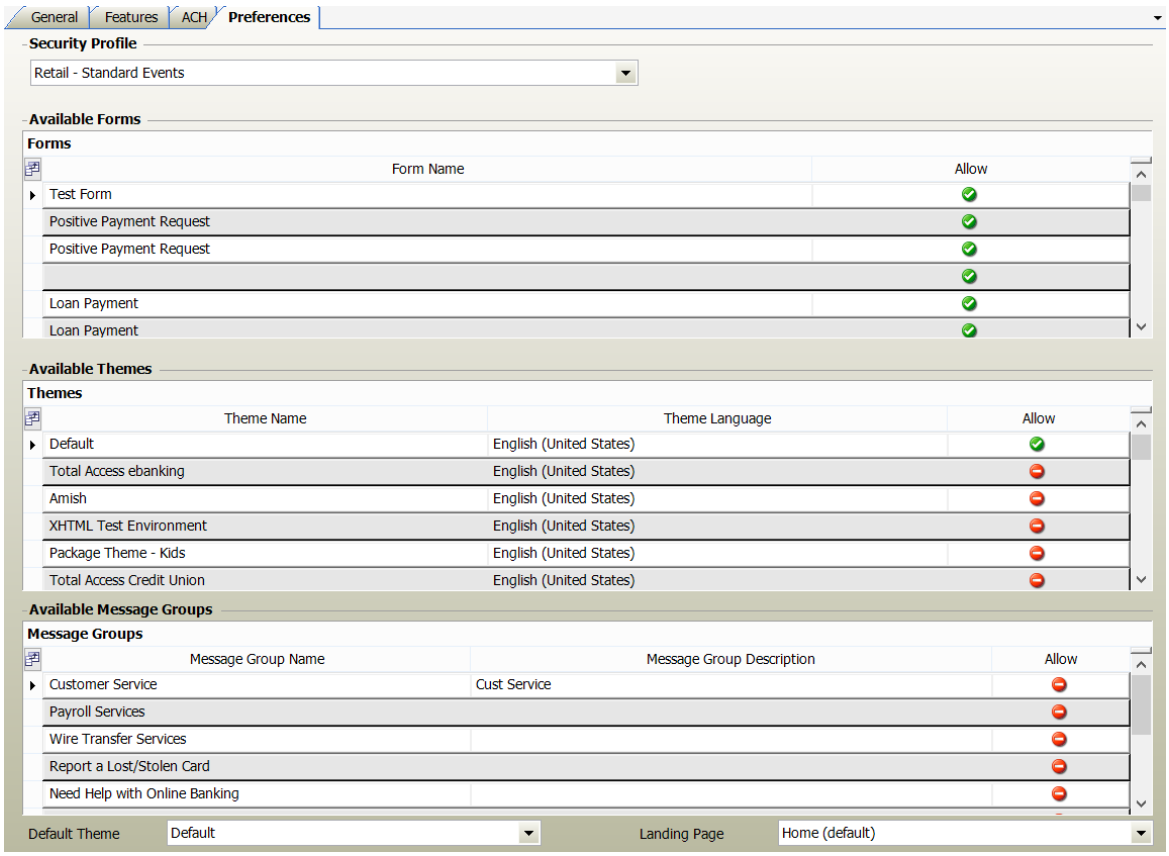
PassThru SEC columns (cont'd)

Column	Description
Requires Entitled Account	If the Allow column is enabled, enable this column to require that a User submitting an ACH PassThru file containing the SEC code have the credit or debit side of at least one batch involve at least one entitled account. An entitled account is one that is housed within your FI, to which this end user has the appropriate rights (for example, withdrawal rights if this is an outgoing credit) as set on the User > Rights tab and User > Account Management tab. If *Requires Entitled Account* is enabled, the system rejects an ACH PassThru file at submission if it includes this SEC code and does not meet the entitlement requirements.

Group Preferences tab

The Group Preferences tab controls some aspects of the online banking experience, such as themes that change the look and feel of the user interface. Preferences set here cannot be modified at the Customer or User level.

Group Preferences tab



Security Profile section

Select the type of alerts you want to make available to online banking end users in this Group.

Options may include:

- Commercial - Standard Events
- Consumer Banking - Standard Events
- Corporate Banking Alerts (includes Commercial Standard Alerts)
- Consumer Banking - All Events

Each alert has a setting (**Forced**, **On but not forced**, or **Optional**) that determines if end users can configure the alert in online banking, as decided upon by the FI during implementation. To change a default setting after implementation, contact Q2 Software.

For a list of security alerts, refer to the *Q2central Reference Lists* document.

Available Forms section

This section lists forms available for end users to complete in online banking. Forms here are added by Q2 during implementation and may include Micro Deposit forms or similar forms. This section usually appears on the Services > Other Services menu in online banking, unless an FI asked to place it elsewhere during implementation.

Available Themes section

In addition to the standard user interface, FIs can purchase additional themes that affect the text, colors, and graphics that end users see in online banking. Each template that affects how the user interface appears to end users is a theme, and end users themselves may select from among available themes. For example, themes may appeal to teens, young children, or the visually impaired; the underlying Customer, User and account data is unaffected.

To give end users in this Group the ability to select a theme from within online banking, enable the Allow column for that theme.

Available Message Group section

A Secure Messaging group is a set of CSR Users who receive messages sent by end users. You can control the Groups that have access to different types of secure messages in the Available Message Group section of the Group window's Preferences tab.



Note: To manage Secure Message permissions for Groups, you must be assigned a CSR Role with the *ADMINISTRATION: Message Group Members permission* enabled.

Setting a default theme for a Group

By selecting a value in the Default Theme field at the bottom of the Group Preferences tab, you apply the same theme as a default for all Customers and Users in a Group.

Note: To minimize end user confusion, Q2 recommends changing the default theme only when creating a Group of new end users, or if you are retiring a theme that was previously used as the default theme.

Setting a landing page for a Group

By selecting a value in the Landing Page field at the bottom of the Group Preferences tab, you can set the default landing page in online banking for all Customers and Users in a Group.

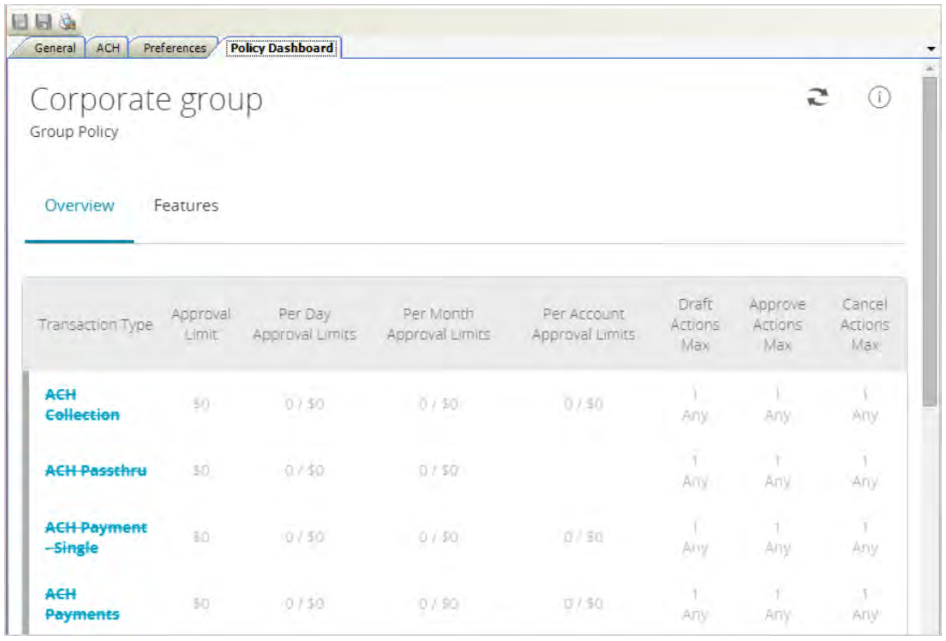
A *landing page* is the first page that appears after a User logs into online banking. Unless otherwise specified by an FI during implementation, the landing page is the Home page that displays account names, account numbers, balances, and an Account Summary graph.

Group Policy Dashboard tab overview (Corporate Banking)

The Group Policy Dashboard tab contains an Overview tab that allows you to set the limits for transaction types used by Corporate Groups.

Tip: This tab appears if you select a Corporate Group record in the Q2central workspace. For Consumer and Business Banking Groups, use the General tab to set transaction rights and limits, and then use the Features tab to enable features instead.

Group Policy Dashboard tab overview



The following outlines the Transaction Types available for Corporate Banking Groups in the Overview tab:

- ACH Collection
- ACH Passthru
- ACH Payment - Single
- ACH Payments
- ACH Receipt - Single
- Change Address
- Check Reorder
- EFTPS
- Payroll
- Stop payment
- Transfer - Internal
- Wire - Domestic
- Wire - International

Selecting a Transaction Type to display the restrictions established for that type and allows for new rules to be created

Note: Group Transaction Types are established and maintained by the FI. This level of management is never seen by the end user.

Group Policy Dashboard tab features (Corporate Banking)

The Group Policy Dashboard tab contains a Features tab that allows access to Corporate Banking features in Q2online and Q2mobility Apps. These features are similar to those set for non-Corporate users.

Note: Group Features are established and maintained by the FI. This level of management is never seen by the end user.

Group tasks

Group records can be added, edited, viewed, and deleted from this option. This section contains commonly performed tasks for working with Group records.

Note the following details about working with Groups:

- You must perform a search to display records on the Groups search grid, unless you saved a default search.
  See "Searching for information in Q2central" on page 348.
- You can customize most information displayed on the Groups search grid by using the Field Chooser. See "Using the Field Chooser" on page 349.
- If your FI uses the Group Access Mapping feature, the CSR Team to which you are assigned controls your ability to manage records in certain Groups. See "Group Access Mapping" on page 46.

This section contains the following topics:

- "Adding a Group" on page 179
- "Displaying a Group" on page 179
- "Editing a Group" on page 179
- "Copying a Group" on page 180
- "Deleting a Group" on page 180
- "Enabling features for a Group" on page 181
- "Enabling mobile remote deposit capture (mRDC) for a Group" on page 181
- "Viewing a Group's Customer records" on page 182
- "Sending a Secure Message to a Group, Customer, User, or Login ID" on page 182

Adding a Group

This section describes how to add a Consumer or Business Banking Group. To add a Corporate Banking Group, click the **User Management > Corporate** option in the workspace tree.

To add a Group

1. In the workspace tree, click **User Management > Groups** to display the Groups list.
2. In the Groups list, right-click and click **New Group**.
3. When a message appears to ask if the new Group will have Corporate Banking features, click **Yes**, **No**, or **Cancel**.
4. In the Group Name box, enter a name for the Group.
5. In the Group Type box, indicate whether the Group is **Consumer** or **Business**.
6. Enter information directly in each tab, saving each tab as you complete it.
7. Click **Close and Save**.



Note: If your FI uses Group Access Mapping, you will be prompted to update CSR Teams to ensure that the necessary CSRs can access records in the Group. See "Group Access Mapping" on page 46.

Displaying a Group

To display the Group window

1. In the workspace tree, click **User Management > Groups** to display the Groups list.
2. Double-click the row for the Group whose details you want to view.

Editing a Group

Editing a Group applies all changes to all members in the Group.

To edit a Group

1. In the workspace tree, click **User Management > Groups** to display the Groups list.
2. In the Groups list, select the Group record you want to edit, right-click the record and select **Edit Group**.

3. Make changes directly to the information on the tabs, saving each tab as you complete them.
4. On the toolbar, click **Save and Close**.

Copying a Group

When creating a Group you can use the Copy Group command. The Corporate Banking attribute must be assigned at the time the Group is copied; it cannot be assigned after the Group is created.

To copy an existing Group

1. In the workspace tree, click **User Management > Groups** to display the Groups list.
2. In the Groups list, right-click the Group you want to copy and click **Copy Group**.
3. In the Copy Group dialog box, enter the Group name in the **Name of new Group** field.
4. If the new Group is a Corporate Banking Group, click the **Make the new Group a Corporate Group** option.
5. In the Group dialog box, complete the following:
    - In the General tab, the Group Name is automatically populated; select the **Group Type**.
    - In the ACH tab, specify any ACH Limits and Class Codes that may differ from the original Group.
    - In the Preferences tab, configure any differences in the Security Profile, Available Forms, Available Themes, and Default Theme from the original Group.
    - Complete other tabs as needed.
6. Click **Save**, then close the Group dialog.
7. In Q2central, assign one or more Customers to the new Group.

Deleting a Group



Note: Before you can delete a Group, you must delete any Customers in the Group or move them to another Group.

To delete a Group

1. In the workspace tree, click **User Management > Groups**.
2. In the Groups list, right-click the Group you want to delete and click **Delete Group**.
3. The Delete Group window displays a confirmation for the deletion of the selected Group. Click **Yes** to delete the Group.

Enabling features for a Group

To enable a feature for a Group

1. In the workspace tree, click **User Management > Groups**.
2. Search for and select the Group for which you want to enable features.
3. Right-click the Group record and click **Edit Group**.
4. Click the **Features** tab.
5. Click the **Description** column header to alphabetize the list.
6. Click an item in the Group Features pane to place the focus arrow beside the item.
7. In the Enabled column, click the icon to enable each feature that members of this Group can use.
8. Click **Save** before proceeding to another tab or closing the window.

Enabling mobile remote deposit capture (mRDC) for a Group

To enable mRDC for a Group:

1. In the workspace tree, click **User Management > Groups**.
2. Search for and select the Group for which you want to enable mRDC.
3. Right-click the Group record and click **Edit Group**.
4. Click the **Features** tab, and click the **Description** column header to alphabetize the list.
5. Locate and click the Enable icon for the **Mobile: Allow Mobile Capture Access** feature.
6. Click **Save**.

Viewing a Group's Customer records

To view the Customer records that belong to a Group

1. In the workspace tree, click **User Management > Customers**.
2. At the top of the Customer search grid, select:
   a. **Group Name**
   b. **Contains**
   c. *The name of the Group*
3. Click **Search**.



Note: If your FI uses the Group Access Mapping feature, the CSR Team to which you are assigned controls your ability to display Customer records for a Group. Some values may appear masked. See "Group Access Mapping" on page 46.

Sending a Secure Message to a Group, Customer, User, or Login ID

To learn more about secure messages, see "Secure Messaging" on page 297.

To send a secure message to a Group, Customer, User, or Login ID

1. In the User Management section of the workspace tree, select the audience (Groups, Customers, Users, or Logins) for which you want to send a message.
2. Search for and select the specific Group, Customer, User, or Login you want to receive the message.



Note: If you select a Group or Customer, the message will go to all Users under the selected Group or Customer.

3. Right-click and select **Send Secure Message to *<audience>***, or press **F10**. The Broadcast Message window appears.
4. In the **From** box, select the Secure Messaging group that you want to appear as the "sender" of the message.
5. In the **Subject** box, summarize the title of the message.
6. In the **Message Text** box, type the message you wish to send.

Note: Q2central does not have a spell check feature, but you can compose a message in Microsoft Word, apply spell check, and then copy and paste text into the Message Text box.

7. (Optional) Click add to attach a file to the message.
8. Click **Send**.

Note: To send the same message to all Groups, Customers, and Users simultaneously, refer to "Sending a secure broadcast message to all end users" on page 310.

CHAPTER 13: WORKING WITH CUSTOMERS

In Q2central, every Group is made up of Customers. Customers can be configured as Consumer, Business, or Corporate Banking Customers. These designations help an FI provision both Customers and Users for certain rights and specific limits that allow for better user management across the Q2platform.

This chapter discusses Consumer and Business Customers and how this provisioning impacts the end user access to online banking. If your FI uses the Corporate Banking product, be sure to refer to "Corporate Banking Policies and Users" on page 93 to learn how Customers are handled in Corporate Banking.

This chapter includes the following sections:

- "Customer overview" on page 184
- "Customer reference" on page 186
- "Customer tasks" on page 205

Customer overview

You can use the Customers page to search for and display Customers established at your FI. A Customer is an umbrella record to which Users and Logins belong, as described earlier in "User management definitions and relationships" on page 87.



Note: You must perform a search to get records to appear, unless you saved a default search for this option. See "Searching for information in Q2central" on page 348.



Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.



Note: If your FI uses the Group Access Mapping feature, the CSR Team to which you are assigned controls your ability to manage Customers. You may also notice that some Customer details are masked. See "Group Access Mapping" on page 46.

Customer accounts overview

Unless your FI uses Advanced Enrollment (also called *End-to-End Enrollment*), accounts are automatically added when a Customer completes the enrollment process successfully by validating personal data stored on the FI core, along with other demographic information.

Note the following details about Customer accounts:

- An account will disappear from view in Q2central if it is closed on the core, is linked by a customer information file (CIF), and an FI provides a closed account list to Q2 regularly via the host interface or a batch file.
- Depending on how the core handles returning accounts when the call for retrieval is made, an account may continue to appear until it is manually removed from the core, or a closed account batch file script is used.

There are two ways to link accounts to Customers:

- Linking through CIF
- Linking through account number

Linking through CIFs

CIF is a digital filing system used in the banking industry for maintaining Customer data for all related accounts including separate savings, safe deposit boxes, CDs, IRAs, mortgages, and personal loans. CIFs typically contain demographic data, along with member numbers; they are commonly used to link Customers to accounts. These details can also be used to generate targeted customer lists for marketing purposes.

The recommended way to add accounts for which a Consumer Banking Customer is the primary account holder is to link accounts through internal CIF. With this method, FI staff asks the system to display a list of all accounts listed on the core for this Customer's CIF, then manually selects which account(s) to add to the Customer record. Benefits of this method include convenience and accuracy, as well as that new accounts can be easily added to the Customer/User.

If FI staff chooses to Link Accounts by Internal CIF, when an account is severed from the CIF record on the host, it is also removed from the online banking database without additional work by FI staff. If this option is not selected, then accounts linked through CIF behave similarly to those linked through account number.

Note: This method is only recommended for Consumer Banking Customers.

Linking through account number

This method allows FI staff to add accounts for which the Customer is not the primary account holder. Use this method for secondary account holders for the purpose of making online deposits to that account.

FI staff manually types the account number and selects the appropriate account type from the drop-down list to add it to the Customer record. Even if the account is severed from the CIF of the primary account holder, this account remains available to the secondary unless FI staff takes explicit action.

If you select this method when adding an account to the primary account holder's Customer record, the system presents you with all accounts for the CIF and offers you the opportunity to add more accounts and link through the CIF.

Note: This method is recommended for commercial Customers so that Users do not automatically inherit everything on the primary account holder's CIF.

Customer reference

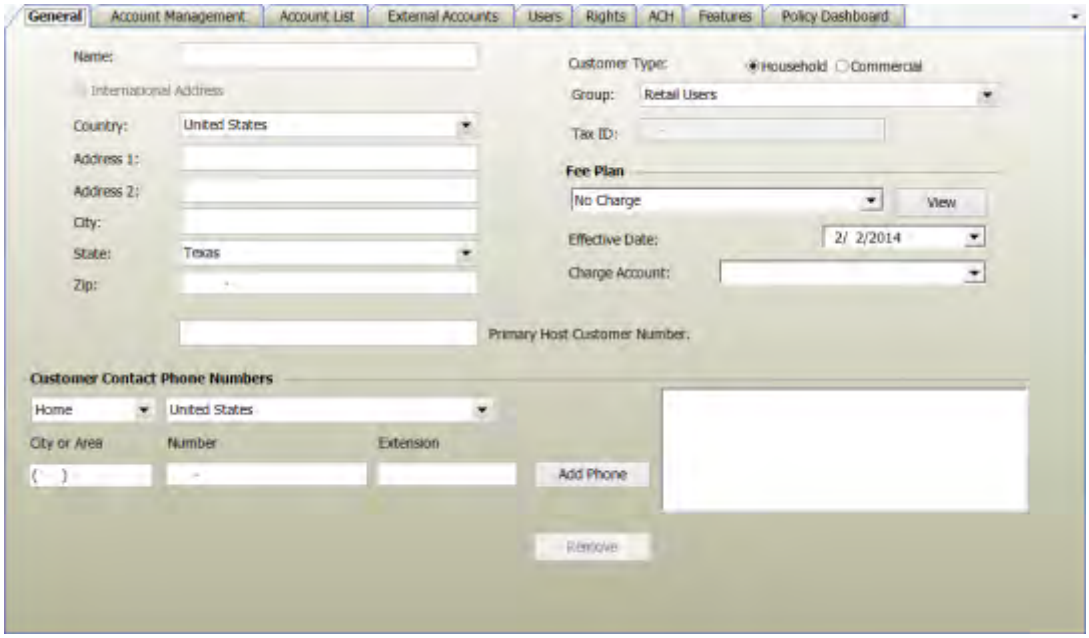
The Customer tabs are where you view, add, edit, delete, or send a secure message to a specific Customer. The following sections provide a detailed reference for each of the tabs in the Customers option.

If your FI purchased Corporate Banking, references to Corporate-specific settings are also included.

Customer General tab

The Customer General tab stores detailed contact information as well as any fee plan that may be applicable.

Customer General tab



Customer General tab options

Option	Description
Name	The name of an organization, a family, or an individual. End users do not see this name in online banking, but it may appear on fee statements, reports, and other outputs.
International Address	Indicates if this is a non-U.S. address. This check box can be selected only when creating a new record; it affects whether a State or Province field appears. (Some FIs may use this information for end-to-end enrollment that authenticates end users requesting access to online banking.)

Customer General tab options (cont'd)

Option	Description
Address fields	The mailing address for this record. Address 2 is not a separate address; it is a continuation of Address 1, if needed. The Country box contains the list of countries your FI requested at implementation. Unless your FI requested that the Q2 database be updated regularly with information from the core, this is not necessarily the same as the information on the core.
Customer Type	*Household* indicates that a Customer is an individual or family conducting personal activity that use the Consumer version of online banking. *Business/Corporate* is a commercial entity or organization, which may include Business Banking or Corporate Banking end users. **Note:** If this field is set to *Business/Corporate*, the Tax ID field should display the main Tax ID number (TIN) for use in ACH and/or Wire transactions.
Primary Host Customer Number	The primary identification number (PIN) that provides access to an FI's core if it is an Open Solutions, Inc. (OSI) core that requires a host PIN to pull back data. Any User records added to the Customer record will inherit this value. **Note:** This value is used only to connect information and serve as an additional authentication method when pulling data in real time. It will not overwrite values on the core.

Customer General tab options (cont'd)

Option	Description
Group	The name of the Group to which this Customer belongs. **Note:** You must have sufficient rights to assign a Customer to a Group. **Caution:** If you change the Group to which an existing Customer belongs, the Users and Logins belonging to that Customer may lose rights to functionality and transaction limits, if moved to a more restrictive Group. To learn more about the impacts of switching Groups, see "Changing Customers between Corporate and non-Corporate Groups" on page 206 .
Tax ID	The Employer ID Number (EIN). (Social Security Numbers are stored at the User level, but EINs are stored at the Customer level.) Be aware that subsidiaries are managed in Q2online and Q2mobility Apps only, and not in Q2central. A subsidiary is an alternate company profile that can be created and then used when creating payment or templates in online banking for a business that has multiple entities. For example, a holding company can create a subsidiary for each of the company's real subsidiaries. An accountant who pays taxes on behalf of clients can create a subsidiary for each client.
Fee Plan	The fee plan to which this Customer is currently assigned, if fee plans are enabled at the FI. Click **View** to see fee plan details.

Customer General tab options (cont'd)

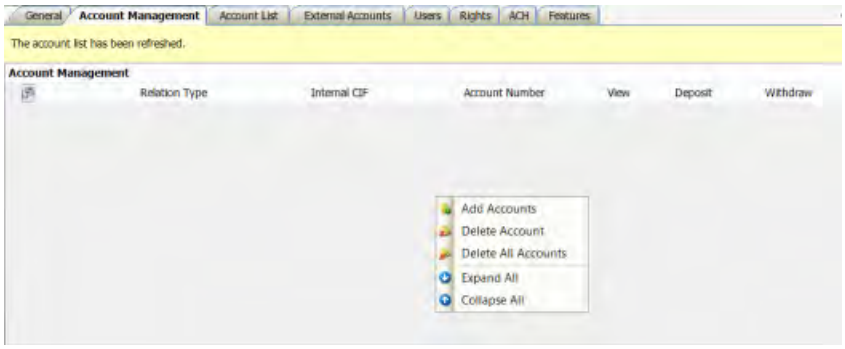
Option	Description
Effective Date	If a Customer is associated with a fee plan, this is the date when the Customer was first linked to the fee plan. **Note:** This is not necessarily the first date when costs began to incur; the FI may have set up a cost-free introductory period, and fee plans only bill for complete calendar months.
Charge Account	The account that will receive the debits created when fees are processed at month-end. This field is optional and is only required if the FI wants to charge the Customer for fees. **Tip:** You may want to inform the Customer this account will be used for all charges incurred by any account that the Customer owns. For example, if a Customer performs a stop payment on a check written against Account 1234 (and is charged a fee for Stop Payments), the fee will be deducted from Account 1235, if that is the Charge Account specified here.
Customer Contact Phone Numbers	
Phone Numbers	All phone numbers on record for the Customer. Click in the rightmost pane to view country information for each number listed. The Country box contains the list of countries your FI requested at implementation. If the list of phone numbers is long, you may need to scroll to view them all. **Note:** These phone numbers are not used to deliver secure access codes (SACs) or system alerts. To update that information, use the User > Secure Access tab instead. See "User Secure Access tab" on page 222.

Customer Account Management tab

The Account Management tab allows you to set Customer-level view, deposit, and withdrawal permissions to all accounts associated with this Customer. Use this tab to add an account housed at another FI, if this Customer belongs to a Group with the External Transfers option enabled.

Tip: If you mistakenly delete an account, click **X** to close the Customer window, then select No when asked whether you want to save changes.

Customers Account Management tab



Account Management shortcut menu options

Menu Option	Description
Add Accounts	Adds an Account to the Customer record. See "Using the Add Account wizard" on page 210.
Delete Account	Deletes the selected account.
Delete All Accounts	Deletes all accounts associated with this Customer.

Account Management shortcut menu options (cont'd)

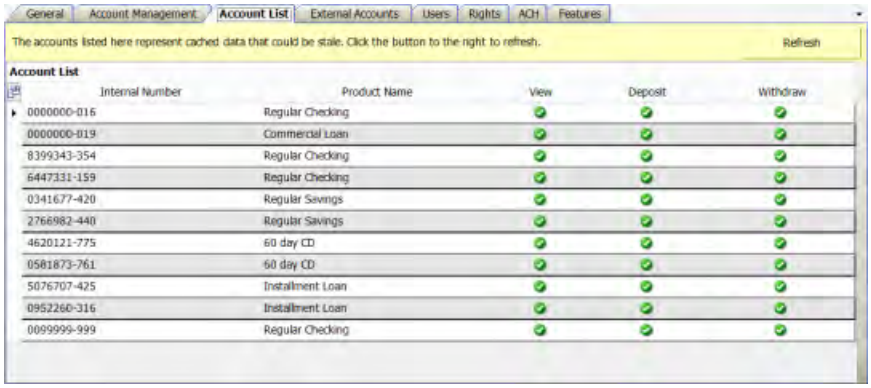
Menu Option	Description
Expand All	Displays the Field Chooser selections and settings for all listed accounts. Settings include Override, View, Deposit, and Withdraw permissions. Override is available only when accounts have been related to the Customer record by CIF, so that multiple accounts are listed in the expanded view. Enabling Override allows you to set separate permissions on each account (however, first you must save the Customer window with Override enabled). **Note:** Ignore the Override switch if the CIF-linked accounts you are adding share identical permissions for this Customer.
Collapse All	Returns to the default view.

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

Customer Account List tab

The Customer Account List tab is for verification only. It allows you to see a streamlined list of on-us accounts associated with this Customer and the permissions for each account. Use this to double-check your work on the Accounts Management tab.

Customer Account List tab



Tip: Click **Refresh** to display updated account information.

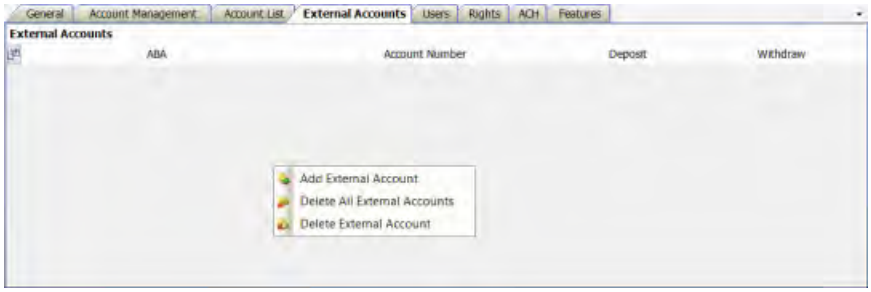
Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

Customer External Accounts tab

The micro deposits process may be available to end users to provide information about external accounts they wish to add to their profiles. When end users successfully complete that process, the external account is automatically added as a transfer destination in the Fund Transfer Account field in online banking on the External Accounts tab of the Customer record.

It is also possible for CSRs to set up external accounts in Q2central. For example, if an end user has difficulty adding an account, or if the FI is configured to prevent end-user addition of external accounts.

Customer External Accounts tab



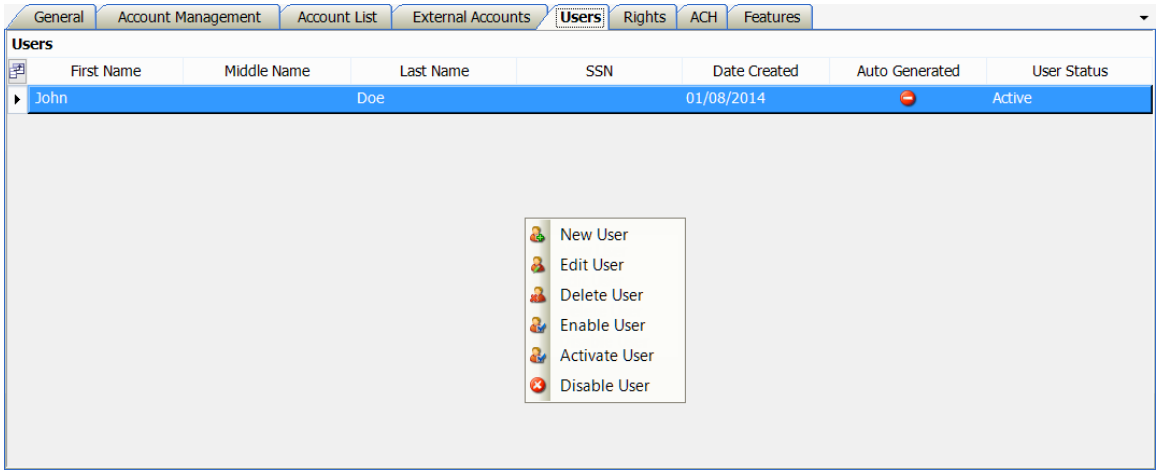
External Accounts shortcut menu options

Menu Option	Description
Add External Account	Adds an external account for the Customer. See "Using the Add External Accounts wizard" on page 211.
Delete All External Accounts	Prevents all external accounts listed here from being accessed via your FI.
Delete External Account	Prevents the selected external account from being accessed via your FI.

Customer Users tab

FI staff can use the Customer Users tab to manage Users linked to a Customer. FI staff must add a Customer's first User (typically the primary account holder). An FI may choose to empower certain administrative-level Users to add Users to the Customer; that right is granted on the User > Features tab; see "Enabling features for a User" on page 247.

Customer Users tab



To access a menu where you can manage Customer Users, right-click anywhere on the Customer Users tab to display a shortcut menu.

Customer Users tab right-click menu options

Option	Description
New User	Display the New User window.
Edit User	Display the User window. See "Editing a User" on page 247. **Tip:** You cannot save a User record if a User has pending transactions that would be impacted by limit changes. See "User Account Management tab" on page 224.
Delete User	Permanently delete the selected User. When prompted to confirm the deletion of the User, click **Yes**. **Caution:** Deleting a User also deletes associated Logins. Also, Q2central will prevent you from deleting a primary User record linked to pending transactions.
Enable User	Allow a User to log in or move funds. See "Enabling a User" on page 252.

Customer Users tab right-click menu options (cont'd)

Option	Description
Activate User	Allow a User to log in. See "Activating a User" on page 251.
Disable User	Prevent a User from logging in or moving funds. See "Disabling a User" on page 252.

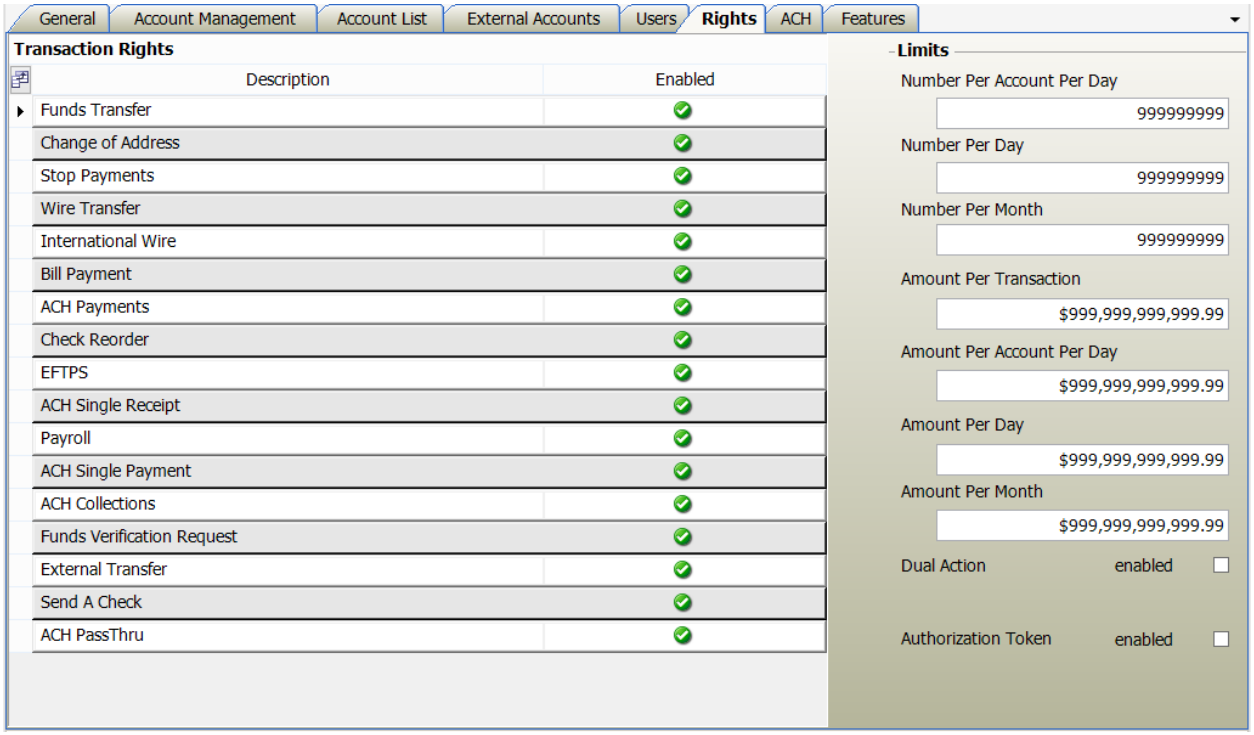
Customer Rights tab

Until changes are made, the Customer Rights tab displays the transaction types and associated limits for each enabled transaction type, as set at the Customer's Group level. On this tab, you can disable rights or reduce transaction type limits. The CSR may choose to reduce limits for a single User or even remove access to certain transaction types.

Caution: Reducing transaction type limits here at the Customer level will affect all Users linked to the Customer.

Tip: Save periodically while setting rights and limits.

Customer Rights tab



Transaction Rights pane

In the Enabled column, click the icon to enable each transaction type that Users belonging to this Customer can perform. This setting will impact which options appear on the Navigation menu in online banking. For example, enabling Payroll here means it will appear as a menu option in online banking, while end users linked to a different Customer will not see the Payroll option.

Note the following details about transaction rights:

- The options available here are inherited at the Group level.
- A transaction right takes effect as soon as the right is enabled but can be used only if you provide non-zero amounts for that transaction type in the Limits pane.

Limits pane

Click an item in the Transaction Rights pane to place the focus arrow beside it. Complete the Limits boxes with non-zero amounts for just the transaction type in focus.

Options displayed in the Limits pane vary depending on the transaction type selected in the Transaction Rights pane. Limits are assigned based on the transaction type selected. These are approval limits; they can be further lowered (but cannot be raised) at the User level.

Provide a value other than 0 for each field. Otherwise, Users within this Customer cannot use the associated transaction type.

- Number per Account per Day
- Number per Day
- Number per Month
- Amount per Transaction
- Amount per Account per Day
- Amount per Day
- Amount per Month

Dual Action

Select the Dual Action check box to require that two Users within this Customer record approve transactions of the transaction type in focus. This setting can be overridden by FI staff at the User level, if necessary. Note that unlike most rights that automatically inherit a setting from the parent Group, this right can be enabled even if it is not enabled for the Group.

Authorization Token

Select the Authorization Token check box to require that a Symantec VIP token or secure access code (SAC) be provided every time a User within this Customer approves a transaction of the transaction type in focus. This setting can be overridden by FI staff at the User level, if necessary. Also, note that unlike most rights that automatically inherit a setting from the parent Group, this right can be enabled even if it is not enabled for the Group.

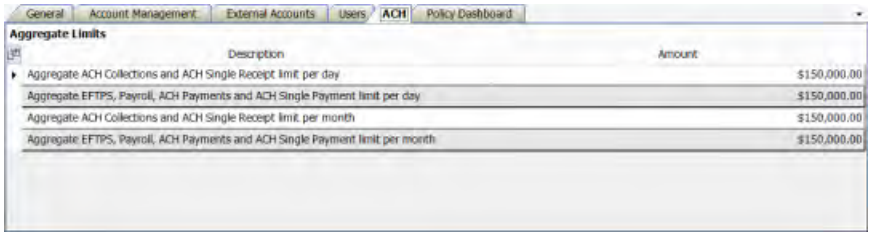


Tip: Save the settings before proceeding to another tab or closing the window.

Customer ACH tab

The Customer ACH tab displays a list of ACH-related parameters that need to be set for Customers with ACH capabilities, as inherited from the Group ACH tab. Skip this tab for Customers that do not originate ACH transactions.

Customer ACH tab



Aggregate Limits

On the Rights tab, you set limits for each individual transaction type; in the ACH tab you set limits across multiple transaction types. Selections in this section are optional; if left at $0.00, they do not affect the transaction limits set on the Rights tab. You cannot set higher levels here than what have been set at the Group level (unless the Group level specifies $0.00). To learn more, see "Group ACH tab — Aggregate Limits section" on page 170. .

Aggregate Limit Settings

Aggregate Limit	Description
Aggregate ACH Collections and ACH Single Receipt limit per day	The maximum combined daily total that Users at this Customer may authorize for the listed debit types.
Aggregate EFTPS, Payroll, ACH Payments and ACH Single Payment limit per day	The maximum combined daily total that Users at this Customer may authorize for the listed credit types.
Aggregate ACH Collections and ACH Single Receipt limit per month	The maximum combined monthly total that Users at this Customer may authorize for the listed debit types.
Aggregate EFTPS, Payroll, ACH Payments and ACH Single Payment limit per month	The maximum combined monthly total that Users at this Customer may authorize for the listed credit types.

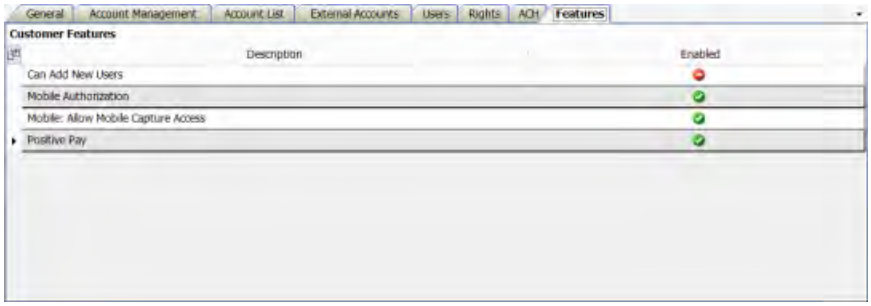
Note: Changes on this tab must be saved before making other changes on the Customer record.

Customer Features tab

The Customer Features tab displays a list of capabilities that can be enabled for this Customer. Note these details about this tab:

- Features that appear on this tab depend on features enabled at the Group level (see "Group Features tab" on page 143).
- Additional features may appear that are custom for your FI, such as *Enable Payveris SSO*.
- For Corporate Banking Customers, configure Customer Features on the Policy Dashboard instead. See the *Business and Corporate Banking User Guide* for details.
- There are exceptions regarding how rights are inherited for Business and Corporate Banking features that warrant extra security, such as Multi-Wires. See "Feature right exceptions" on page 107.

Customer Features tab



The following table includes default features that may appear on this tab.

Customer Features tab options

Option	Description
Allow one-time recipients	This feature allows commercial users to create a one-time recipient for a single payment. The information will not be saved as a Recipient record like regular, repeat recipients, nor will it appear on the Recipient Management page in online banking.
Business Payments for UUX	Determines if the Payments option appears in the Commercial menu in online banking.

Customer Features tab options (cont'd)

Option	Description
Mobile: Allow Mobile Capture Access	This setting enables mobile remote deposit capture (mRDC) for this Customer, assuming the FI has an mRDC vendor.
Mobile: Mobile Authorization	Enabling this setting allows a transaction originator to send a mobile alert to another person who has the ability to approve a transaction, typically for Dual Action scenarios. The approver can either provide a mobile authorization code (MAC) to approve the transaction when receiving the alert via telephone, or log in to online banking to approve the transaction.
Rights: Can Add New Users	Enable this item to allow the Customer to establish one or more Users at the Customer who are authorized to add other Users to the Customer. Individual administrative Users are enabled on the Features tab of their User records. Enabling this feature may reduce security slightly, but offers great convenience to both the FI and the Customer. This is typically granted to commercial Customers; however, granting this is at your FI's discretion.
PFM: Account Aggregation	Enables Consumer Banking (and sometimes Business Banking) users of the PFM product to link accounts held at other FIs to their online banking profile so that they can see balances and transactions for all accounts in a single view, across all devices. **Note:** Business Banking Customers may want this feature and the *PFM: Transaction Categorization and Widgets* feature (described next) set differently for various Users, depending on how much information they want to make accessible.
PFM: Transaction Categorization and Widgets	If enabled, PFM will automatically categorize end-user transactions for linked accounts. End users can change transaction categories, split transactions across multiple categories, create subcategories, and use PFM widgets.

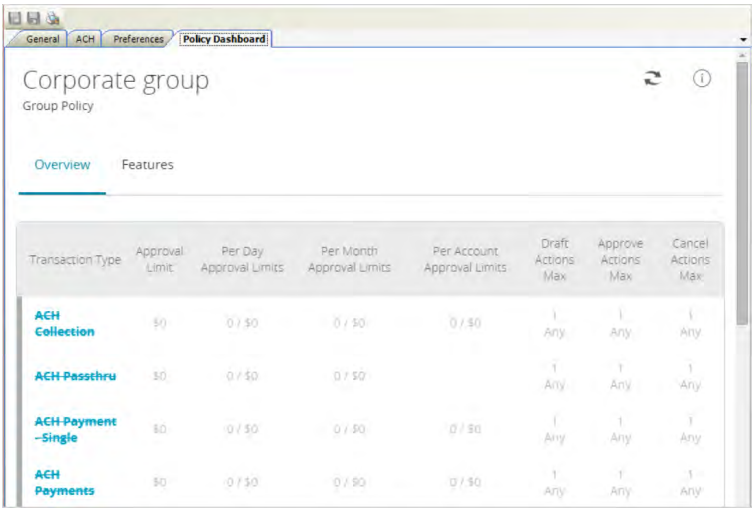
Customer Features tab options (cont'd)

Option	Description
SSO: Custom application single sign on	This feature may have a different name, as assigned during implementation. Enable this feature to allow this Group to access the window for the SSO application identified in the name.
SSO: Positive pay single sign on	Enable this feature to provide commercial users with access to an automated fraud detection tool that matches the account number, check number, and dollar amount of each check presented for payment against a list of checks previously authorized and issued by the company.
Suppress account memos for landing page	This option is enabled, by default, to block account memos from being downloaded which may impact system response time for Users that have numerous accounts.

Customer Policy Dashboard tab overview

The Customer Policy Dashboard tab contains an Overview tab where you can set limits for various transaction types in Corporate Banking.

Customer Policy Dashboard tab overview

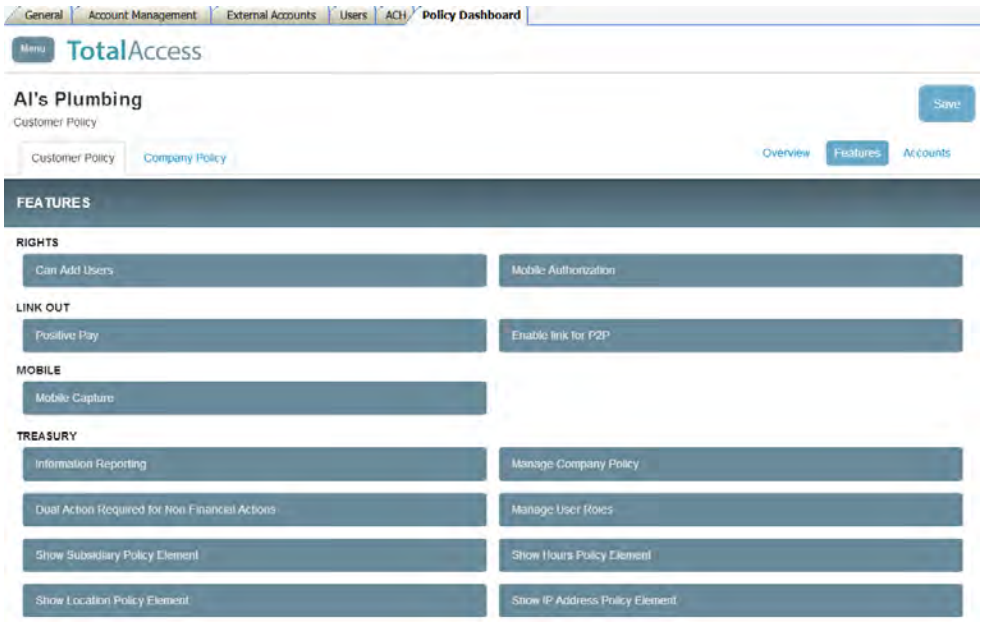


Select a transaction type to display restrictions established for that type and allows for new rules to be created. See "Configuring Allowed Actions for transaction types" on page 101.

Customer Policy Dashboard tab features

The Customer Policy Dashboard tab contains a Features tab that allows access for end users to the Corporate Banking features in online banking. These features are similar to those set for non-Corporate users. The following illustrates some of the possible features available for Corporate Groups.

Customer Policy Dashboard tab Features



Note: In general, features enabled at this level cannot be more than what were enabled at the Group Policy level. However, there are exceptions regarding how rights are inherited for Business and Corporate features that warrant extra security, such as Multi-Wires. See "Feature right exceptions" on page 107.

Customer tasks

This section contains common tasks for working with Customer records including:

- "Viewing a Group's Customer records" on page 182
- "Adding a new Customer" on page 205
- "Editing a Customer" on page 206
- "Changing Customers between Corporate and non-Corporate Groups" on page 206
- "Deleting a Customer" on page 208
- "Using the Add Account wizard" on page 210
- "Managing Customer accounts" on page 209
- "Using the Add External Accounts wizard" on page 211
- "Viewing Users that belong to a Customer" on page 212

Adding a new Customer

To add a new Customer

1. In the workspace tree, click **User Management > Customer**.
2. In the Customers search window, right-click anywhere and choose **New Customer**.



Note: If your FI uses the Group Access Mapping feature and you are assigned to a CSR Team without Full access to any Groups, a message will appear to indicate that you do not have sufficient rights to assign a Customer to a Group. This message may appear even if your CSR Role has the *User Management: Manage Customers* option enabled. To learn more, see "Group Access Mapping" on page 46

3. Enter information directly in each tab, saving each tab before moving to the next tab.
4. Click **Close and Save**.



Note: Customers inherit the permissions and limits that were predefined for the Group to which they are added.

Editing a Customer

Note: If your FI uses Group Access Mapping, you must have rights to a Group to manage Customers in that Group. To learn more, see "Group Access Mapping" on page 46.

Note: Changes (for example, adding or removing accounts) may be blocked if there are pending transactions associated with the record.

To edit a Customer

1. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
2. Search for and select the Customer record that you want to edit. Right-click and select **Edit Customer**.
3. Make changes directly to the information on the tabs.

   Caution: Before changing the Group to which an existing Customer belongs, review the possible impacts noted in "Changing Customers between Corporate and non-Corporate Groups" on page 206.

4. In the toolbar, click **Save** after changes are complete on each tab, and click **Save and Close** when all changes are complete.

Changing Customers between Corporate and non-Corporate Groups

Here are points to consider if switching a Customer from a non-Corporate Group to a Corporate Group

- Unique User Roles are created for each User linked to the Customer and each new User Role will reflect that User's current settings. This may result in a large number of User Roles for the Customer and the Customer's administrative staff may wish to consolidate Users into a few User Roles and delete excess User Roles. See "User Roles" on page 115.



Caution: If you change the Group for an existing Customer, be aware that Users and Logins belonging to that Customer may lose rights to functionality and transaction limits they previously had, if moved to a more restrictive Group.

- Conflicts may occur between a Customer's original limits and rights and the limits and rights provided by the Corporate Group to which the Customer is migrating. While the system does not overwrite the migrated Customer settings, note that the Corporate Group settings will be enforced over the migrated Customer settings. Therefore, it is important to adjust either the Group Policy settings or Customer Policy settings so that reporting and risk management for the Group are correct. Use the Overview and Features tabs on the Group Policy and Customer Policy windows to see where the conflicts are and adjust values accordingly. (See "Group Policy" on page 100 and "Customer Policy" on page 113.) Conflicting limits appear in red text on the Overview tab.



Caution: If you switch an existing Customer from a Corporate to a non-Corporate Group, User Roles created by the Customer will be lost and cannot be recovered. Any assignments of Users to User Roles will also be lost and cannot be recovered. This may incur a significant cost to the Customer in time and effort.

To change the Group to which an existing Customer belongs

1. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
2. Search for and select the Customer record that you want to edit. Right-click and select **Edit Customer**.
3. On the Customer General tab, select a different Group in the **Group** drop-down listbox. (Groups with Corporate features include "*Corporate*" in the drop-down list.)
4. If you select a Corporate Group for a Customer that is currently part of a non-Corporate Group, you will be prompted to confirm the change. Click **Yes** to continue.



Note: If your FI uses Group Access Mapping, a CSR must have full rights to a Group to assign Customers to the Group.

5. In the toolbar, click **Save** after making changes on the Customer General tab.
6. Make any other necessary changes on the other Customer tabs, and then click **Save and Close**.

Deleting a Customer

Deleting a Customer removes the Customer and all associated Users and Logins from the system.

To delete a Customer

1. In the workspace tree, click **User Management > Customer**.
2. In the Customers search window, search for and select the Customer record you want to delete.
3. Right-click the record and click **Delete Customer**.
4. The Delete Customer window displays a confirmation message.
5. Click **Yes** to confirm deleting the Customer.

> **Note:** You are prevented from deleting a Customer if there are pending transactions associated with the record, including recurring transactions.

Using the Add Account wizard

Add an account to a Customer during Customer creation or at any point afterward.

To add accounts to a Customer using the Add Account wizard

1. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
2. Search for and select the Customer record you want to add accounts to and display the record.
3. On the Customer toolbar click the arrow beside the page icon and select **Add Accounts** to launch the Add Account Wizard.
4. Choose from the **Please Select Account Link Type** list (see "Customer accounts overview" on page 185):
    - Customer Number - indicates you plan to link one or more accounts by CIF and will provide the CIF number for which the system should search.

- Account (deposit, loan, credit, investment, or other) - indicates that you want the system to search accounts of the specified type for the account number you will type in. The types of accounts listed here vary depending on your FI's implementation.

5. Select the **Reference Internal** check box to indicate to the system that the number you are supplying will be the internal CIF or account number. Clear the check box to indicate that the CIF or account number is external.
6. Enter either a CIF number or account number in the **Please enter** box, as prompted, depending on the Account Link Type you entered.
   The CIF Number indicates you plan to link one or more accounts by CIF and will provide the CIF number for which the system should search.
7. Click **Next** to start the search. The Accounts pane appears with a list of accounts matching the CIF or the account number you provided.
   - If prompted, you may choose to view other unlinked accounts associated with this Customer's CIF.
8. In the Link By Account column, select the account(s) you wish to add. Accounts already linked to this Customer via CIF are unavailable.
9. Click **Link Accounts by Internal CIF** to add the selected accounts to the Customer record in a way that automatically updates the Customer record if the account is ever removed from this CIF on the core.
10. To add the selected account(s) to the Customer record, click **Finish**.
11. Click **OK** on the confirmation prompt. The newly added account(s) appear on the Account List tab.



Tip: For details, see "Customer Account List tab" on page 193.

Managing Customer accounts

To manage Customer accounts

1. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
2. Search for and select the Customer record that you want to manage accounts for. Right-click and select **Edit Customer**.
3. Access the Account Management tab for this Customer, then click **Refresh**.
4. For each account, set account permissions for the Customer; these can be further restricted at the User level.
5. Click to enable or disable View, Deposit, and/or Withdraw for each account.
6. In the toolbar, click **Save**.

Tip: Check your work by viewing the account list. See "Customer Account List tab" on page 193.

Note: To add external accounts, see "User External Accounts tab" on page 227.

Using the Add Account wizard

Add an account to a Customer during Customer creation or at any point afterward.

To add accounts to a Customer using the Add Account wizard

1. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
2. Search for and select the Customer record you want to add accounts to and display the record.
3. On the Customer toolbar click the arrow beside the page icon and select **Add Accounts** to launch the Add Account Wizard.
4. Choose from the **Please Select Account Link Type** list (see "Customer accounts overview" on page 185):
    - Customer Number - indicates you plan to link one or more accounts by CIF and will provide the CIF number for which the system should search.
    - Account (deposit, loan, credit, investment, or other) - indicates that you want the system to search accounts of the specified type for the account number you will type in. The types of accounts listed here vary depending on your FI's implementation.
5. Select the **Reference Internal** check box to indicate to the system that the number you are supplying will be the internal CIF or account number. Clear the check box to indicate that the CIF or account number is external.
6. Enter either a CIF number or account number in the **Please enter** box, as prompted, depending on the Account Link Type you entered.
   The CIF Number indicates you plan to link one or more accounts by CIF and will provide the CIF number for which the system should search.
7. Click **Next** to start the search. The Accounts pane appears with a list of accounts matching the CIF or the account number you provided.
    - If prompted, you may choose to view other unlinked accounts associated with this Customer's CIF.

8. In the Link By Account column, select the account(s) you wish to add. Accounts already linked to this Customer via CIF are unavailable.
9. Click **Link Accounts by Internal CIF** to add the selected accounts to the Customer record in a way that automatically updates the Customer record if the account is ever removed from this CIF on the core.
10. To add the selected account(s) to the Customer record, click **Finish**.
11. Click **OK** on the confirmation prompt. The newly added account(s) appear on the Account List tab.



Tip: For details, see "Customer Account List tab" on page 193.

Using the Add External Accounts wizard

To use the Add External Account wizard

1. Collect information about the external account. Follow your FI's security procedures to verify the legitimacy of the end user's request.
2. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
3. Search for, locate, and display the Customer record to which you want to add an external account.
4. In the Customer record, right-click anywhere in the External Accounts pane and click **Add External Account**.
5. In Product, choose **External Checking** or **External Savings**.
6. In **ABA Routing Number**, enter the routing number provided in the message.
7. In **Account Number**, enter the account number provided in the message.
8. Click to select the **Deposit** and/or **Withdraw** check box(es).
9. Click **OK**.



Tip: Double-check your work and confirm with the end user that the account was properly set up. Q2central does not verify the existence or ownership of the external account.

Viewing Users that belong to a Customer

To view Users that belong to a Customer

1. In the workspace tree, click **User Management > Customer**. The Customer search options appear.
2. In the Customers search window, search for and select the Customer record of which you want to view the Users.
3. In the Customer record, click the **Users** tab.

CHAPTER 14: MANAGING USERS

Managing Users in Q2central is an important piece of the User Management functionality. The Users, rights, features, and accounts assigned to a commercial user are driven by a Customer's business needs and factors such as business structure, number of owners, and number of employees.

This chapter includes the following sections for working with Users in Q2central:

- "User overview" on page 213
- "User reference" on page 218
- "User tasks" on page 243



Note: If your FI uses the Corporate Banking product, be sure to refer to "Corporate Banking Policies and Users" on page 93 to learn about how Users are handled in Corporate Banking.

User overview

A User represents a person who belongs to a Customer and may have one or more Login IDs. Every User has an individual set of rights, including:

- Rights to create payments and templates of specific transaction types.
- Limits on the transactions the user can approve.
- Rights to access specific accounts.
- Rights to features in Q2online and Q2mobility Apps.

These rights control what each User can do in Q2online and Q2mobility Apps. Ideally, Users have all of the permissions that they need to perform their jobs.

To learn how Users relate to Groups, Customers, and Logins, see "User management definitions and relationships" on page 87. To learn about User Statuses; see "Understanding User Statuses" on page 217.



Note: Although many concepts in this chapter also apply to the Corporate Banking product, see "Corporate Banking Policies and Users" on page 93 if your FI uses that product. In addition to rights and limits, Corporate Banking includes User Roles with varying levels of entitlements, as well as Company Policies.

After a User is added to a Customer, navigate to the **User Management > User** page to edit, enable, disable, activate, and delete Users.



Note: You must perform a search to get records to appear, unless you saved a default search for this option. See "Searching for information in Q2central" on page 348.



Note: If your FI uses the Group Access Mapping feature, the CSR Team to which you are assigned controls your ability to manage Users, based on their assigned Group. You may also notice that some User details are masked. See "Group Access Mapping" on page 46.

User enrollment

These are the main ways that a User can be added to the system:

- FI staff manually add a User to a Customer record, as described in "Adding a new User" on page 243.
- FI staff authorize an administrative User within a Customer to add other Users via the User > Features tab using the flag labeled *Rights: Manage rights for all users*.
- Auto-enrollment, in which a User provides information independently through your FI's website. FI staff can look up newly created Customer/User records, assign account access, and activate Logins. Auto-enrollment helps to minimize redundant or erroneous data entry; some FIs also appreciate the security advantage of not auto-associating end user accounts.
- "End-to-end" enrollment is a custom development offering that requires a User to provide sufficient data for identity verification, then retrieves end-user data from the core to create Customer/User/Login records and link automatically to accounts. Secondary association (non-primary account holders' interaction with accounts for which they are authorized) can be customized to match your FI's core. In a normal end-to-end workflow, FI staff do not participate in end-user enrollment at all.

Auto-enrollment in Q2online and Q2mobility Apps

If your FI uses auto-enrollment, Users who want access to online banking complete an electronic enrollment form that is posted on the FI website. Upon saving, the new User record is automatically created in Q2central in the Group and Customer that your FI set up for this purpose during implementation.

When a new User record is successfully created, the system sends a CSR Notification to FI staff. Depending on how the Group is configured in Q2central, the Login IDs linked to a new User record may default to a *Disabled* status. FI staff can then enable Login IDs at the Customer, User, or Login ID level, as necessary. New end users may be listed in the Disabled Users option and require enablement by FI staff. See "Group Features tab" on page 143.

By default, a new User record has no access to accounts (unless your FI has the end-to-end enrollment service). FI staff associate the appropriate accounts. FI staff also create a login ID, as described in "User Logins tab" on page 228. FI staff must then contact the end user to deliver the login ID and temporary password, unless this data was gathered during the enrollment process.

End users may choose to initiate First-time Login through the Q2mobility Apps or through Q2online. No special setup is required to enable this.

End users must change their password after they log into online banking for the first time. They can access any account for which the FI has granted them access, including secondary accounts and any other accounts that are linked in Q2central.

If you receive a secure message or CSR Notification indicating that Auto-Enrollment failed, view the message details. It is possible that the ID chosen already exists or that a special character caused the failure.

Enrollment in Q2text (Text Banking)

To allow an end user to enroll in Q2mobile Web (browser-based Q2online access via mobile device), FI staff enable a Group-level option; see Mobile-related options in "Group Features tab" on page 143.

After the Group feature is enabled, end users see a Mobile option on their Preferences tab in Q2online.

Text Banking (Q2text) allows end users to transact within your FI only—external funds transfers are not possible. End users enroll in Text Banking in Q2online and select accounts for access. They also assign account nicknames that are

transmitted instead of personal information or account numbers. The availability of Text Banking is controlled by the Mobile: Allow Text Banking setting in Q2central on the Group > Features tab; see "Group Features tab" on page 143.

Enrollment in Q2voice (Voice Banking)

If your FI purchased Q2voice, a menu layout and call routing options were provided for the voice system during implementation. Account lockout criteria and password policies for the Voice Channel can be configured on the **Administration > Password Policy** page in Q2central.

The method for enrolling users depends on the type of Q2voice system, either an account-based, user-based, or a hybrid approach where a user can log into any account for which the user is the primary account holder.

For account-based and hybrid logins, users can enroll themselves with their account number and last four digits of a Social Security Number. For user-based logins, users call their FI and a CSR manually creates the voice login and associated accounts.



Note: Activity in Q2voice is limited to moving funds among the end user's own accounts.

Password-free migration

This enrollment method is used primarily when an FI converts to the Q2platform. With it, end users can log in securely to Q2online or Q2mobility Apps for the first time without using a password from the old system. An end user provides a Login ID, selects the first-time login option, and chooses from their own existing contact information to receive a secure access code (SAC). (If the contact information is out of date, they cannot proceed without contacting the FI.)

After retrieving and supplying the code, the user is prompted to create a password according to the FI rules, which are displayed for them. After clicking **Submit**, the password and login ID are enabled. FI staff is not involved unless an update to contact information is needed; updates are performed as described in "User Secure Access tab" on page 222.

Understanding User Statuses

The User Status that appears on many Q2central windows indicates the current status of the User, which may be:

- **Active:** The User can log in and use online banking according to the permissions and rights provided in Q2central. If your FI uses the Corporate Banking product, the assigned User Role and Company Policy also control what a User can do in online banking.
- **Inactive:** The User cannot log into online banking because a Corporate Banking administrator with "Admin Role" as a User Role deactivated the User on the **Commercial > User Management > View User** page in online banking.
- **Disabled:** A CSR may have disabled the User record due to suspected fraud or for added security during an extended leave. Another reason why a User Status may be set to *Disabled* is if it is a new User record created via Auto-enrollment.

  Note the following details about the *Disabled* User Status:

  - CSRs can disable all Users linked to a specific Customer by right-clicking a record on the **User Management > Customers** search window and then selecting **Disable All Users** from the shortcut menu that appears.
  - When a User Status is *Disabled*, all logins under the User are unusable regardless of their displayed status.
  - Corporate Banking administrators with "Admin Role" as their User Role cannot enable disabled User records, only CSRs can.

Many Q2central pages include an Effective User Status value that can be *Active*, *Inactive*, or *Disabled*, as described above. If the *Dual Action for Non-financial Transactions* feature is enabled in Corporate Banking, the following statuses may also appear:

- **Inactive, awaiting activation approval:** A Corporate Banking administrative User activated a User record that was previously deactivated.
- **Active, awaiting role change approval:** A Corporate Banking administrative User changed the User Role for a User and the change cannot take effect until another User approves it.

User reference

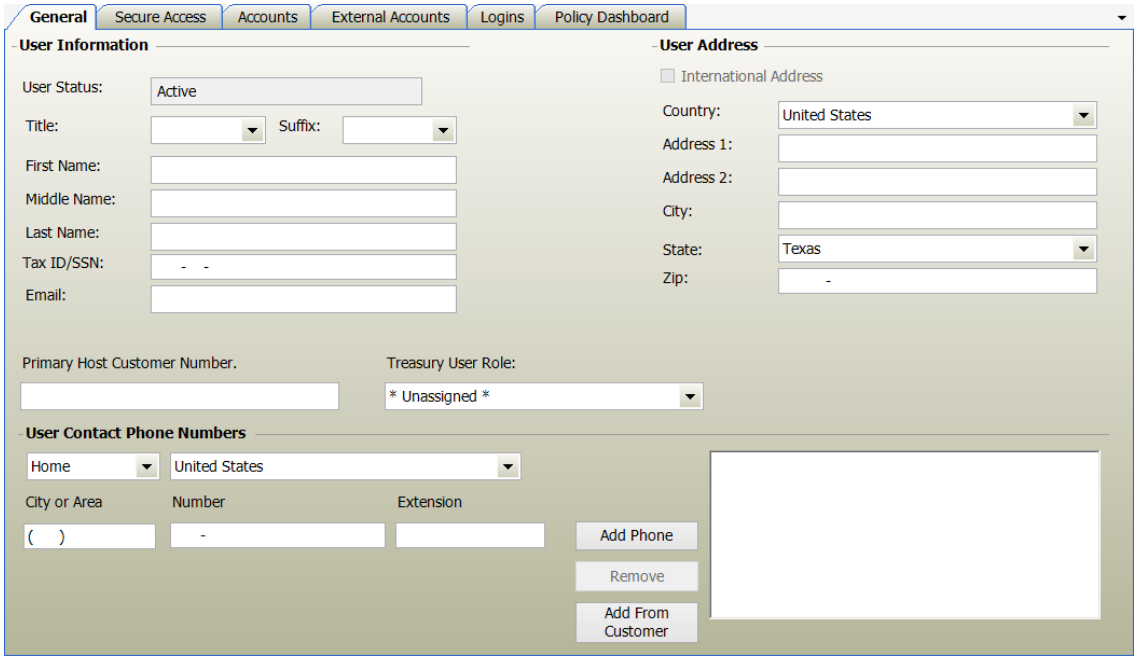
The Users option allows you to search for, view, edit and delete Users that are assigned to your Customer records. The following sections provide a detailed reference for each of the tabs in the User option.

If you purchased Corporate Banking, references to Corporate Banking-specific settings are also included.

User General tab

The General tab of the User page displays User contact information including address and phone information. For security purposes, always use FI core contact information to verify transactions with end users. Changes made to phone numbers and email addresses in online banking are automatically passed to Q2central, including changes that may have been made by a fraudster.

User General tab



The following table describes each option in the User General tab:

User General tab options

Option	Description
User Information section (all fields are optional)	
User Status	The current status of the User: Active, Inactive, or Disabled. Some Q2central pages include an Effective User Status column. See "Understanding User Statuses" on page 217.
Title	The name title. Options are selected from the drop-down list.
Suffix	The name suffix. Options are selected from the drop-down list.
First Name	The User's first name.
Middle Name	The User's middle name (if used).
Last Name	The User's last name.
Tax ID/SSN	The Tax ID Number (TIN) or Social Security Number (SSN) for this User. If an incomplete SSN is entered (for example, 8 digits instead of 9), the original entry is cleared so you can enter the SSN again. Employer ID Numbers (EINs) are entered on Customer records.
Email	The email address for the User. **Note:** This value is required for all Users of the Q2 Contextual PFM product.
User Address section	
International Address	Indicates a non-U.S. address. This check box only appears if creating a new record; it affects whether State or Province is displayed. This data may be used by some adapters.
Country	The list of countries your FI requested at implementation.
Address fields	Indicates the mailing address for this record. Address 2 is not a separate address, it is a continuation of Address 1, if needed. Unless your FI has linked the database to your core, this is not necessarily the same as the information on the core.

User General tab options (cont'd)

Option	Description
Primary Host Customer Number	The primary identification number (PIN) that provides access to the FI's core for the Customer record to which the User belong. If an FI uses an Open Solutions, Inc. (OSI) core that requires a host PIN to pull back data, this value is automatically inherited from the Customer record when a new User is added. **Note:** This value is used only to connect information and serve as an additional authentication method when pulling data in real time. It will not overwrite values on the core.
Corporate User Role	The User Role to which the User is assigned. Each User Role has a different combination of Corporate entitlements, account permissions, and features. See "Corporate Banking User Roles" on page 115. **Note:** This field only appears if your FI purchased the Corporate Banking product.
User Contact Phone Numbers	
Contact Number Type	Contact number type options (selected from the drop-down list).
Country	The drop-down list of countries your FI requested at implementation. The default option is United States.
City or Area	Area Code for the selected phone number.
Number	Phone number for the User.
Extension	Phone number extension, if applicable.
Add Phone	Complete the entries on the left, then click **Add Phone** to enter an additional phone number to the User record.
Remove	Select a phone number from the phone numbers list on the right, and click **Remove** to delete it.

User General tab options (cont'd)

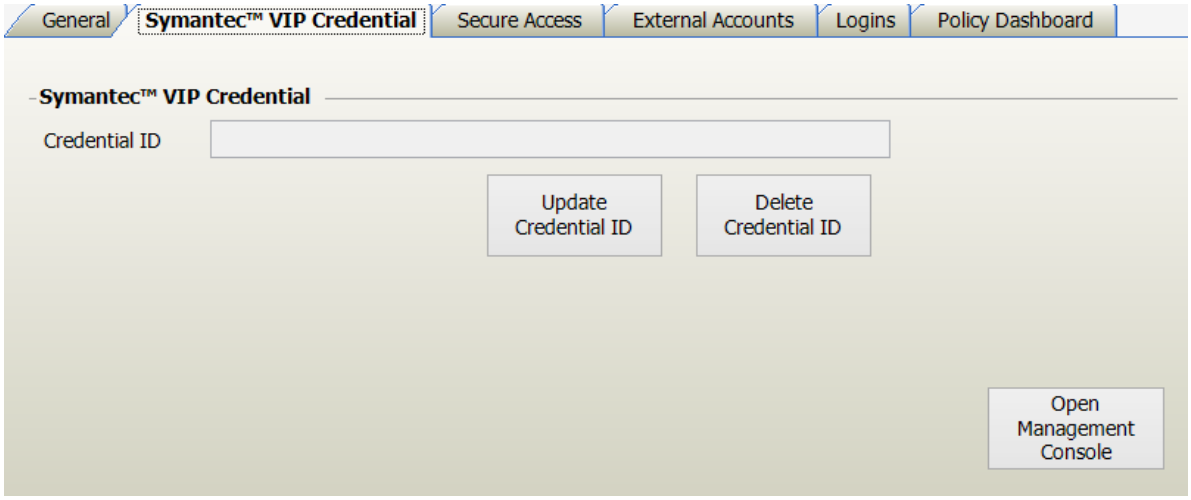
Option	Description
Add from Customer	Automatically adds all valid Phone numbers from the Customer record to this User record.
Phone Number List	Lists all the valid contact phone numbers on record for the selected User.

Note: These phone numbers are not used to deliver secure access codes (SAC) or system alerts. To update that information, use the Secure Access tab instead. See "User Secure Access tab" on page 222.

User Symantec VIP Credential tab

This tab appears on the User window only if your FI offers Symantec™ VIP third-party authentication service and the associated Customer record is enrolled in the service. To learn more, see "Symantec VIP token codes" on page 77

User Symantec VIP Credential tab



Symantec VIP Credential tab options

Option	Description
Credential ID	The current Credential ID that Symantec uses to authenticate the end user.
Update Credential ID	Provides the new or replacement Credential ID issued by Symantec. The end user provides FI staff with this number.
Delete Credential ID	Deletes the Credential ID. If a credential is deleted then authorization defaults to out-of-band authorization code.
Open Management Console	Launches the Symantec application that allows FI staff to troubleshoot end-user status questions and request reports.

Note the following details about VIP token codes:

- The first time a device is used to obtain a Symantec VIP token code, the end user must provide two sequential token codes.
- Enable the *Authentication: Enable access via Symantec VIP Token option* on the Group page's Feature tab to require that all Users in a Group enter a VIP token code to log into online banking.

User Secure Access tab

The User window's Secure Access tab helps you manage the end user contact info used to send secure access codes required for login using multi-factor authentication (MFA) or transaction authorization. A destination where an end user can receive secure access codes is known as a *SAC target*.

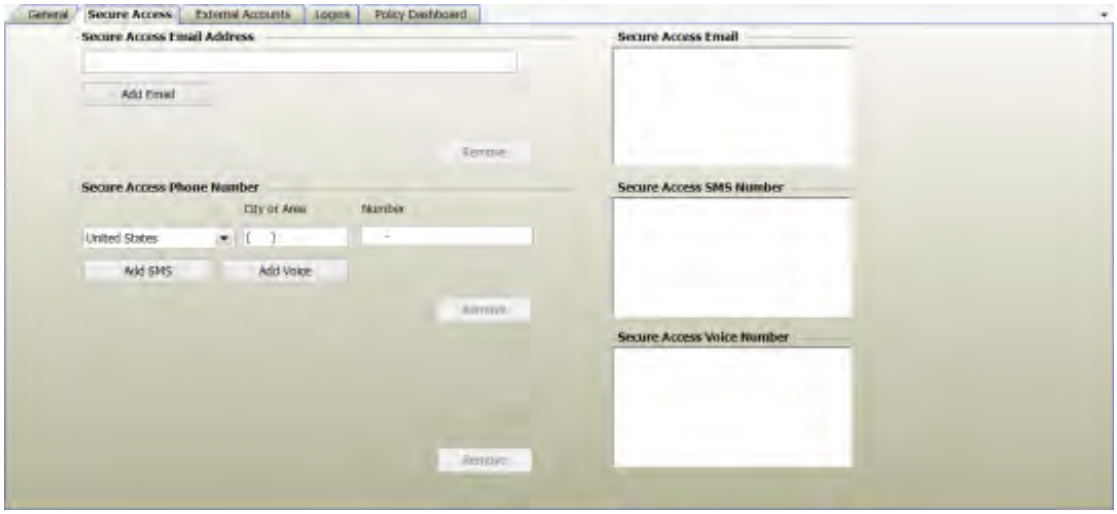
SACs provide an additional layer of security if the user's login ID and password are compromised. The validation occurs when the user enters the SAC provided by the delivery channel of their choice. Each SAC is valid for one-time use and expires if not used promptly.



Note: Not all SMS and Voice notifications are successful if they involve international phone numbers. In these situations, a Challenge Code may work. See "Challenge questions" on page 81 for details.

Targets can be added for SMS and Voice if an FI allows it. These are controlled via the *MFA: Allow secure access code delivery via SMS* and *MFA: Allow secure access code delivery via Voice* options on the Group > Features tab. Additionally, an FI must own these products in order for these targets to take effect. Be aware that Q2central does not indicate lack of success in delivering SACs; for example, when an email cannot be delivered.

User Secure Access tab



Secure Access tab options

Option	Description
Secure Access Email Address	The email address(es) where the end user wishes to receive a secure access code.
Add Email	Adds an email address as a target for this User. **Note:** Q2 recommends against SAC email targets, particularly for Groups with commercial functionality or external transfer capability, due to the possibility of email hacking. It is more secure to receive a SAC out-of-band—that is, on a device other than the one to which the end user is logging in.

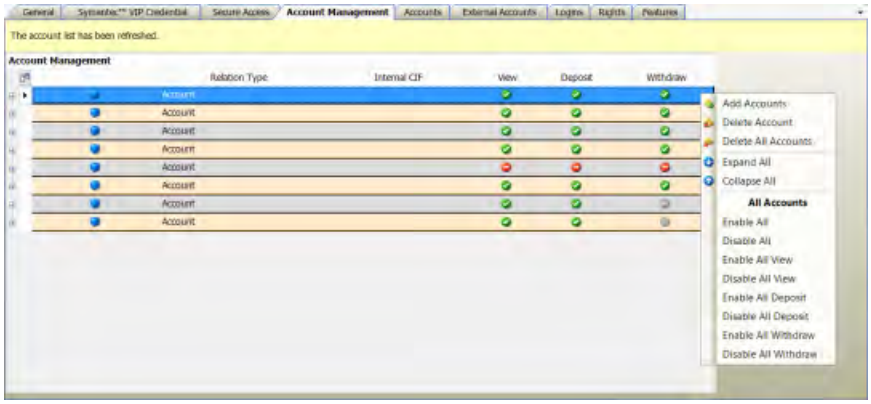
Secure Access tab options (cont'd)

Option	Description
Remove (Email)	Removes a selected item from the Secure Access Email list.
Secure Access Email list	Displays all email addresses to which a SAC is sent for this User.
Secure Access Phone Number	The country, city code or area code, and phone number where the end user wishes to receive SACs.
Add SMS	Adds the phone number as a text target for this User.
Add Voice	Adds the phone number as a voicemail target for this User.
Remove	Removes the selected target from the corresponding list (Secure Access SMS Number or Secure Access Voice Number).

User Account Management tab

This tab allows you to set User-level view, deposit, and withdrawal permissions to on-us accounts belonging to the associated Customer (accounts held at a different FI are listed on the User's External Accounts tab). If any accounts are missing, see "Adding accounts to a User record" on page 244.

User Account Management tab



User Account Management shortcut menu options

Menu Option	Description
Add Accounts	Adds an account to the User record.
Delete Account	Deletes the selected account.
Delete All Accounts	Deletes all accounts associated with this User.
Expand All	Allows viewing of Customer-level selections regarding the Override, View, Deposit, and Withdraw permissions.
Collapse All	Returns to the default view.
Enable All	Enables all permissions for all accounts in this view.
Disable All	Disables all permissions for all accounts in this view.
Enable All View	Enables all View permissions for all accounts in this view.
Disable All View	Disables all View permissions for all accounts in this view.
Enable All Deposits	Enables all Deposit permissions for all accounts in this view.
Disable All Deposits	Disables all Deposit permissions for all accounts in this view.

User Account Management shortcut menu options (cont'd)

Menu Option	Description
Enable All Withdrawals	Enables all Withdrawal permissions for all accounts in this view.
Disable All Withdrawals	Disables all Withdrawal permissions for all accounts in this view.

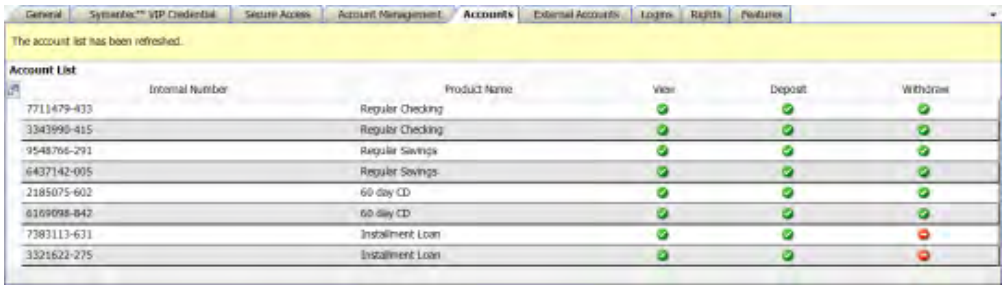
Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

User Accounts tab

This tab is for verification only. It provides a streamlined list of all the on-us accounts associated with this User and the permissions for each. Use this to review your work on the Accounts Management tab.

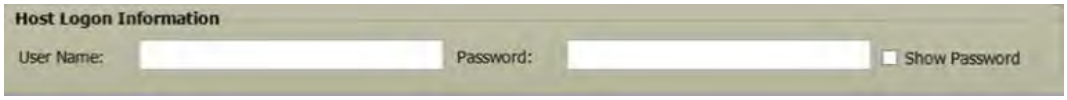
You can control the information displayed about the items. Field Chooser selections on this window are the same as for the Accounts Management tab. See "User Account Management tab" on page 224.

User Accounts tab



If your FI uses an Open Systems Interconnection (OSI) host with Customer-level Host PINs, a Host Logon Information section appears at the bottom of the User Accounts tab.

Host Logon Information fields (User Accounts tab)



Note: These fields may appear for FIs that do not use an OSI host, but they have no adverse effects on the system.

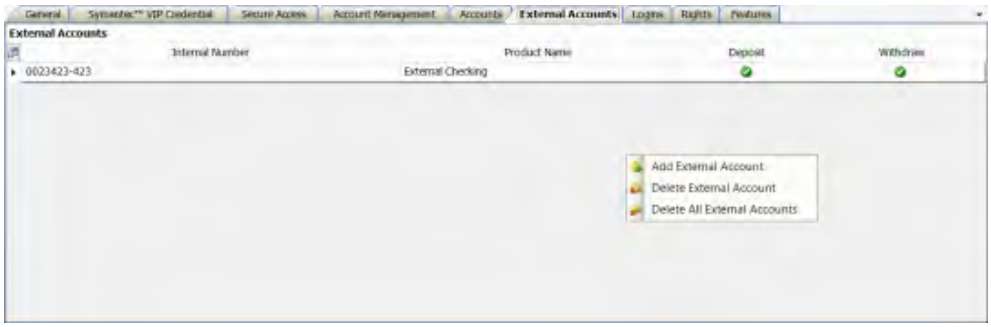
User External Accounts tab

An external account is one that does not reside in your FI's core. It is available so that end users can make external funds transfers with a different FI. Like other accounts, external accounts are added first to the Customer record, then to one or more User records.

Note: Only the External Accounts linked at the Customer level can be added to the User level.

External accounts are linked to the user for either deposit, withdrawal, or both. Users may assign nicknames for linked external accounts, but may not view the account.

Users External Accounts tab



Users External Accounts right-click options

Menu Option	Description
Add External Account	See "Adding accounts to a User record" on page 244.

Users External Accounts right-click options (cont'd)

Menu Option	Description
Delete External Account	Deletes the selected external account.
Delete All External Accounts	Deletes all external accounts associated with this User.

Tip: If you mistakenly delete an account, click **X** to close the Customer window, then click **No** when asked whether you want to save changes.

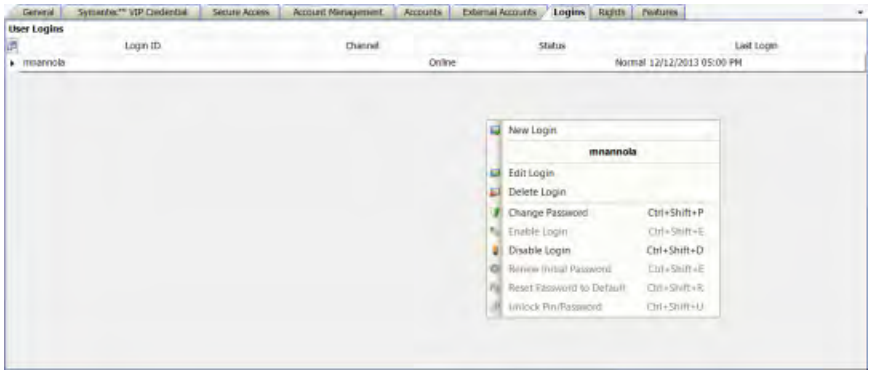
Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

User Logins tab

The Logins tab lists the Login records associated with a User. A Login record is the place where FI staff can assist end users who have become locked out of the system. (This tab is not visible to FI staff whose role lacks the UserManagementManageUserLogins right.)

You can double-click a row on this tab to access the Login record.

User Logins tab



Users Logins tab right-click options

Option	Description
New Login	Adds a new login for the current User record only.
Edit Login	Allows changes to the selected login.
Delete Login	Removes the selected login. The end user cannot log in to that channel after a login deletion, but continues to have access to other channels. Login deletion can be a quick response to suspected fraud.
Password and access options	See "Troubleshooting Login issues" on page 264.

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

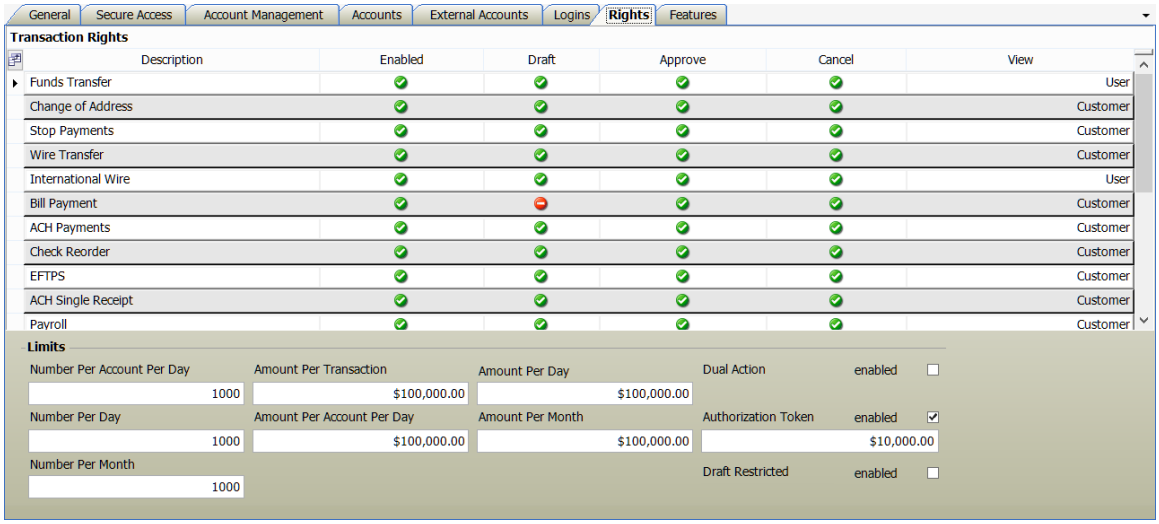
User Rights tab

The Rights tab of the User window displays the transaction types enabled or disabled at the Customer level and this User's limits for each enabled transaction type. Draft-restricted Users are also set up here.

If your FI requires account entitlement for ACH PassThru, this is one tab where the User must be entitled to act on the relevant accounts.

Tip: Save periodically while setting rights and limits. Advise end users that changes you make for them take effect only after they log out of online banking, then log back in.

User Rights tab



Transaction Rights pane

In the Enabled column, enable each available transaction type or activity that this User has reason to use in all accessible channels. The options available here are determined at the Customer level; see "Customer Rights tab" on page 196.

In the Draft column, enable each transaction type for which this User should be able to initiate transactions in the channel(s) associated with this User record.

In the Approve column, enable each transaction type for which this User should be able to approve transactions in all accessible channels.

If the *Funds transfers: Hide draft step* feature is enabled on the Group > Features tab, fund transfers drafted by end users with rights to perform them may be immediately submitted as authorized. (For more info about the feature, see "Group Features tab" on page 143.)

In the Cancel column, enable each transaction type for which this User should be able to cancel transactions in all accessible channels. Users may cancel ACH transactions only before FI processing has occurred.

In the View column, select the level of visibility that this User should have for this transaction type. Never means this end user cannot view any transactions of this type; User means this end user can see only transactions that he or she creates; Customer means this end user can see any transactions of this type created by any Users for this Customer.



Note: In order for Mobile Authorization and Dual Action to work for a User, Customer view must be enabled.

In the Update column, enable each transaction type for which this User should be able to edit transactions in all accessible channels.

A transaction right takes effect only if enabled and if you also provide non-zero amounts for that transaction type in the Limits pane.

Limits pane

The options displayed in the Limits pane vary depending on the transaction type selected in the Transaction Rights pane. Limits are assigned based on the transaction type selected.

You are prevented from assigning limits that are higher than what is allowed on the Customer record.

Provide a value other than zero for each field. Otherwise, this User cannot transact the associated transaction type.

- Number per Account per Day
- Number per Day
- Number per Month
- Amount per Transaction
- Amount per Account per Day
- Amount per Day
- Amount per Month

Dual Action

Select the Dual Action check box to require that whenever this User drafts a transaction of the selected type that is greater than the amount specified in the text box, a different User within this Customer record must approve it.



Note: Unlike most rights that automatically inherit settings from a parent Group or Customer, this right can be enabled for a User even if it is not enabled at the Group or Customer level.

See "Understanding Dual Action" on page 97 for details.

Authorization Token

Select the **Authorization Token** check box to require that whenever this User approves a transaction of the selected type that is greater than the amount specified in the text box, a Symantec VIP token code or secure access code (SAC) must be provided.

This setting can be different from what is shown on the Customer level; however, if there is a limit specified at the Customer level, the limit here cannot exceed that. Also, note that unlike most rights that automatically inherit a setting from a parent Group or Customer, this right can be enabled even if it is not enabled at the Group or Customer level.

Note: If your FI is set up to prompt for a VIP token code but the User does not have a Symantec account, then the system prompts for a SAC.

Draft Restricted

If the *Rights: Enable draft restricted* feature applies at the Group level and the User has permission to draft transactions of the selected transaction type, select the Draft Restricted check box to indicate that this User's draft rights are restricted. (For more info about the feature, see "Group Features tab" on page 143.)

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

Consumer model

John Smith is an end user at the FI. John Smith is the Customer in this example. Because John Smith is a Consumer user, he will also be the User. John Smith's User has two Logins, jsmith (used to access Q2online) and 11111 (used to access Voice banking).

John Smith has one manual account, checking account number 101, and his CIF number is 123456789. User John Smith has full access (deposit, view, and withdrawal) to these accounts. He belongs to the Consumer Users Group. However, he does not want access to Bill Payment at this time.

He would like to add his accountant, XYZ Accounting, Inc., as a User. XYZ Accounting should only have view access to John Smith's accounts. This User record has one Login ID, xyzonline, used to access Q2online. The XYZ Accounting user is temporary and can be enabled or disabled depending on the time of year.

Business Banking model

Acme Builders is a company that has accounts at the FI. Acme Builders is the Customer in our example. The owner, Jack Johnson, is a User. He has two Logins: jjohnson (used to access Q2online) and 22222 (used to access Voice banking).

The bookkeeper, Dorothy Davis, is another User. She has one Login, ddavis, used to access Q2online. Both Jack Johnson and Dorothy Davis should have full access (deposit, view, and withdrawal) to all of Acme Builders' accounts.

If the FI chooses to allow it, a main User can be set up as an administrative User with rights to control or remove access of the other Users.

User Features tab

Features enabled on the Customer record's Features tab that also appear here can be disabled at the User level, if necessary, in the User Features tab.



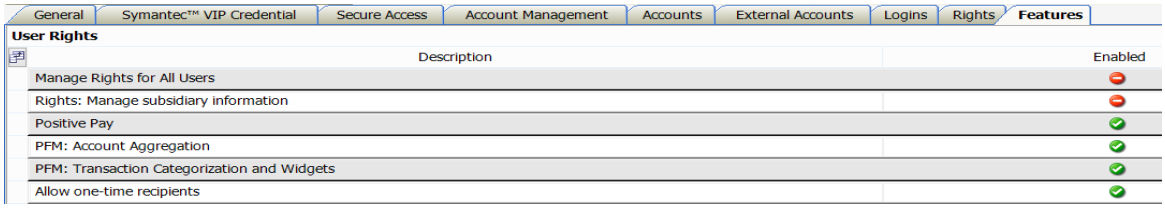
Note: There are exceptions regarding how rights are inherited for Business and Corporate Banking features that warrant extra security, such as Multi-Wires. See "Feature right exceptions" on page 107.

For Corporate Banking Users, configure User Features on the Policy Dashboard instead.



Tip: There is not an exact overlap between Customer features and User features. That is, there may be Customer-appropriate features that are not displayed here and User-appropriate features here that do not appear on the Customer record. That makes it important to check both places when verifying User access.

User Features tab



User Features options

Option	Description
BillPay: Admin	If an FI purchased Business Bill Pay, this option allows this User to manage the rights for other Business Bill Pay end users.
BillPay: SubUser	If an FI purchased Business Bill Pay, this option allows this User to access the Business Bill Payment tool. **Note:** Although this option controls access to the Bill Payment tool, the ability to actually make payments is controlled on the Bill Pay vendor's site.
Mobile: Allow Mobile Capture Access	Enrolls this User for mobile remote deposit capture (mRDC), if the FI offers an mRDC product.
PFM: Account Aggregation	Enables Consumer Banking (and sometimes Business Banking) users of Q2 Contextual PFM to link accounts held at other FIs to their online banking profile so that they can see balances and transactions for all accounts in a single view, across all devices.

User Features options (cont'd)

Option	Description
PFM: Transaction Categorization and Widgets	If enabled, Q2 Contextual PFM will automatically categorize end-user transactions for linked accounts. End users can change transaction categories, split transactions across multiple categories, create subcategories, and use PFM widgets.
Rights: Access online statements	Allows this User to access banking statements in Q2online.
Rights: Access to all payment templates	Allows this User full access (including create and delete rights) to the payment templates that have been established by this Customer.
Rights: Manage recipients	Allows this User full access to manage the payment recipient list established by this Customer.

User Features options (cont'd)

Option	Description
Rights: Allow one-time recipients	Allows a User to create a one-time recipient for a single payment. Data will not be saved as a Recipient record like regular, repeat recipients, nor will it appear on the Recipient Management page. Note the following details about this option: • If this option and the *Manage Recipients* option are enabled, the user can click **Create Recipient** to store the new recipient as a permanent record, or click **OK** to add the recipient for the payment without saving a record. • If this option is disabled and the *Manage Recipients* option is enabled, the user will only see the Create Recipient button, and the new recipient is stored as a permanent record. • If this option and the *Manage Recipients* option are disabled, the user cannot see the existing recipient list when drafting a one-time payment unless the *Can view all recipients* option is enabled. The *Can view all recipients* option allows a user to see the existing list if making a one-time payment.

User Features options (cont'd)

Option	Description
Rights: Can view all recipients	Allows a User to pick from the entire recipient list to create a payment. Note these details about the this option: • If this option is enabled and *Manage Recipients* is enabled, the user can see all recipients in a one-time payment workflow, and create new permanent recipient records in the workflow. • If this option is enabled and *Manage Recipients* is disabled, the user can see all recipients in a one-time payment workflow, but cannot create new permanent recipient records in the workflow. • If this option is disabled and *Manage Recipients* is enabled, the user can see all recipients in a one-time payment workflow, and create new recipient records in the workflow. • If this option is disabled and *Manage Recipients* is disabled, the user cannot see all recipients in a one-time payment flow, and cannot create new recipient records in the workflow. If the *Allow one-time recipient* option is enabled, the user can create a one-time recipient (that is, the OK button appears) in the one-time payment workflow.
Rights: Manage rights for all users	Assigns administrative rights that allow this User to provision other Users within this Customer. This right must first be enabled on the Features tab of the Customer record.

User Features options (cont'd)

Option	Description
Rights: Manage subsidiary information	Allows this User to set up subsidiaries for this Customer on the Subsidiary page in online banking. FI staff cannot control or modify the information that the User sets up, and cannot view it except by using CSR Assist. **Note:** For compliance with wire transfer regulations, it is important that end users maintain the correct address of the originator of wire transfers in the Subsidiary page in online banking.
SSO: Positive pay single sign on	Allows this User to log in to the Positive Pay SSO for this Customer.
SSO: {Name varies}	Allows this User to login to the specified SSO for this Customer.

Understanding How Feature Rights Impact Payments

This section describes how different payment-related feature rights affect a User's ability to create payment templates, edit templates, and make one-time payments.

On the **User > Features** tab, enabling the *Allow one-time recipients* option allows ends users in a one-time payment flow to create a new recipient that is not saved as a permanent record in the database. The *Can view all recipients* option allows the user to only pick from the existing recipients list when making a one-time payment.

Note the following details about the *Allow one-time recipients* option:

- If this is option is enabled and the *Manage Recipients* is enabled, then the user can either click **Create Recipient** to store the new recipient as a permanent record or click **OK** to add the recipient for the payment without storing the recipient as a permanent record.

- If this option is disabled and the *Manage Recipients* option is enabled, then the user will only see the **Create Recipient** button and the new recipient will be stored as a permanent record.
- If this option is disabled and the *Manage Recipients* option is disabled, then the user cannot see the existing recipient list when drafting a one-time payment unless *Can view all recipients* is enabled. The *Can view all recipients* option allows the user to see the existing list when making a one-time payment.

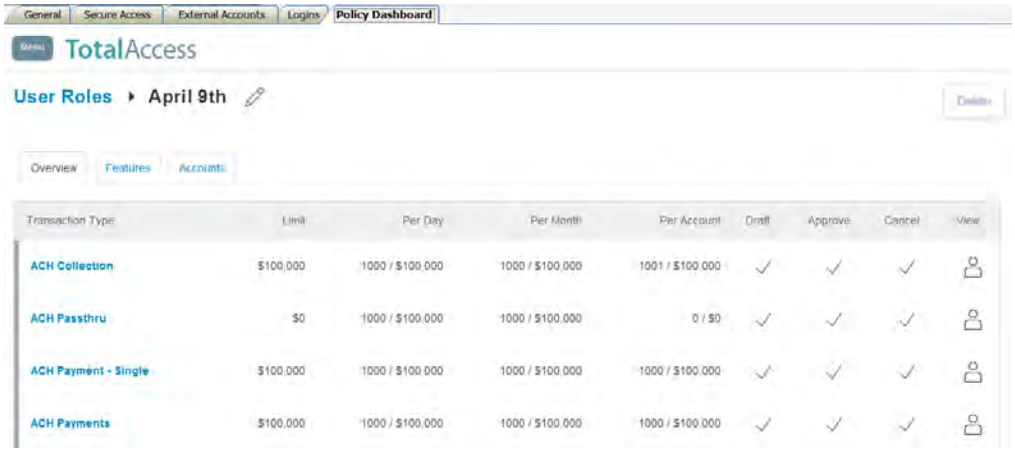
Note these details about the *Can view all recipients* option:

- If this option is enabled and *Manage Recipients* is enabled, then the user can see all recipients in a one-time payment workflow and create new permanent recipient records in the workflow.
- If this option is enabled and *Manage Recipients* is disabled, then the user can see all recipients in a one-time payment workflow, but cannot create new permanent recipient records in the workflow.
- If this option is disabled and *Manage Recipients* is enabled, then the user can see all recipients in a one-time payment workflow and create new recipient records in the workflow.
- If this option is disabled and *Manage Recipients* is disabled, then the user cannot see all recipients in a one-time payment flow and cannot create new recipient records in the workflow. If the *Allow one-time recipient* option is enabled, the user can create a one-time recipient (that is, the **OK** button appears) in the one-time payment workflow.

User Policy Dashboard Overview tab (Corporate)

The User Policy Dashboard tab contains an Overview tab where you can set the limits for the various transaction types.

User Policy Dashboard tab Overview



The following transaction types appear for Corporate Banking Users in the Overview tab:

- ACH Collection
- ACH Passthru
- ACH Payment - Single
- ACH Payments
- ACH Receipt - Single
- Change Address
- Check Reorder
- EFTPS
- Payroll
- Stop payment
- Transfer - Internal
- Wire - Domestic
- Wire - International

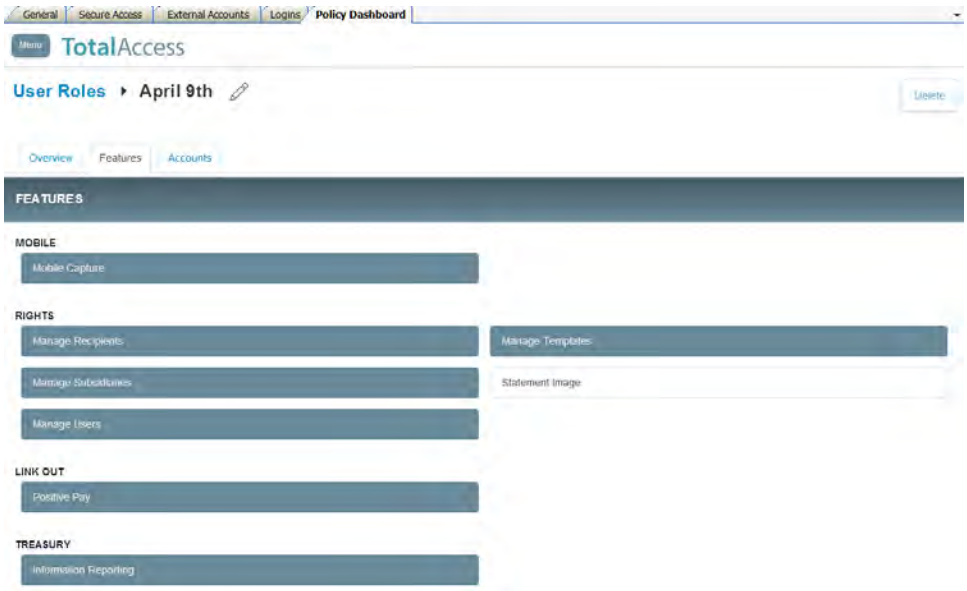
Selecting any of the transaction types, displays the restrictions that are established for that type and allows for new rules to be created. See "Configuring Allowed Actions for transaction types" on page 101 for details about creating rules and restrictions.

User Policy Dashboard Features tab (Corporate)

The User Policy Dashboard tab contains a Features tab that allows access to the Corporate Banking features in online banking for each Corporate User. These features are similar to those set for non-Corporate users. The following illustrates some of the possible features available for Corporate Banking Users.

Note: To see the User Policy Dashboard tab, the User must have a Corporate User Role applied in the User General tab.

User Policy Dashboard tab Features

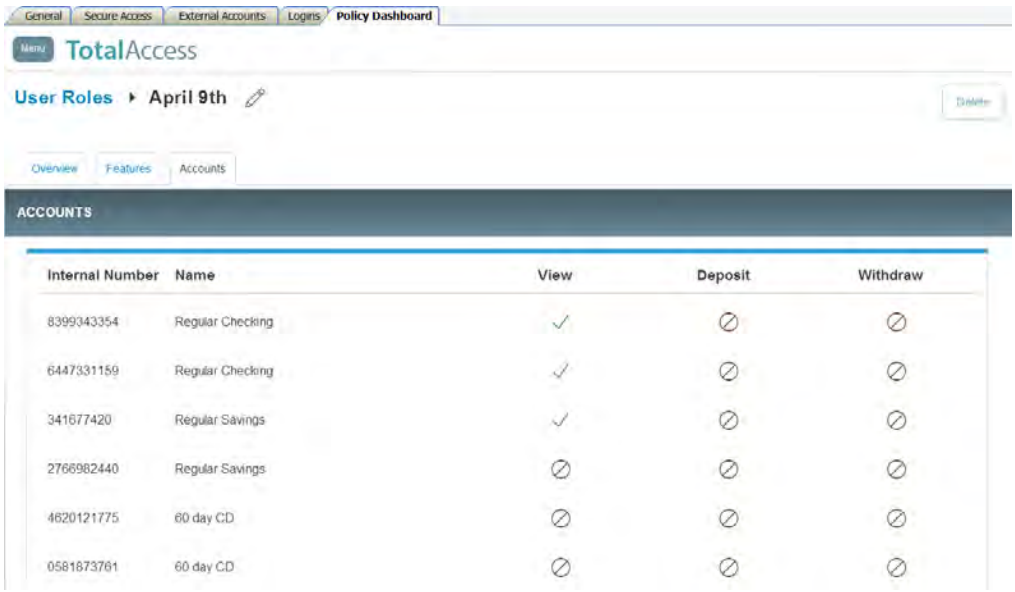


Note: There are exceptions regarding how rights are inherited for Business and Corporate Banking features that warrant extra security, such as Multi-Wires. See "Feature right exceptions" on page 107.

User Policy Dashboard Accounts tab (Corporate)

The User Policy Dashboard tab contains an Accounts tab that allows you to assign rights to the Accounts established for the Company and assigned User Role.

User Policy Dashboard tab Accounts



Each account carries with it assigned View, Deposit, and Withdraw rights. Assigned rights use the check mark symbol and restrictions use the circle with the line through it.

See "Configuring Allowed Actions for transaction types" on page 101 for more information on creating rules and restrictions.

User tasks

This section contains the most commonly performed tasks for working with User records.

- "Adding a new User" on page 243
- "Adding a Q2voice User" on page 244
- "Adding accounts to a User record" on page 244
- "Managing User account access" on page 246
- "Managing User access to external accounts" on page 247
- "Editing a User" on page 247
- "Enabling features for a User" on page 247
- "Enabling all account management rights for a User" on page 248
- "Maintaining secure access information for Users" on page 250
- "Changing a Password" on page 251
- "Deleting a User" on page 253
- "Activating a User" on page 251
- "Disabling a User" on page 252
- "Disabling all Users" on page 253
- "Enabling a User" on page 252
- "Determining when a User record was created" on page 253
- "Using CSR Assist" on page 261

Adding a new User

New Users are added from the Customer record and can be created at any time. Users are created without any account rights (unless a pending transaction at conversion requires them). However, the limits to what Users can be granted are inherited from the Customer to which they are added.

To add a New User

1. In the workspace tree, click **User Management > Customers** and display the Customers list.
2. Double-click the record for the Customer for which you are adding the User.
3. On the Users tab, right-click anywhere and click **New User**.
4. In the User window, enter information directly in each of the tabs, saving each tab as you complete them.
5. Click **Close and Save**.

User creation may be affected by a control on the Group > Features tab named *New logins are disabled until CSR approves*. If this feature is enabled, the new User records will have a *Disabled* status until enabled by FI staff. See "Understanding User Statuses" on page 217.

The next step is to establish the login(s) required; see "New User Login window" on page 255.

Adding a Q2voice User

Adding a Q2voice User is similar to adding other Users, except:

- Accessing each account may be a separate login event for the end user, depending on which configuration your FI selected.
- Activity in Q2voice is limited to moving funds among the end user's own accounts. For that reason, setup involving limits, external accounts, and more is unnecessary, and the only relevant tab is General.

Adding accounts to a User record

Accounts are added first at the Customer level and again at the User level. By default, Users do not have access to Customer accounts.

Access to Customer accounts is controlled at the User level on the Add Accounts window, available through the Account Management tab.

When an account is added to a User, the system usually assigns no rights to the account for that User; you must take action to specify the User's rights. However, if you are adding an account to a User and there are already pending transactions on the new account, the system automatically elevates the User's rights to accommodate those transactions. For example, if there is a pending payment on the account, the system assigns withdrawal rights to the User so that the transaction can occur. The system displays a message if this happens; FI staff should review the User's rights set and make adjustments.

The elevation of User rights to accommodate one or more pending transactions on a new account does not affect limits, because in this case the pending transactions were previously authorized.

To add accounts to a User

1. In the workspace tree, click **User Management > Users**.
2. In the User search window, select the User record for which you want to add the account.

3. On the User record, right-click and select **Add Accounts**.
    - View the list, which shows accounts attached to the Customer record to which this User does not yet have access.
    - If no accounts have not been added yet, the following actions are available on this window:

Add Accounts options

Option	Description
Add All Relationships	Links all remaining Customer accounts and creates a relationship with the CIF. Selecting this option triggers an update to the account(s) when they change on the CIF record.
Add All Accounts	Links all remaining Customer accounts without linking to the CIF.
Expand All	Allows viewing of Customer-level permission settings for all listed accounts.
Collapse All	Returns to the default view.

4. Enable or disable the current User's access of that type to that account.



Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

Managing User account access

To manage User account access

1. In the workspace tree, click **User Management > Users**.
2. Search for and select the User record.
3. In the User record, click the **Account Management** tab for the User, then click **Refresh**.
4. Select each account for the User and click to enable or disable View, Deposit, and/or Withdraw permissions for each account.

   Note: By default, all permissions are disabled. For Consumer Banking Customers, you may choose to give access to all accounts, since the User is the same person as the Customer.

5. In the toolbar, click **Save**.

Tip: Check your work by viewing the User Accounts list.

About restricting a User's access

If a User has scheduled an outstanding transaction of any type, FI staff cannot restrict that User's rights if it would affect the transaction. Instead, Q2central notifies FI staff that the action cannot be completed.

For example, if a User scheduled a funds transfer from a checking account that has not yet occurred, FI staff cannot remove the right of that User to perform funds transfers and cannot restrict that User's withdrawal rights from the checking account unless:

- FI staff waits until after the funds transfer is complete, or
- FI staff cancels the funds transfer first

Recurring transactions may prevent FI staff from restricting a User's access if the transactions have been generated (recurring transactions are generated dynamically, as needed).

Managing User access to external accounts

Verify that the end user has met your FI's requirements for transferring to and from external accounts.

To manage User access to external accounts

1. In the workspace tree, click **User Management > Users**.
2. Search for and select the User record.
3. In the User record, click the **External Accounts** tab for the User.
4. Select each account for the User and click to enable or disable Deposit and/or Withdraw permissions for each account.

   Note: By default, permissions are disabled. For restrictions on editing a User record, see "User Account Management tab" on page 224.

5. In the toolbar, click **Save**.

Editing a User

Note: Changes (for example, adding or removing accounts) may be blocked if there are pending transactions associated with the record.

To edit a User

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. Search for and select the User record that you want to edit. Right-click and select **Edit User**.
3. Make changes directly to the information on the tabs.
4. In the toolbar, click **Save** after changes on each tab, and click **Save and Close** when all changes are complete.

Enabling features for a User

To enable a feature for a User

1. In the workspace tree, click **User Management > Users**.
2. Search for and select the User for which you want to enable features.
3. In the User record, select the **Features** tab.

> **Tip:** Click the **Description** column header to alphabetize the list.

4. Click an item in the User Features pane to place the focus arrow beside it.
5. Click the icon in the Enable column to enable each feature that this User is allowed to use.
6. In the toolbar, click **Save and Close**.

> **Tip:** Quickly view Customer settings by clicking **Show Customer** in the toolbar.

Enabling all account management rights for a User

To enable all account management rights for a user

1. In the workspace tree, click **User Management > Users**.
2. Search for and select the User record for which you want to enable all Account Management rights.
3. In the User record, click the **Account Management** tab.
4. Right-click anywhere in the Account Management tab and select one of the following options:
   - **Enable All**—enables all (view, deposit, and withdraw) rights for all accounts.
   - **Enable All View**—enables only view rights for all accounts.
   - **Enable All Deposit**—enables only deposit rights for all accounts.
   - **Enable All Withdraw**—enables only withdraw rights for all accounts.
5. The Set Account Access window displays, asking you to confirm the change for the selected account or on all accounts. Choose **This One** or **All**, based on your needs.
6. Click **Save**.

Enabling User rights to view, draft, approve, or cancel transactions

This section describes how FI staff can enable User rights to view, draft, approve, or cancel transactions. For example, FI staff can enable rights for the first User in a Company to set that person up as an administrator that can enable rights for other Users.

Note: This section is specific to Business Banking end users. To learn about enabling rights for Corporate Banking end users, refer to "Corporate Banking User Roles" on page 115.

By default, most rights enabled at the Customer level are enabled for all Users within the Customer. Typically, you cannot provide a User with a right that is disabled at the Customer level.

Dual Action and Authorization Token are exceptions; they can be set at a User level without being enabled at higher levels. There are also exceptions for features that warrant extra security; see "Feature right exceptions" on page 107.

To enable User rights to view, draft, approve, or cancel transactions

1. In the workspace tree, click **User Management > Users**.
2. Search for and select the User record for which you want to enable rights.
3. Right-click the User record and click **Edit User**.
4. Access the Rights tab, and adjust the settings for each column, as necessary. Use the following table for reference.
5. Click **Save**.

User rights for Transaction Types

Setting	Description
Enabled	Enable each transaction type to be listed in this end user's menus in online banking. If this column is off (red), the end user has no action-related rights to draft, approve, and/or cancel a transaction of this type. However, the end user still has any view rights that were assigned.
Draft	Enable each transaction type that this end user has the right to draft. The Limits section of this User window does not apply to drafts; when checking drafts, the system uses the Customer record.
Approve	Enable each transaction type that this end user has the right to authorize. Transaction limits for authorizations are listed in the Limits section for this end user.
Cancel	Enable each transaction type that this end user has the right to cancel. End users with this right can cancel any transaction they can see.

User rights for Transaction Types (cont'd)

Setting	Description
View	Select the level of viewing rights this end user has for the specified transaction type. • Customer allows end users to see all transactions of this type that are associated with the Customer, regardless of who created them. • User allows end users to see only transactions they created. • None blocks viewing of this ACH transaction type by this end user, regardless of who created the transaction. A view assigned here is visible even if the Enabled column is off (red).

Maintaining secure access information for Users

This section describes how to access a User record and then update the User's contact information that will be used to send secure access codes (SACs) to the User.

Before following these steps, make sure that the Group to which the User belongs has the corresponding feature(s) enabled in the Group Features tab, which include:

- *MFA: Allow secure access code delivery via email*
- *MFA: Allow secure access code delivery via SMS*
- *MFA: Allow secure access code delivery via voice*

To maintain the User's secure access information

1. In the workspace tree, click **User Management > Users**.
2. In the Users search window that appears, search for and select the User record for which you want to maintain secure access information.
3. In the User record, click **Secure Access** tab.
4. To enter an email address, enter the email address in the Secure Access Email Address section and click **Add Email**. Repeat this step for all email addresses.
5. To enter a phone number, enter the phone number in the Secure Access Phone Number section.
6. Select from among the countries that were configured for your FI at implementation.

7. Either click **Add SMS** to add a text message destination or **Add Voice** to add a voice call destination.
8. Your FI must own Q2text (text banking/SMS) for end users to receive SACs by text message.
9. In the toolbar, click **Save**.

Changing a Password

Changing the Password allows you to set and confirm a new password while viewing the FI's current password policy.

To change a password

1. In the workspace tree, click **User Management > Users**. The Users list appears.
2. In the Users list, select the User whose password you want to change, right-click and select **Change Password**.
3. In the Change Password window, enter and confirm a new password and click **OK**. The Change Password confirmation window displays.
4. Click **OK**.

Activating a User

A User must have an Inactive status to be activated.



Note: This option is only available if you are assigned to a CSR Role with the Corporate Banking right.

To activate a User

1. In the workspace tree, click **User Management > Users**. The Users search list appears.
2. In the Users search list, search for and select the User record you want to activate.
3. Right-click the User you want to activate, and click **Activate User**. The Activate User confirmation window appears.
4. In the Activate User confirmation window, click **Yes**.



Note: Once the User is activated, the Effective User Status column on the User search list shows the User as Active.

Enabling a User

There are two places in Q2central where you can enable a disabled User record:

- The User Management > Customer > Users tab
- The User Management > Users search grid

To enable a User on the Users search grid

1. In the workspace tree, click **User Management > Users**.
2. When the Users search grid appears, search for and select the User record you want to enable.
3. Right-click to display the shortcut menu and click **Enable User**.
4. When the Enable User confirmation window appears, click **Yes**.

Disabling a User

Disabling a User prevents the User from logging in or moving funds. It also disables all Login IDs associated with the User. A User must have an Active, Pending, or Inactive status to be disabled. There are two places in Q2central where you can disable a User record:

- The User Management > Customer > Users tab
- The User Management > Users search grid

To disable a User on the Users search grid

1. In the workspace tree, click **User Management > Users**.
2. When the Users search grid appears, search for and select the User record you want to disable.
3. Right-click the User record you want to disable, and click **Disable User**.
4. When the Disable User confirmation window appears, click **Yes**.



Note: Once the User is disabled, the Effective User Status column on the User search grid shows the User as Disabled.

Disabling all Users

Disabling all Users for a Customer prevents these Users from performing certain actions in their current session and prevents them from logging in. All Users must have an Active status to be disabled.

To disable all Users for a Customer

1. In the workspace tree, click **User Management > Customers**. The Customer search options appear.
2. Navigate to the Customer record for which you want to disable all Users.
3. Right-click and select **Disable All Users**.
4. When the Disable All Users confirmation window appears, click **Yes**.



Note: After disabling Users with this option, each User must be individually enabled.

Deleting a User

To delete a User

1. In the workspace tree, click **User Management > Users**.
2. In the Users search list, navigate to the User record you want to delete.
3. Right-click the User you want to delete, and click **Delete User**. The Delete User window displays a confirmation for the deletion of the selected User.
4. Click **Yes** to delete the User.

Determining when a User record was created

To view the date and time when a User record was created

1. In the workspace tree, click **Reporting > Operations**. The list of Operations reports appears.
2. In the Operations report list, choose the **Customer Contact Information by Customer** report. The report window appears.
3. Enter a Customer Name, or leave blank for all Customers.
4. In Sort By, select **User** from the drop-down list.
5. Click **OK** to generate the report.
6. Scroll through the report to the desired User.



Note: The Created On date and time appears with User Login data.

CHAPTER 15: WORKING WITH LOGIN IDS

All users of Q2 applications, whether Q2central, Q2online, or Q2mobility Apps, require a valid Login ID.

This chapter includes the following sections for working with Login IDs in Q2central:

- "Login IDs overview" on page 254
- "Login IDs reference" on page 255
- "Logins tasks" on page 257
- "Troubleshooting Login issues" on page 264

Login IDs overview

The Logins option, located in the User Management section of the Q2central workspace tree, lists all login IDs established at your FI. A Login record is the place where FI staff can assist end users who become locked out of the system (see "Troubleshooting Login issues" on page 264).

Note: You must perform a search to get records to appear, unless you saved a default search for this option. See "Searching for information in Q2central" on page 348.

Note: If your FI uses Group Access Mapping, the CSR Team to which you are assigned controls your ability to manage Login IDs, based on the assigned Group. You may also notice that some Login IDs are masked. See "Group Access Mapping" on page 46.

When working with the Logins search results, you can use the Field Chooser to add the Customer Name column header to the Logins window. Then drag the CustomerName column header into the space labeled *Drag a column header here to group by that column*, so that Login records sort by Customer Name first. To more information, see "Using the Field Chooser" on page 349.

If an end user has difficulties with online banking, you can use a featured called CSR Assist to view the end user's online banking environment. See "Using CSR Assist" on page 261 for details.

Another Q2 product, Q2assist, provides limited access to end user data so that CSRs can provide support for end users while meeting minimal installation requirements. Q2assist can be used to reset passwords, unlock login IDs, and send secure access codes (SACs)to end users.

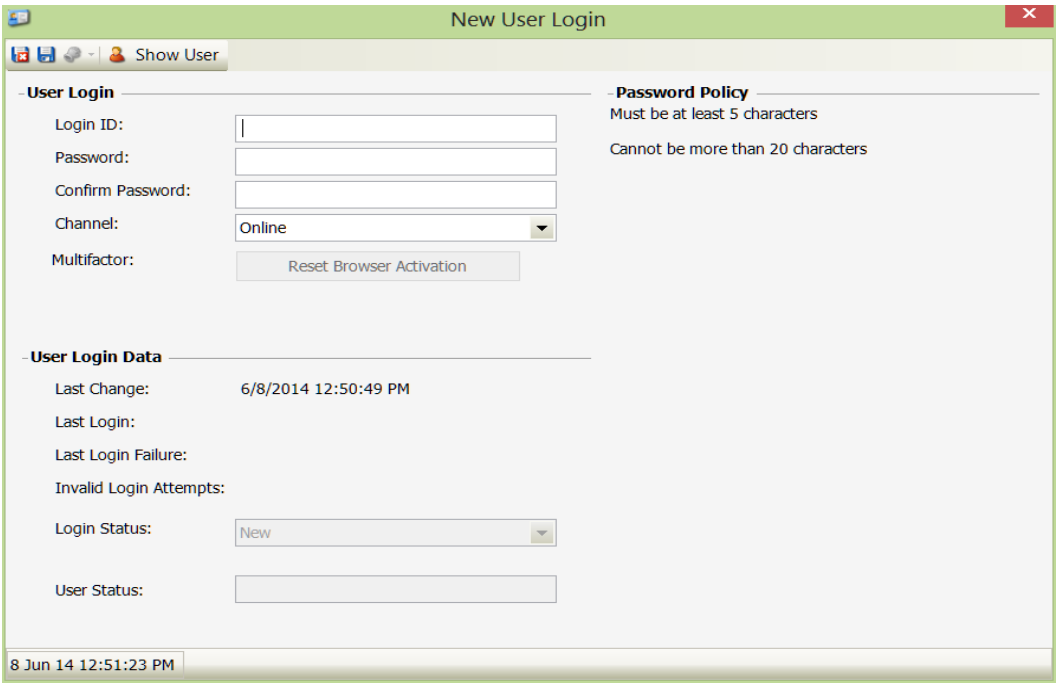
Login IDs reference

The User Login window allows you to view or edit information about a selected login. The New User Login and User Login windows are accessible from the User record and the Logins search results and contain the same information.

New User Login window

You can use the New User Login window to establish the login information and view the associated password policy for a User.

New User Login window



New User Login window options

Option	Description
Login ID	The unique name for this end user in this channel. Your FI established login length requirements during implementation, and the system notifies you if the specified Login ID does not meet complexity requirements. (End users are also informed of unmet requirements when attempting to change their own Login ID in Q2online.) If your FI needs to change login requirements, contact Q2 Customer Support. These requirements are not maintained in Q2central.
Password	The password that conforms with the established Password Policy.
Confirm Password	A reentry of the password for confirmation purposes. This should be communicated to the end user as the temporary password. After logging it, the end user will be prompted to create a new password.
Channel	The channel for which you want to create this login. Available channels depend on products that an FI owns, and may include: • Online: For logging into online banking; • Voice: For logging into Q2voice; • Merchant: For logging in to check the viability of a check that is written at a merchant site; • Text: Not in use. End users can enable text banking via the Settings > Text Enrollment page in online banking.
MultiFactor	Clears the incrementation of times this login is allowed to register a browser.
User Login Data	
Last Change	The date of the most recent edit made to this login.
Last Login	The date of the most recent successful login event for this login.
Last Login Failure	The date of the most recent unsuccessful login attempt using this login.

New User Login window options (cont'd)

Option	Description
Invalid Login Attempts	The number of unsuccessful login attempts using this login; the date of the most recent attempt is displayed in the LastFailed column. The maximum number of invalid attempts is configurable per FI, but is usually set to 3. After the final attempt, the system locks the login. See "Troubleshooting Login issues" on page 264. This value resets when the login is unlocked. Ensure end users have current email addresses and phone numbers in the Secure Access delivery section. See "User Secure Access tab" on page 222.
Login Status	The current status of this Login. Normal indicates that there is nothing that prevents this end user from logging in. For additional statuses, see "Login statuses" on page 334.
User Status	The overall status of the end user.
Password Policy	A summary of your FI's current password requirements. This information may assist you in responding to end-user questions and in resetting passwords.

Logins tasks

Because Logins provide the system access for your users, there are a lot of tasks associated with keeping end user Logins active and viable in the system.

This section includes the following tasks for maintaining the logins in Q2central:

- "Adding a new Login" on page 258
- "Editing a Login" on page 259
- "Viewing a Login" on page 259
- "Deleting a Login" on page 260
- "Disabling a Login" on page 260
- "Enabling a Login" on page 260
- "Renewing an initial password" on page 261
- "Unlocking a password" on page 261

Adding a new Login

Before you add a new user Login, it is a good idea to view the Password Policy to see your FI's current password requirements.

To add a new User Login

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. Search for and select the User record for which you want to add a Login, and click the **Logins** tab.
3. Right-click anywhere in the Logins tab and click **New Login**. The New User Login window appears.
4. Complete the following information:
   - Enter a unique **Login ID** for the end user in this channel.
   - Enter the **Password**.
   - Re-enter the Password in **Confirm Password**.

   > **Tip:** View the Password Policy to see your FI's current password requirements.

5. Select a **Channel** from the drop-down list. Options include:
   - Online: To log into online banking
   - Voice: To log into Q2voice
   - Merchant: To log in and check the viability of a check that is written at a merchant site
   - Mobile: To log into Q2mobility Apps
   - Text: Not in use. End users must self-enroll using the opt-in available in online banking, via the Preferences > Mobile menu option
6. In Multifactor, click **Reset Browser Activation** to clear the incrementation of times this login is allowed to retrieve an MFA secure access code.

   > **Note:** The User Login Data section is for informational purposes only.

7. On the toolbar, click **Save and Close**.

Editing a Login

Your FI established Login ID length requirements during implementation, and the system will notify FI staff if a Login ID does not meet complexity requirements. (End users are also informed of unmet requirements when attempting to change their own login IDs in Q2online or Q2mobility Apps.)



Note: If your FI needs to change login requirements, contact Q2 Customer Support. These requirements are not maintained in Q2central.

To edit a Login

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. Search for and select the User record for which you want to edit the Login, and click the **Logins** tab.
3. Right-click anywhere in the Logins tab and click **Edit Login**. The User Login window appears.
4. Update any of the following information:
    - Enter a unique **Login ID** for the end user in this channel.
    - Click **Change Password** to open the Change Password window.
        a. Complete the **New Password** and **Confirm Password** entries, then communicate the temporary password to the end user.
        b. Click **OK** when complete.
    - In the Multifactor section, click **Reset Browser Activation** to clear the incrementation of times this login is allowed to retrieve an MFA secure access code.
    - The **User Login Data** and **Password Policy** sections are for informational purposes only.
5. In the toolbar, click **Save and Close**.

Viewing a Login

To view a Login

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. Search for and select the User record for which you want to display the Login, and click the **Logins** tab.
3. Right-click anywhere in the Logins tab and click **Edit Login**.

Deleting a Login

Logins with associated pending or recurring transactions cannot be deleted.



Caution: Deleted Logins cannot be reactivated.

To delete a Login

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. In the Users search window, search for and select the User record for which you want to delete the Login, and click the **Logins** tab.
3. Right-click anywhere in the Logins tab and click **Delete Login**.
4. The Confirm Deletion window displays a confirmation for the selected login. Click **Yes** to delete the login.

Disabling a Login

Disabling a Login sets the login status to *Disabled*, and the end user is unable to use this Login ID until it is enabled by FI staff. Disabling a login does not reduce the number of end users for which your FI is charged; only deleting Users affects the active user count.

To disable a Login

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. Search for and select the User record for which you want to disable the Login, and click the **Logins** tab.
3. Right-click anywhere in the Logins tab and click **Disable Login**. The Status column on the Logins tab shows the Login ID as Disabled.

Enabling a Login

Enabling a Login returns a disabled Login Status to Normal (enabled).

To enable a Login

1. In the workspace tree, click **User Management > Users**. The Users search window appears.
2. Search for and select the User record for which you want to enable the Login.

3. Click the **Logins** tab.
4. Right-click anywhere in the Logins tab and click **Enable Login**.
5. The Status column on the Logins tab shows the Login ID as Enabled.

Renewing an initial password

This option extends the time that a first-time end user's FI-provided password is valid. Use this option with logins whose status is New Password Has Expired. This option is unavailable after the first-time login is successful.

To renew an initial password

1. In the workspace tree, click **User Management > Logins**. The Logins search window appears.
2. In the Logins search window, search for and select the Login record for which you want to renew the initial password.
3. Right-click and click **Renew Initial Password**.

Unlocking a password

This option sets the Login Status to Normal, which enables the FI staff person to log in with the existing password.

To unlock a password

1. In the workspace tree, click **User Management > Logins**. The Logins search window appears.
2. Search for and select the Login record for which you want to unlock the password.
3. Right-click and click **Unlock Pin/Password**.

Using CSR Assist

With the CSR Assist feature, a CSR can log into online banking on behalf of an end user and see the same information that the end user sees, assuming that the CSR has the same browser version (or greater) as the end user.

CSRs can access CSR Assist from either the Logins or Users option in User Management section of the workspace tree if their CSR Role has the following rights enabled:

- *ADMINISTRATION: CSR Assist*
- *USER MANAGEMENT: Manage User Logins*

Note the following details about using CSR Assist:

- Before CSR Assist can be utilized, the end user must have logged into online banking at least once and the status of the Login ID must be *Normal*.
- If Group Access Mapping is enabled at your FI, only CSRs that belong to a CSR Team with Full rights to a Group can log in on behalf of a user that belongs to the Group. See "Group Access Mapping" on page 46.
- While logged in on behalf of a user, CSRs cannot accept disclaimers or agreements.
- SSO functionality (for example, Bill Pay transactions) and the Information Reporting features of the Corporate Banking product are not supported.

To use CSR Assist

1. In the Q2central workspace tree, click **User Management > Users**. The Users search window appears.
2. In the Users search window, search for and select the User record.
3. Right-click that row to display the shortcut menu and click **CSR Assist**.
4. On the CSR Assist page that appears, select a **Policy** from the drop-down list.
    - View Only
    - View and Draft
    - View, Draft, Approve, and Cancel
    - View, Draft, Approve, Cancel, and Recipient
5. Enter your Q2central **Password**.

    Note: If you enter an incorrect password and exceed the maximum number of attempts allowed, your Q2central account will be locked.

6. Select your **Display** method. You can view online banking from within Q2central or using the computer's default browser.
7. Click **OK**.
8. When the Customer Service Assistance window appears, click **Login**. Q2online displays the user's Home page.

Using Q2assist

Q2assist provides limited access to end user data so that an FI can provide Level 1 support for Q2 products while meeting minimal installation requirements. If this Q2 product is set up for your FI, you can use it to reset passwords, unlock login IDs, and send the latest secure access code (SAC) to an end user.

Normally, end user data is visible only through Q2central. However, there may be circumstances in which it is not practical for an FI to install or allow access to Q2central solely to provide support, for example:

- Staff providing support is entry-level, and training on the powerful Q2central application is not planned or has not yet occurred
- Staff providing support is mobile within your IP addresses; Q2central is not mobile for technical and security reasons
- The FI seeks to outsource its Level 1 support function

With Q2assist, an FI can provide support in these circumstances without exposing sensitive end user data to editing. With primarily read-only access, Q2assist provides useful functionality to non-Q2central-authorized staff through a kiosk-like model with multiple users accessing the same data but with limitations.



Note: If you have a Q2central account with permission to access Q2assist, you will be locked out of Q2central if you are locked out of Q2assist and vice versa.

For more information, refer to the *Q2assist Quick Start Guide* and the *Q2assist User Guide*, available on the Q2 Customer Portal.

Troubleshooting Login issues

Most password and lockout issues (which typically result from mistyping a password too many times in a row) are resolved at the Login level. You can perform the actions described on the Logins page, on the User page Logins tab, or on the **System Alerts > Locked Logins** page

To resolve a locked login

- In the Logins list, right-click and choose **Unlock Pin/Password** to set the login status to Normal and allow the end user additional attempts to provide credentials (with no change to the password).

To select the appropriate password action

- In the Logins list, right-click and choose one of the following options:
  - **Change Password**: If an end user forgets a password, or the password is compromised, choose this option to set a temporary password that you can communicate to the end user.
  - **Renew Initial Password**: Use this option to set the Login status to *Normal* and reinstate the original password.
  - **Reset Password to Default**: Use this option to set the Login status to *Normal* and reset the password to the default value specified in the system configuration.

To respond to a request to enable a disabled login

Follow your FI's policy on re-enablement. A disabled login is different from a lockout, because this status is not accidental—someone in a position of authority (either an administration User or FI staff) may have taken action to disable it. You may wish to view events leading to the disablement using Q2central's Administration> Auditing feature; see the *Q2central Reporting Guide*.



Note: New end users' Logins are disabled if new users created through the online channel are disabled but are enabled for the Group.

CHAPTER 16: MANAGING SUBSIDIARIES

This chapter describes how FI staff can maintain subsidiaries on behalf of Customers in Q2central. It includes the following sections:

- "Subsidiaries overview" on page 265
- "Subsidiaries reference" on page 266
- "Subsidiaries tasks" on page 269

Subsidiaries overview

If enabled for your FI, the **User Management > Subsidiaries** option in Q2central allows FI staff to manage subsidiaries directly in Q2central. This feature can eliminate transaction processing failures that can occur if subsidiaries are added within online banking but the FI core is not updated in real-time.

In online banking, there are two ways to add subsidiaries can be added:

- Business or Corporate Banking Users with administrative permissions can manage their own subsidiaries in online banking.
- FI staff can use CSR Assist to log into online banking and manage subsidiaries on behalf of Customers. (See "Using CSR Assist" on page 261.)

However, neither method updates the FI core in real time so the core will reject the ACH Tax ID if it does not have that data. Historically, FI staff had to research ACH transactions to determine a subsidiary's owner. Now FI staff can use the Subsidiaries page in Q2central to maintain subsidiaries directly. The core receives data in real time so the new subsidiary and its parent Customer are linked immediately in Q2central.



Tip: To block administrative end users from managing subsidiaries in online banking, disable the *Manage Subsidiaries* feature at the Group or Customer level.

One common approach to ACH risk management is for an FI to use their ACH system's ability to track and report originated and returned items by monitoring the Company Identification field contained in the Batch Header record of the NACHA file, which is populated with data obtained when a Subsidiary is created. By managing this process from Q2central, FIs can ensure the Sending Company ID is consistent for tracking in their downstream applications.

Understanding Organizations

In Q2central, an *Organization* represents a Business or Corporate Banking Customer. The primary purpose for Organizations is to distinguish between:

- Consumer Customer records that use *Household* as the Customer Type and typically match the related User record exactly.
- Business and Corporate Banking Customer records that use *Commercial* as the Customer Type, but are linked to distinctly different User records. For example, one Corporate User with administrative privileges may be able to add Users while another Corporate User cannot.

Only Business and Corporate Customer records appear on the Organizations tab of the Subsidiaries page. This speeds searches for subsidiary owners using criteria such as Organization name, Login ID, Tax ID, or CIF.

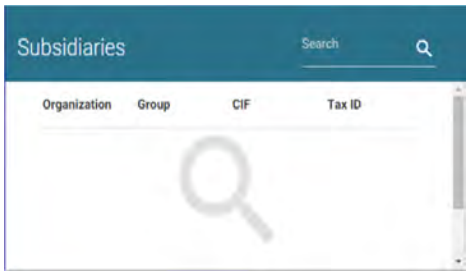
FI staff requirements

To manage subsidiaries, you must belong to a CSR Role with the *CUSTOMER: Manage Subsidiaries* right enabled. If Group Access Mapping is active, you must belong to a CSR Team with View or Full rights to an Organization's parent Group and its child records. See "Group Access Mapping" on page 46.

Subsidiaries reference

This section describes the Subsidiaries page that FI staff can use to manage subsidiaries, accessible via the **User Management > Subsidiaries** in the Q2central workspace tree.

Subsidiaries page



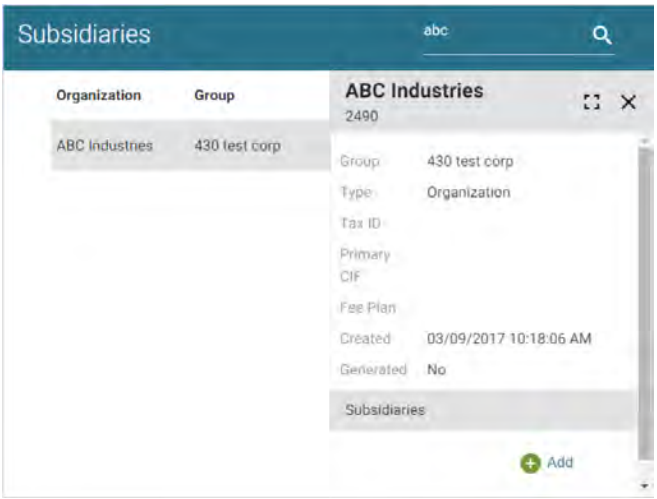
Subsidiaries page options

Element	Description
Search	Enter search criteria in the Search field at the top of the page. Click the Search icon ( ) to display a list of results.
Organization	The name of the Organization.
Group	The Group to which the Organization belongs.
CIF	The Primary CIF for the Organization.
Tax ID	The Tax ID for the Organization.

Organization Details pane

After performing a search on the Subsidiaries page, click a subsidiary to open the Organization Details pane to display details such as Tax ID, CIF, etc.

Organizational Details pane



On the Organization Details pane, CSRs can add, edit, and delete subsidiaries, as described in "Subsidiaries tasks" on page 269.

Organization Details pane options

Option	Description
Search	Enter search criteria in the Search field at the top of the page. Click the magnifying glass icon to display a list of matching Organizations.
Organization	The name of the Organization.
Group	The Group to which the Organization belongs.
CIF	The customer information file (CIF) for the Organization.
Tax ID	The Tax ID for the Organization.

Subsidiaries tasks

You can perform the following tasks on the Subsidiaries page:

- "Searching for an Organization" on page 269
- "Adding a subsidiary" on page 269
- "Viewing subsidiary details" on page 270
- "Editing a subsidiary" on page 271
- "Deleting a subsidiary" on page 271

Searching for an Organization

To find the Business or Corporate Banking Customer that owns a subsidiary

1. In the workspace tree, click **User Management > Subsidiaries**.
2. On the Subsidiaries page, enter all or part of a keyword or phrase in the search bar. (You can also search by Group, Tax ID, or CIF.)
3. Click the Search icon ( ) to return a list of matching results.
4. In the results list, click an Organization to display details about the Business or Corporate Customer that owns the subsidiary.

Tip: Click the Expand icon ( ) to enlarge the Organization Details pane. To close it, click the Close icon ( ).

Adding a subsidiary

To add a subsidiary

1. Navigate to the Organization to which you want to add a subsidiary. (See "Searching for an Organization" on page 269.)
2. Scroll to the **Subsidiaries** section of the Organization Details pane.
3. Click **Add**.
4. Complete fields on the Add Subsidiary window that appears.
   - **Name** – A unique ID consisting of up to 50 characters.
   - **Payment Type** – The type of payment used by the subsidiary payment type: *ACH*, *Wire*, or *ACH & Wire*.
   - **ACH Header** – The ACH header for the subsidiary, up to 16 characters long.
   - **ACH Tax ID** – The ACH Tax ID for the subsidiary, up to 11 characters long. Special characters that match the NACHA specification for tax IDs are supported.

- **Wire Header** – The wire header, up to 35 characters long.
- **Country** – The country in which the subsidiary exists.
- **Address** – The subsidiary's physical address.
- **City** – The city in which the subsidiary exists.
- **State** – The state in which the subsidiary exists.
- **Postal Code** – The subsidiary's postal or ZIP code.

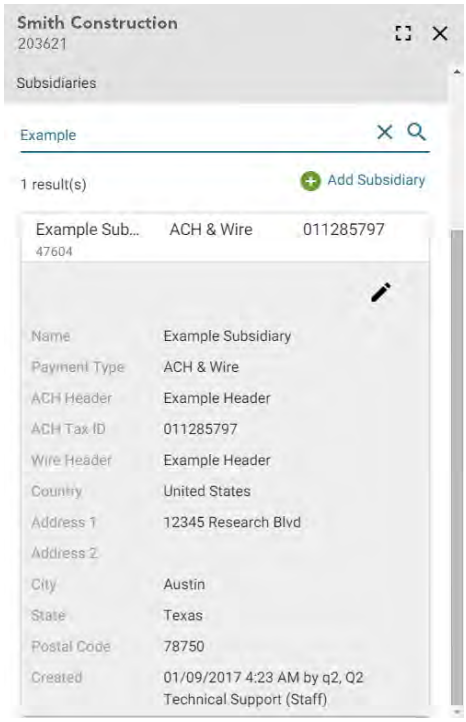
5. Click **Save**.

Note: Required fields depend on the Payment Type.

Viewing subsidiary details

FI staff can view details about an Organization's various subsidiaries, such as when each subsidiary was created, on the Subsidiary Details pane.

Subsidiary Details pane



To view subsidiary details

1. After locating the Organization that owns a subsidiary (see "Searching for an Organization" on page 269), click the subsidiary in the Organization pane.

2. Click a subsidiary to display details about it on the Subsidiary Details pane.
3. (Optional) If an Organization owns many subsidiaries, narrow search criteria further.
   a. Enter all or part of a keyword or phrase in the search bar. You can also search by Group, Tax ID, or CIF.
   b. Click the Search icon ( ) to return a list of results.

Editing a subsidiary

To edit a subsidiary

1. On the Subsidiaries page, navigate to the Organization that owns the subsidiary. See "Searching for an Organization" on page 269.
2. In the Organization Details pane, scroll to the Subsidiaries section.
3. Navigate to the subsidiary and select it.
4. Click the Edit icon ( ).
5. Make the necessary changes on the Edit Subsidiary page.
6. Click **Save**. A message appears to confirm changes to the subsidiary.

Deleting a subsidiary

Caution: Deleting a subsidiary is permanent and cannot be undone.

To delete a subsidiary

1. On the Subsidiaries page, navigate to the Organization that owns the subsidiary. See "Searching for an Organization" on page 269.
2. In the Organization Details pane, scroll to the Subsidiaries section.
3. Navigate to the subsidiary and select it.
4. Click the Edit icon ( ).
5. Click the Delete icon ( ) on the Edit Subsidiary page.
6. When a confirmation window appears, click **Delete**. A message appears to confirm that the subsidiary was deleted.

Section III - Configuration

This section provides you detailed information about features in the Configuration menu that you can use to customize and maintain Transaction Codes and Transaction Code Groups that are internal to your FI.

CHAPTER 17: TRANSACTION CODES

This chapter builds on the previous chapter and provides the framework for creating and maintaining your Transaction Codes in Q2central. It includes the following sections:

- "Transaction Codes overview" on page 273
- "Transaction Code reference" on page 273
- "Transaction Code Tasks" on page 276

Transaction Codes overview

The Transaction Codes option is a place where your FI can establish user-friendly names for transaction codes (also called *tran codes*), which describe the activities and transactions end users conduct at your FI. Transaction codes set up in Q2central are used to describe incoming activity brought in from the core, which will appear with historical transactions in online banking.

For example, a withdrawal via ATM may have a different transaction code from an in-branch withdrawal from a teller, and assignment of distinct transaction codes can reflect this difference in what the end user sees.

Transaction Code reference

The New or Edit Transaction Code page allows you to describe a Transaction Code to represent an activity or transaction type. End users can see the Transaction Code in transaction history. For background information, see "Transaction Codes overview" on page 273.

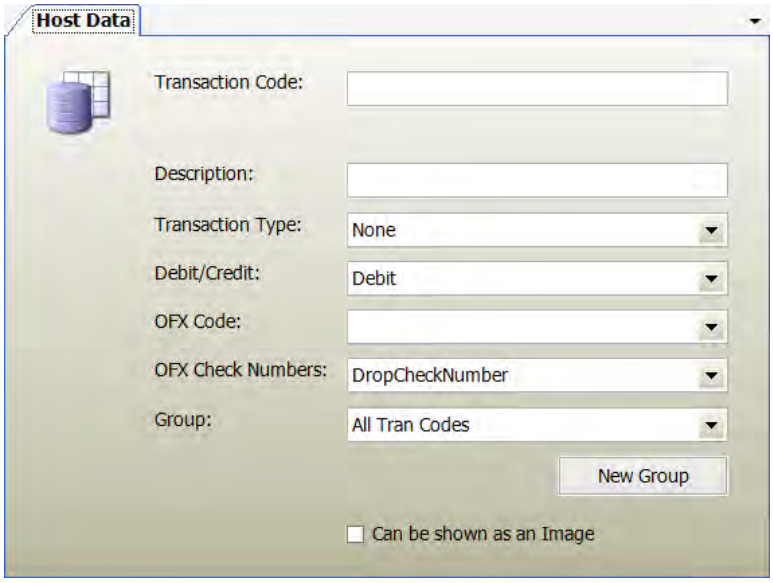


Tip: Plan Transaction Code Groups and Transaction Codes before adding them in Q2central.

New or Edit Transaction Code page

Complete the Host Data tab when entering or editing a Transaction Code.

Transaction Code Host Data tab



New Transaction Code page options

Option	Description
Transaction Code	The code or name for this transaction or activity type that is visible to FI staff within Q2central. Transaction codes must be unique within a Transaction Code Group.
Description	The name for this transaction or activity type that is visible to end users. The name here is displayed only if the core does not provide a description.
Transaction Type	Select from the options set up for your FI at implementation. Common options are Check, ATM, POS, EFT, DirectDeposit, or SystemGeneratedMemo.
Debit/Credit	Select one to represent the Transaction Code. Remember that a debit is a transaction that withdraws funds from another account; a credit is a payment to another account.

New Transaction Code page options (cont'd)

Option	Description
OFX Code	Provide the code that you want to appear in an Open Financial Exchange (OFX) file to which this activity may be exported by the user. This code may also be used by an OFX-format-compliant vendor, often Intuit. The code indicates whether the item is a debit or a credit. For debits, select Generic Debit here. For credits, select Generic Credit.
OFX Check Numbers	This setting indicates how your FI wishes to port the check number to the third-party (often Intuit) OFX file, if at all. • Drop Check Number removes the check number from showing in the Intuit product, so Quickbooks and Quicken show only the transaction description from the core. • Change transaction type to check is used the most for checks; it places the check number in the Check # column in the Intuit product. • Append to description adds the check number after the description in the Intuit product, so Quickbooks and Quicken display the core description and the check number. • Prepend to description adds the check number before the description in the Intuit product, so Quickbooks and Quicken display the check number and the description.
Group	Select the Transaction Code Group to associate with this Transaction Code. Your FI may establish whatever system you choose for organizing transaction codes. For example, one group could be for savings-related transaction codes. See "Transaction Code Groups overview" on page 278.
New Group	Displays the New Transaction Code Group page to add a Transaction Code Group to the Group list. See "Transaction Code Groups overview" on page 278.
Can be shown as an image	Enables the end user to view an image of this item in online banking. Enable this only for items with associated images, such as a check.

Transaction Code Tasks

The following are the most common tasks you can perform when working with Transaction Codes:

- "Adding a Transaction Code" on page 276
- "Editing a Transaction Code" on page 276
- "Deleting a Transaction Code" on page 277

Adding a Transaction Code

To add a Transaction Code

1. In the workspace tree, click **Configuration > Transaction Codes**.
2. In the list of All Tran Codes Transaction Codes that appears, right-click and click **New Transaction Code**.
3. In the New Transaction Code window, complete the following:
   a. Enter the **Transaction Code**.
   b. Enter a **Description**.
   c. Select a **Transaction Type** from the drop-down list.
   d. Select **Debit/Credit** from the drop-down list.
   e. Select an **OFX Code** from the drop-down list.
   f. Select an **OFX Check Number** from the drop-down list.
   g. Select a **Group** from the drop-down list, or click **New Group** to add a new Group for the Transaction Code.
   h. Click **Save and Close**.



Note: To learn more about these fields, see "New or Edit Transaction Code page" on page 274. To learn about creating a Transaction Code Group, see "Adding a Transaction Code Group" on page 279.

Editing a Transaction Code

To edit or view a Transaction Code

1. In the workspace tree, click **Configuration > Transaction Codes**.
2. When a list of all Transaction Codes appears, double-click a row, or, right-click and choose **Edit Transaction Code**.
3. Make any necessary changes and click **Save**.

Deleting a Transaction Code

To delete a Transaction Code

1. In the workspace tree, click **Configuration > Transaction Codes**.
2. When a list of all Transaction Codes appears, select the code you want to delete, right-click and click **Delete Trancode**.
3. Click **Yes** to confirm the deletion.

CHAPTER 18: TRANSACTION CODE GROUPS

This chapter provides you with the foundation for configuring Transaction Code Groups in Q2central. It includes the following sections:

- "Transaction Code Groups overview" on page 278
- "Transaction Code Group reference" on page 278
- "Transaction Code Group tasks" on page 279

Transaction Code Groups overview

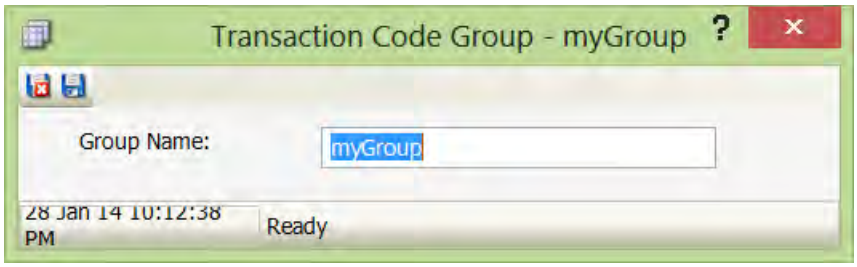
Transaction Code Group is simply a grouping by which you can sort Transaction Codes. Each Transaction Code Group is identified by a name that you assign and a system-generated ID number. This is a very open feature that your FI may adapt to meet its needs.

Transaction Code Groups are not visible to end users, but the Transaction Codes they contain are.

Transaction Code Group reference

The Transaction Code Group consists of the following page.

Transaction Code Group page



Transaction Code Group tasks

The following are the common tasks you perform with Transaction Code Groups:

- "Adding a Transaction Code Group" on page 279
- "Editing a Transaction Code Group" on page 279
- "Deleting a Transaction Code Group" on page 279

Adding a Transaction Code Group

To add a Transaction Group

1. In the workspace tree, click **Configuration > Transaction Code Groups**.
2. In the All Tran Codes list that appears, right-click and select **New Transaction Code Group**.
3. When the New Transaction Code Group window appears, enter a **Group Name**.
4. Click **Save and Close**.
   The new Transaction Code Group is available to any Transaction Code you add or edit.

Editing a Transaction Code Group

To edit a Transaction Code Group

1. In the workspace tree, click **Configuration > Transaction Code Groups**.
2. In the list that appears, select the record you want to edit, right-click and click **Edit Trancode Group**.
3. In the Transaction Code Group window, change the **Group Name** for the selected group.
4. Click **Close and Save**.

Deleting a Transaction Code Group

To delete a Transaction Code Group

1. In the workspace tree, click **Configuration > Transaction Code Groups**.
2. In the All Tran Codes list that appears, select the Transaction Code Group you want to delete.
3. Right-click and click **Delete Trancode Group**.
4. Click **Yes** to confirm the deletion.

CHAPTER 19: FEE PLANS

This chapter includes the following sections:

- "Fee Plans overview" on page 280
- "Fee Plan reference" on page 283
- "Fee Plan tasks" on page 285
- "Generating fees and Fee Plan processing" on page 287
- "Supplemental information" on page 291

Fee Plans overview

Financial institutions (FI) can create Fee Plans for assessing charges for online banking features, which are created and administered via the User Management > Fee Plans option in Q2central.

The Q2platform provides flexibility regarding Fee Plans that allow an FI to charge separately for monthly access to a service, as well as for usage of that service. (For example, an FI may charge a monthly fee to each commercial user who wants the ability to perform wire transfers and can also charge a fee for each wire transfer conducted.) This flexibility allows for greater customization of Fee Plans and can mean potentially higher revenue for an FI.

Fee Plans can be configured for almost any system event that can be tracked by the Q2platform, including access to and usage of single sign-on (SSO) interfaces such as Bill Pay. Fee Plans can also be added for individual transaction types (Wire Transfers, ACH Single Payment, ACH Collections, ACH PassThru, etc.), as well as the components of those Transactions Types (ACH Debit and ACH Credit).

Each FI should consult with Q2 to discuss the different ways that the Fee Plan structure can be created and managed to:

- Optimize the structure of Fee Plans so that they can be used across multiple lines of business.
- Ensure that the final arrangement does not result in erroneous charges.
- Determine how much custom development, if any, is required to meet the FI's billing needs, as well as how much the custom development will cost.

For more information about Fee Plans, contact your Q2 Relationship Manager.

Note: The Additional Use Fee for SSOs is applied each time a user accesses an SSO interface, such as Bill Pay. Q2 cannot count third-party transactions that the end user initiates from within an SSO.

Fee Plan maintenance

This section describes Fee Plan maintenance and contains information on Fee Plan Setup window settings and viewing, editing, creating, copying, and deleting Fee Plans.

Configuring the Fee Plan Setup window

This topic describes controls on the Fee Plan Setup window.

Monthly fees

The Monthly Fees grid provides a way to add or edit fees for all Customers to whom this fee plan applies. Fees are always calculated per full calendar month. Columns may vary depending on your configuration.

Fee Plan Setup window columns

Column	Description
Fee Description	Shows the list of services to which you may assign fees. This list is unique to your FI, and consists of the services established in your system's database at implementation.
Base Fee	Specify the monthly dollar amount that your FI charges to make the service available to the Customer. Another name for this is access fee. If the Charge Base Only If Used option is enabled, then this fee is applied only if the Customer actually used this service at any point during the month.
Number Free	Specify the number of events per month that your FI provides the Customer at no charge before applying the Additional Use Fee.
Additional Use Fee	Specify the per-item fee that your FI charges after the Number Free is exceeded. This counter resets each month.

Fee Plan Setup window columns (cont'd)

Column	Description
Charge Base Only If Used	Enable this control if you wish to waive the base fee for a particular service in months when the Customer does not use that service.

Note: The Potential Base Fee Total displays the sum of amounts in the Base Fee column. It assumes that the base fee was not waived for any services. Use the total to quickly assess the value of this fee plan without adding fees manually; it includes fees that may not be visible without scrolling.

A Monthly Plan Charge section also appears in the Fee Plan Setup window.

Monthly Plan Charge

Field	Description
Initial Plan Months	Specify the number of free months a Customer receives under this plan before all fees take effect.
Base Customer Fee	Specify a flat fee this Customer is charged each month. This is separate from (not included in) the Potential Base Fee Total.
Maximum Monthly Fee	Specify an amount to cap the fees a Customer pays. If this is 0.00, no fees are charged. All fees on this window are subject to the maximum, including all Monthly Fees and the Base Customer Fee.

Monthly Plan Charge (cont'd)

Field	Description
Unlimited	Enable this if you want the system to charge all available fees and ignore an amount in the Maximum Monthly Fees box. If you provide Initial Plan Months, be aware that if you change the charges on this fee plan in the future, the system treats the amounts in the fee plan as new. As a result, the system resets its count of how long the Customer has been assigned to this fee plan. The system honors the Initial Plan Months by waiving fees for the number of full months indicated.

What does "per item" mean?

Usually, an "item" refers to each credit or debit in an ACH file. That is, an ACH Payroll file paying 20 employees would have 20 credits and at least one debit, resulting in 21 chargeable items. Whether your FI charges the same fee for credits and debits alike depends on your configuration.

You can configure your system's counter to charge per transaction type instead of at the level of individual credits and debits. In this scenario, an ACH Payroll file would incur the same fee regardless of whether it contains one credit or 20.

Fee Plan reference

This section describes some of the terminology used in the Fee Plan Setup window.

Monthly base fees versus usage fees

The Fee Plan Setup window allows you to charge separately for monthly access to a service and for usage of that service. For example, an FI may charge a monthly fee to each commercial end user who wants the ability to make wire transfers and can also charge a fee per wire transfer conducted. This allows for greater customization of fees to meet end user expectations and can mean potentially higher revenue for the FI.

Custom fees for auditable events

FIs can create custom fees for almost any system event, including access to and usage of SSOs. We can consult with you to add a fee type for nearly any end-user-initiated activity that can be tracked by Q2platform, providing a means of assigning fees per month and/or per event. (Customization charges apply.) Note that the Additional Use Fee column for SSOs is applied to each click into the SSO application; Q2 cannot count third-party transactions that the end user initiates while interacting with the SSO application.

Charge only if used option

If your FI elects or is contractually obligated to refrain from charging a monthly access fee for a service that was not used during the month, the Fee Plan Setup window supports that practice. On a line-item basis, you can choose to turn off the monthly access fee automatically when no usage is recorded during that month. This is especially useful with Consumer or small-business end users who do not have a high usage volume and may respond negatively to the monthly access charge in months of no usage.

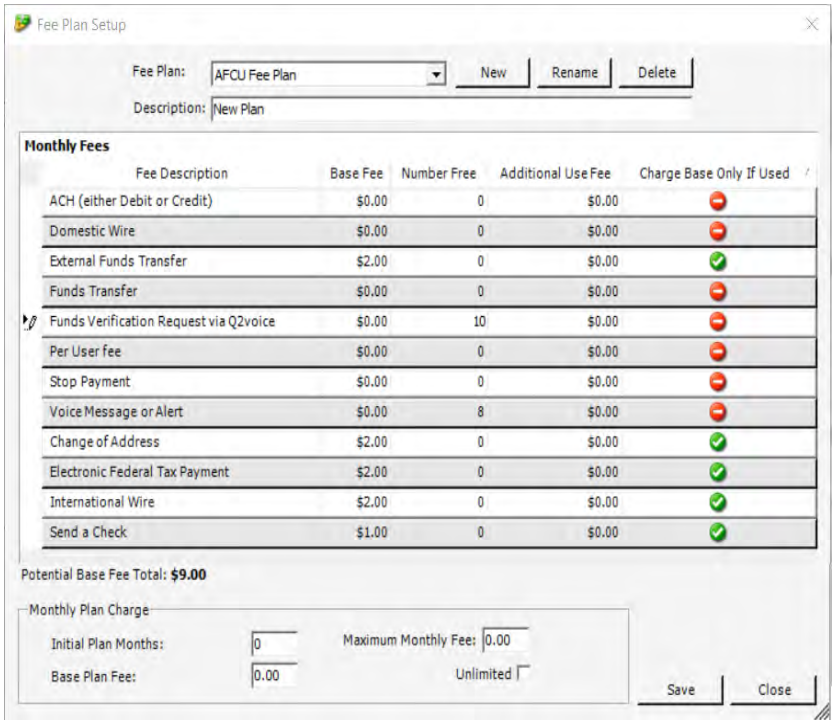
Potential base fee income summary

At a glance, you can view the projected minimum value of a particular fee plan by viewing the Potential Base Fee Total. These totals show the potential earnings from this fee plan if all specified base fees are applied. Not only does this help you to quickly evaluate the plan's value, it also saves you the effort of manually adding up base fees.

Fee Plan Setup window

The Fee Plan Setup window allows you to view all Fee Plans in the system, or to edit or rename a Fee Plan. Before editing a Fee Plan, you may wish to generate a report of all Customers to which it applies by running the Fee Plans Report. In addition, be aware that if you edit a Fee Plan and a Customer has been assigned Initial Plan Months, the system may count the Fee Plan as new and waive fees.
See "Applying a Fee Plan to a Customer" on page 287.

Fee Plan Setup window



Fees are always calculated per full calendar month. All entries are optional. For Fee Plan Setup options, see "Configuring the Fee Plan Setup window" on page 281.

Fee Plan tasks

This section contains the most commonly performed tasks for Fee Plans. These tasks include the following:

- "Creating a Fee Plan" on page 286
- "Copying a Fee Plan" on page 286
- "Viewing or editing a Fee Plan" on page 286
- "Deleting a Fee Plan" on page 287
- "Applying a Fee Plan to a Customer" on page 287
- "Viewing output files for processed activity" on page 290

Creating a Fee Plan

This section describes how to create a new Fee Plan without copying values from another Fee Plan.

To create a new Fee Plan

1. In the workspace tree, click **User Management > Fee Plans**.
2. Click **New** to display the Fee Plan Name window.
3. Enter a new name for this fee plan, then click **OK**.
4. On the Copy Fee Plan window, click **No**.
5. On the Fee Plan Setup window, in the Description field, enter a Fee Plan description. When writing a description, state what makes this Fee Plan different from others in the system.
6. Complete the monthly fee settings. See "Configuring the Fee Plan Setup window" on page 281.
7. Click **Save**, then click **Close**.

Copying a Fee Plan

To copy a Fee Plan

1. In the workspace tree, click **User Management > Fee Plans**.
2. In the Fee Plan chooser, select a Fee Plan that is similar to the one you want to create.
3. Click **New** to display the Fee Plan Name window.
4. Enter a name for the Fee Plan, then click **OK**.
5. On the Copy Fee Plan window, click **Yes**. The Fee Plan Setup window displays the new name with values from the other Fee Plan.
6. In the Description field, explain the purpose or application of this Fee Plan. State what makes this Fee Plan different from others in the system.
7. Complete the monthly fee settings. See "Configuring the Fee Plan Setup window" on page 281.
8. Click **Save**, then click **Close**.

Viewing or editing a Fee Plan

To view or edit a fee plan

1. In the workspace tree, click **User Management > Fee Plans**.
2. In the Fee Plan chooser, select a Fee Plan. Fields on this window update automatically when you select a different fee plan.
3. If you wish to rename the current plan, click **Rename**.

4. Enter a new name, then click **OK**. Customers previously assigned to the old name are retained under the new name. Processing output history referencing the old name is not updated.
5. In the Description field, view or edit the description.
6. View or edit the monthly fee settings. See "Configuring the Fee Plan Setup window" on page 281.
7. Click **Save**, then click **Close**.

Deleting a Fee Plan

Use the Fee Plans Report to identify all Customers to which the Fee Plan currently applies. Reassign the Customers to other Fee Plans as described in "Applying a Fee Plan to a Customer" on page 287.



Caution: You cannot delete a Fee Plan to which Customers are assigned.

To delete a Fee Plan

1. In the workspace tree, click **User Management > Fee Plans**.
2. Select the fee plan that you want to delete from the Fee Plan chooser.
3. Click **Delete.** The Delete Fee Plan window appears.
4. Click **Yes** to confirm deletion.
5. Click **Save**, then click **Close**.

Generating fees and Fee Plan processing

This section outlines applying a Fee Plan to a Customer, Fee Plan processing, and the available options.

Applying a Fee Plan to a Customer

Only one Fee Plan may be associated with a Customer. After you associate a Fee Plan with a Customer, that Customer's fees for the previous month may be calculated, applied to the account indicated, and reflected in the processing output file.



Note: Other processing options are available; see "Fee Plan processing options" on page 290.

Fees are recognized and calculated per calendar month. If a Customer goes live at any point in the month, and you wish to charge for a partial month's fees, Q2central captures and includes these in the file for that month. The next billing cycle then begins on the first of the next month.

To apply a fee plan to a Customer

1. Create the fee plan, if necessary.
2. In the workspace tree, click **User Management > Customers**, then search for the Customer record to which you wish to apply a Fee Plan.
3. Double-click the name of the Customer.
4. On the General tab, use the Fee Plan drop-down menu to choose the Fee Plan you want to apply.
5. To review the details of the Fee Plan, click **View**.
6. Use the **Effective Date** chooser to select the first full month that is to be counted for fee purposes.



Note: If you assign a Fee Plan that provides Initial Plan Months at no cost, the system suspends fees for the number of months indicated, starting with the month you choose here.



Note: It is important to use the Charge Account chooser to select the account that will receive the debits created when fees are processed at month-end.



Tip: Communicate with end users that this account will be used for all charges incurred by any account this Customer owns. For example, if a Customer performs a Stop Payment on a check written against Account 1234 (and is charged a fee for Stop Payments), the fee will be deducted from Account 1235, if that is the Charge Account specified here. Some end users may require this explanation.



Note: You can preview the potential revenue from this Customer in the Fee Plan Calculations Report.

Processing Monthly Fees

The Process Monthly Fees menu option creates an ACH file that contains the accumulated monthly service charges for each Customer based on the charge plan assigned.

You can run monthly fees at any point during the month to see what has accumulated so far without debiting your Customer's account. As you run it during the month, the report grows. It restarts incrementation the first day of each month. For example, if you select to process the previous month's fees on any day in August, fees are calculated for activities performed between July 1 and July 31 inclusive.

It is important to understand that:

- If a Fee Plan was applied to a Customer on July 8, none of that Customer's fees from July are included in the August processing session.
- If a Fee Plan was applied to a Customer on June 8, all of the July fees and none of the June fees are included in the August processing session.

The default is for the previous month, but you may choose another month or year to run.

To process monthly fees

1. In Q2central, navigate to **Transactions > Process Monthly Fees**.
2. Choose the month whose fees you want to process.
3. If needed, choose the year whose fees you want to process.



Tip: Month and Year are separately selected fields.

4. Click **Process**.

Q2central generates output files and places them in the Temp Directory specified on the **Transactions > ACH Management** tab. The Batch Information window appears and displays details about the batch file.

The files generated include:

- An ACH File to charge all Customers for the fees generated. If your process includes this, you may upload the file directly into your core banking software to withdraw funds.
- A List file (.rpt extension) of the detailed charges incurred by each

Customer.
- An Exception file of the Customers that did not incur any charges or who did not have a valid account to charge.

Fee Plan processing options

Q2central supports your fee billing options, whether your FI handles billing in house or via third-party account analysis software.

To apply hard charges from the core

1. Process Fee Plans at month end. See "Processing Monthly Fees" on page 289.
2. Retrieve the ACH output file.
3. Submit the ACH file to the core as you would any other; all transactions will be contained within the FI as "on-us" transactions.

To use third-party account analysis, Q2 offers custom outputs to meet the specifications of your third-party account analysis software. These can include fixed-length or delimited files in the format you need. Please provide file format specifications when you make your request for customization. Contact your Q2 Relationship Manager (RM) for details.

Custom Fee Plan output files are retrievable in Q2central along with standard output.

Viewing output files for processed activity

There are several processing activities that yield output (history) files documenting the information that was processed. These are available indefinitely for viewing in Q2central.

To view output for fee plan processing

1. In Q2central, navigate to **Transactions > Process History**.
2. Make sure Field Chooser shows at least Name, CSR, Result, and Start Date.
3. Set the search fields to **Name > Begins With**, then type `Fee`.
4. Click **Search** to list available processing events.
5. Find the date of the fee plan charges you processed.
6. Verify the charges are at Complete status with no errors.
7. Double-click the row to display the Batch Information window.
8. Click the **Output** tab.

9. Double-click the row that shows the report type you want to view:
    - .ach – Lists processed fees in fixed-length NACHA format.
    - .rpt – Lists processed fees in non-delimited format.
    - .exceptions – Lists Customers to whom fees are not charged due to lack of usage or a missing debit account.
    - [custom file format] – Provides fees and usage, usually without calculations, suitable for import to a third-party account analysis software.

Oversee Fee Plan activity

Q2central tracks actual consumer usage to enable you to charge for services and provides a few ways to oversee fee plan activity:

- Process output describes actual historical usage and the fees that were in place when the activity occurred.
- Fee Plan Report lists Customers currently assigned to each Fee Plan.

Refer to the *Q2central Reporting Guide* for details.

Supplemental information

This section includes more details about Fee Plans.

Credit and debit definitions

Q2central uses the following definitions for credits and debits:

Credit and Debit Definitions

Description	Originating Account	Foreign Account
ACH Payments	Debit	Credit
ACH Collections	Credit	Debit
ACH Single Payment	Debit	Credit
ACH Single Receipt	Credit	Debit
EFTPS	Debit	Credit
Payroll	Debit	Credit

Note: ACH PassThru is not defined here because it may contain multiple originating accounts.

Fee types in Q2central

You can charge fees for user-initiated transactions and audited events in Q2central. When you set up fees for receipt and payment transactions, be aware that fees apply only to situations where an end user actively pulls funds from someone else's external account, or where a funds transfer occurs. That is, fees are applied to movement of money that is active and user-initiated, not passively received.

Note: Only transactions that reach Processed status are counted.

FIs can create custom fees from almost any system event, including access to and usage of the SSOs. We can consult with you to add a fee type for nearly any end-user-initiated activity that can be tracked by Q2platform, providing a means of assigning fees per month and/or per event. (Customization charges apply.)

Note: The **Additional Use Fee** column for SSOs is applied to each click into the SSO interface; transactions that the end user initiates while interacting with the SSO interface cannot be tracked.

If your account analysis strategy requires more granular transaction types, these are available. Contact your Q2 Relationship Management team to inquire about custom development.

Two Fee Plan reports are available: the Fee Plans Report and the Fee Plans Calculation Report. Refer to the *Q2central Reporting Guide* for details.

Below is a list of default fee types on the Fee Plan Setup window. Your FI may not offer all of them, and probably includes many more. In addition, your installation may show slightly different names.

Default Fee Types

Fee Type	Description
ACH - Either Debit or Credit	This is a NACHA-formatted payment or receipt transaction in which the end user's account is debited or credited and one or more external accounts are credited or debited accordingly. The following end-user-facing options are covered by this transaction type: ACH Credit, ACH Debit, ACH Payments, ACH Collections, ACH Payment or ACH Single Payment, ACH Receipt or ACH Single Receipt, ACH PassThru, EFTPS, Payroll.
Change of Address	This event is triggered when the end user's address is changed in Q2central.
Domestic Wire or Wire Transfer	This is a single payment transaction in which the end user's account is debited and an external (non-international) account credited.
EFTPS	This is a single payment transaction in which the end user's account is debited and a single external (taxation entity) account is credited. The mechanism for transferring the payment is the Electronic Federal Tax Payment System.
External Funds Transfer	This is a single receipt or payment transaction in which an end user's account is credited or debited and an external account is debited or credited accordingly. The fee report makes no distinction among external funds transfers that were receipts and those that were payments. The following end-user-facing options are covered by this transaction type: External Funds Transfer Debit, External Funds Transfer Credit.
Funds Transfer or Internal Funds Transfer	This is a transaction in which a Customer's account is debited and another account belonging to the same Customer within the same FI is credited.

Default Fee Types (cont'd)

Fee Type	Description
Funds Verification Request	This is an event in which a merchant uses Q2voice to verify sufficient funds in the end user's account. This option is used only by FIs that purchase Merchant Services as a supplemental feature to Q2voice. To use Merchant Services, local merchants must be set up by your FI as Customers, Users and Logins. The merchants log in with their login names and passwords and can enter any account numbers they wish. To limit the number of verifications, set a limit for the Merchant Verification transaction type (if listed) at the Group or Customer level. **Note:** Merchant Services is not part of the standard offering; it is a separately purchased feature.
International Wire or International Wire Transfer	This is a single payment transaction in which the end user's account is debited and an international account credited.
Send A Check	This is a single payment transaction in which the end user's account is debited and a physical check is mailed to the end user.
Stop Payment	This is a request from an end user to prevent the FI from honoring a previously requested payment. If the FI has not disabled the "For Multiple Checks" option in Q2online, then a single stop payment request may cover multiple checks for the same fee as one that covers a single check.

Default Fee Types (cont'd)

Fee Type	Description
Voice Message or Alert	This fee is based on the number of times an automated alert or voice message was issued in response to a schedule or events that the end user set up as requiring an alert. In Q2online end users set up personal alerts in the Preferences > Alerts menu and security alerts in the Preferences > Security > Alerts menu. Note that there is not a way to charge a fee for personal alerts while exempting security alerts. Your FI may wish to encourage enrollment in security alerts by suspending this fee.
Per User	This fee is based on the number of users in a Company as of the last day of the month. This counts users, not logins. A user's record is not counted only if it contains a deleted date.

Section IV - Communication

Communication in Q2central offers several areas of functionality. One area—Secure Messaging—provides FI staff with the ability to send messages to end users, as well as receive messages from end users. You can also create templates that contain boilerplate text that FI staff can use when corresponding with end users, as well as display secure message history.

The second area of Communication functionality is Marketing Messages that include *Ad Elements* and *System Notifications*. You can use them to communicate to end users through images and messages that appear in online banking.

These messages help you to differentiate your FI to your end users. With Q2central Communication features, it is easy to stay in contact with your end users and receive their requests for assistance.

If your FI opted to include Secure Message templates during implementation, a Select Template button appears on the message window when you reply to a secure message. You can edit the boilerplate text, as necessary.

CHAPTER 20: SECURE MESSAGING

The Secure Messaging functionality in Q2central provides two-way, secure communication between your end users and any message groups established at your FI.

This chapter includes the following sections:

- "Secure Messaging overview" on page 297
- "Secure Messaging reference" on page 301
- "Secure Messaging tasks" on page 308

Tip: The Read Date displayed for a secure message reflects the last date the message was read by FI staff, not the date that the message was originally received.

Secure Messaging overview

Using Secure Messaging ensures that end users always have a way to contact you and that you can respond to them quickly and confidentially, allowing you to provide the best customer service experience possible.

End users can access secure messages via the Conversations menu option (or the Messages menu, depending on the FI) in Q2online and Q2mobility Apps. FI staff can access secure messages sent by end users via the Communications > Secure Messaging option in the Q2central workspace tree.

When end users send secure messages, they select the category that best matches the topic of the message (for example, Customer Service). In Q2central, those categories are known as *Secure Messaging groups* that determine which FI staff will receive the messages. (For example, CSR Users enrolled in the "Report Lost or Stolen Card" group receive messages that end users send to that category from within online banking.) You can also create Secure Message templates with boilerplate text that can be used to respond to messages. To learn more about Secure Messaging groups and templates, see "Configuring Secure Messaging" on page 298.

There are many ways to send secure messages to end users—you can send a message to all end users, or to a specific Group, Customer, User, or Login ID. See "Sending secure messages" on page 308 for details.

To view messages sent by end users, click **System Alerts > New Messages** in the workspace tree. See "New Messages overview" on page 340.

For a list of Secure Messaging tasks, see "Secure Messaging tasks" on page 308.

Configuring Secure Messaging

During the implementation of your online banking system, several Secure Messaging groups were defined depending on your FI's needs. Standard groups include:

- Customer Service
- Report a Lost/Stolen Card
- Payroll Services
- Wire Transfer Services

Your first step in setting up Secure Messaging is to assign CSR Users to the Secure Messaging groups so you can control which FI staff receive messages sent by online banking end users.



Note: To manage Secure Message permissions for Groups or CSR Users, you must be assigned a CSR Role with the *ADMINISTRATION: Message Group Members* permission enabled.

There are two ways to add CSR Users to a Secure Messaging group:

- Using the Manage Secure Messaging page. See "Editing Secure Messaging groups for FI staff" on page 299.
- Using the CSR Users page. See "Enrolling CSR Users in Secure Messaging groups" on page 32.

You can also control the Groups that have access to different types of secure messages on the Group page's Preferences tab. See "Editing a Group" on page 179 for details. The ability for end users to attach files to secure messages is enabled, by default, but can be disabled during implementation or later via a Q2 Customer Support request.

Editing Secure Messaging groups for FI staff

To edit or view the Secure Messaging groups to which FI staff belongs

1. In the workspace tree, click **Administration > Manage Secure Messaging**.
2. In the Manage Secure Messaging list, select **View By CSR** at the top of the page.
3. In the box in the upper left, select the FI staff person you want to look up. The results pane lists the CSRs, the Secure Messaging groups (Group Name), and the membership status (Enrolled).
4. In the Enrolled column, click the icon to add or remove a member.
5. Click **Save**.

Editing or viewing Secure Messaging group membership

To edit or view the membership of a Secure Messaging group

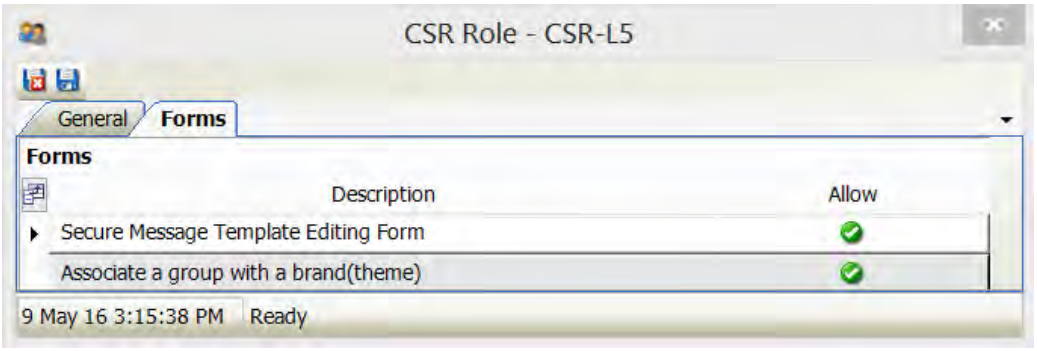
1. In the workspace tree, click **Administration > Manage Secure Messaging**.
2. In the Manage Secure Messaging list, select **View By Topic** at the top of the page.
3. In the box in the upper left, select the Secure Messaging group whose membership you want to see.
   The results pane lists the CSR Name column listing all FI staff and the Enrolled column indicating membership status.
4. In the Enrolled column, click the icon to add or remove a member.
5. Click **Save**.

Secure Message templates overview

If the Secure Message template feature is enabled for your FI, you can create templates with boilerplate text that CSRs can use to quickly respond to messages from end users.

The first step in setting up templates is to provide access to the Message Template Management page to a select group of CSRs. On the Forms tab of the **Administration > CSR Roles** page, enable the *Secure Message Template Editing form* option for a CSR Role, as shown in the following figure.

CSR Roles page — Forms tab



The Message Template Management page, accessible from the Q2central workspace tree by clicking **Communication > Message Templates**, includes two tabs:

- Use the Categories tab to organize Secure Message templates into groups. These categories will appear on the message window when a CSR replies to or forwards a message in the **System Alerts > New Messages** page.
- Use the All Templates tab, which lists all Secure Message templates regardless of category, to add and delete templates.

Note the following details about Secure Message templates:

- Click **Add Template** on the All Templates tab to add a new template.
- On the All Templates tab, click the Edit icon (✎) next to a template to change the text. Click **Save** when finished.

> ⚠ **Caution:** If you delete a template, all Q2central history related to that template (for example, who created it) will be lost.

- You can rename, but not delete, template categories.
- If you remove all templates from a category, the category will not appear as an option on the Message window.
- When a CSR User adds template text to a message, the template text only affects the immediate text field that becomes available for editing during the secure message reply workflow.

See "Using Secure Message templates" on page 345 for step-by-step instructions.

Secure Messaging reference

The following table outlines the various areas in Q2central where Secure Messaging features can be accessed.

Secure Messaging features

Q2central Area	Description
System Alerts > New Messages	Display a list of secure messages sent from end users. See "New Messages overview" on page 340.
User Management > Groups	To send a broadcast message to a specific Group, select the Group and press F10. See "Sending a secure message to all Users in a Group" on page 310. You can also control which types of secure messages are available for a Group on the **Group > Preferences** tab.
User Management > Customers	To send a broadcast message to a specific Customer, select the Customer and press F10. See "Sending a secure message to all Users linked to a Customer" on page 311.
User Management > Users	To send a message to a specific User, select the User and press F10. See "Sending a secure message to a single user" on page 312.
User Management > Logins	To send a message to a specific Login, select the Login and press F10. See "Sending a secure message to a login ID" on page 313.
Communication > Secure Messaging	Provides a list of all unexpired secure messages sent by both end users and FI staff. See "Viewing secure messages" on page 308.
Communication > Message Templates	Manage templates that FI staff can use to quickly respond to secure messages from end users. See "Secure Message templates overview" on page 299.
Administration > Manage Secure Messaging	View the Secure Messaging groups to which a CSR User belongs. You can also view the CSR Users that belong to a Secure Messaging group and then enroll or remove them from the group, as necessary. See "Editing Secure Messaging groups for FI staff" on page 299.

Secure Messaging features (cont'd)

Q2central Area	Description
Administration > Broadcast Message	Send a secure message to all end users in the system. See "Sending a secure broadcast message to all end users" on page 310.

Secure Messaging page

While the New Messages page (accessible via the **System Alerts** node in the workspace tree) shows only new, unread messages from end users, the Secure Messaging page shows both read and unread messages, as well as alerts.

To view all secure messages sent by end users from within online banking plus outbound messages sent by CSRs to end users and alert-related messages, click **Communication > Secure Messaging** in the workspace tree to open the Secure Messaging page.

Note the following details about the Secure Messaging page:

- Default values for Message Status on the Secure Messaging page are *Resolved* or *Unresolved*. However, an FI can request that more granular statuses (for example, "In a work queue/unresolved") be defined during implementation.
- To reduce the amount of messages displayed in the Secure Messaging page, your system can be configured to prevent copies of alert-related messages (for example, activity alerts sent to end users) from appearing on this page. Contact your Q2 Relationship Management (RM) team for details.



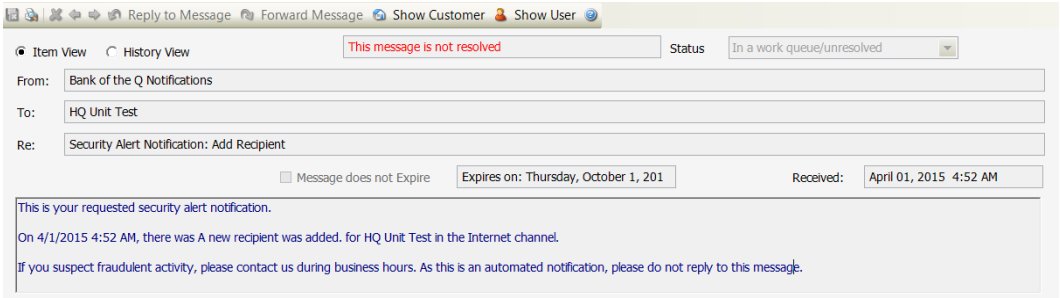
Tip: The Read Date displayed for a secure message reflects the last date the message was read by FI staff, not the date that the message was originally received.

Secure Message page views

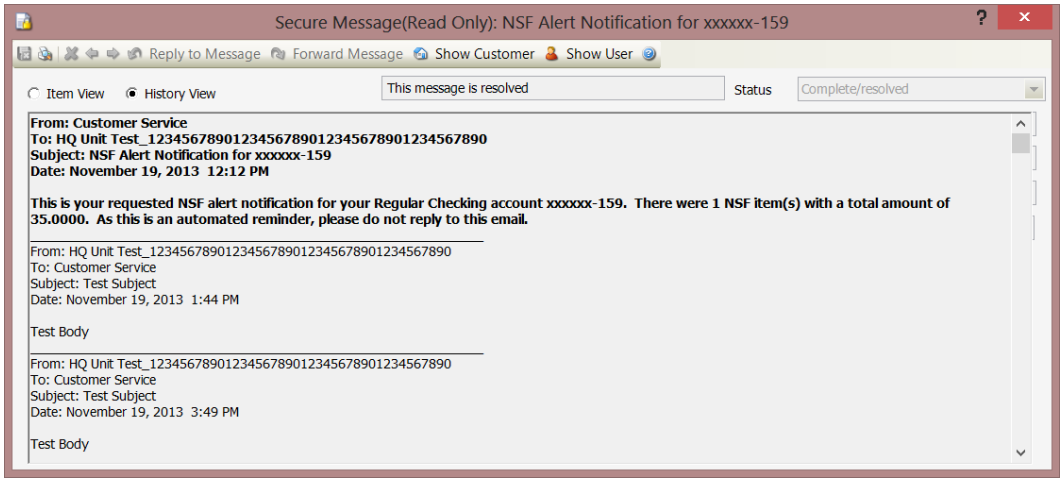
After you search for records on the Secure Messaging page and select a specific record, the Secure Message page appears. This page has two views:

- **Item View** displays the message itself, along with basic details such as the originator, recipient, and status.
- **History View** displays the originator, recipient, subject, and date.

Secure Message page (Item View)



Secure Message page (History View)



Note the following details about the Secure Message page:

- If you are not the original recipient of a message, the message is read-only and you cannot perform any actions that would change the status of the message.
- A message's Read Date reflects the last date that the message was read by FI staff, not the date that the message was originally received.

- The default values for Message Status on the Secure Messaging page are *Resolved* or *Unresolved*. However, your FI may have requested more granular statuses (for example, "In a work queue/unresolved") during implementation.
- There is no Send option on the Secure Message page. Instead, click **Save and Close** on the toolbar to reply to or forward a message.
- To reduce the amount of messages displayed on the Secure Messaging page, your system can be configured to prevent copies of alert-related messages (for example, balance alerts sent to end users) from appearing on this page. Contact your Q2 Relationship Management (RM) team for details.

Secure Message page (Item View) options

Option	Description
Status	The current status of the message. Default values are *Resolved* and *Unresolved* but your FI may have requested more granular statuses (for example, "In a work queue/unresolved") during implementation.
From	The originator of the message.
To	The message recipient.
Re	The subject of the message.
	This Save Attachment button appears if a message includes an attachment. Click this button to save an attachment to a local or network drive.
Message does not Expire	Select this check box to prevent a message from being deleted when the retention period expires. The default retention period is six months but an FI can change that value during implementation.
Received	The date the message was received.

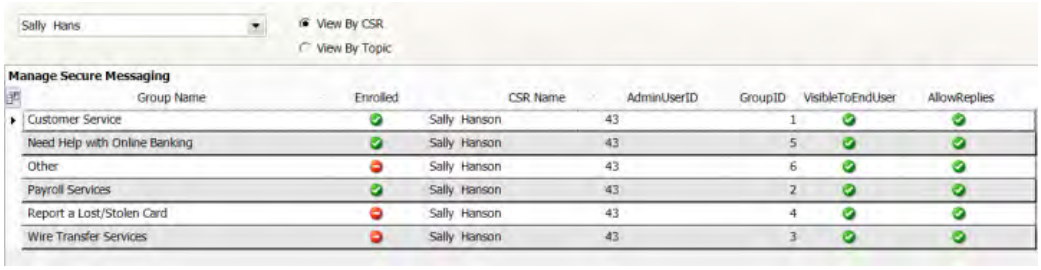
Managing Secure Messaging page

The Manage Secure Messaging page is similar to an interactive report about Secure Messaging groups. You can use it to add a CSR User to a Secure Messaging group and you can also use it to display a list of CSR Users that belong to a group.

To access the Manage Secure Messaging page, click **Administration > Manage Secure Messaging** in the workspace tree. The appearance of this page changes depending on whether the View by CSR or View by Topic option is active.

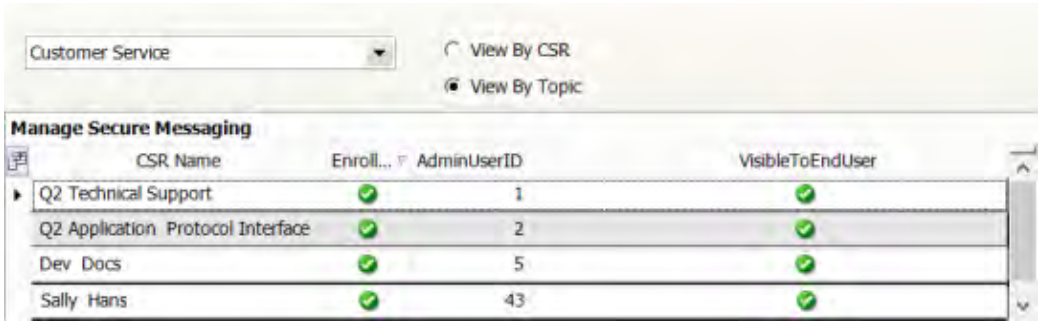
- At the top of the page, select a CSR User and click **View by CSR** to display the Secure Messaging groups to which the CSR User belongs. See "Editing Secure Messaging groups for FI staff" on page 299.

Manage Secure Messaging page (View by CSR)



- At the top of the page, select a Secure Messaging group and click **View by Topic** to display the CSR Users that belong to that Secure Messaging group. See "Editing or viewing Secure Messaging group membership" on page 299.

Manage Secure Messaging page (View by Topic)



Note the following details when working in the Manage Secure Messaging page:

- Adding or removing a CSR User to or from a Secure Messaging group on this page is equivalent to doing so on the CSR User record.
- To sort the values that appear in the Manage Secure Messaging page, click a column header.
- You can use the Field Chooser to add more columns to the Manage Secure Messaging page. See "Using the Field Chooser" on page 349.

Manage Secure Messaging page options

Option	Description
View By CSR	At the top of the page, select a CSR User from the drop-down listbox and click **View by CSR** to display the Secure Messaging groups to which the CSR belongs. See "Editing Secure Messaging groups for FI staff" on page 299.
View By Topic	At the top of the page, select a Secure Messaging group and click **View by Topic** to display CSRs that belong to that group. See "Editing or viewing Secure Messaging group membership" on page 299.
Manage Secure Messaging section (View By CSR option active)	
Group Name	The name of the Secure Messaging group.
Group Description	A description of the Secure Messaging group. **Note:** This field appears if the option was enabled during implementation and the field is selected in the Field Chooser. See "Understanding Secure Messaging group descriptions" on page 307.
Enrolled	Indicates if a CSR is enrolled in a Secure Messaging group.
Visible to End User	Indicates if end users can select the Secure Messaging group when sending messages from within online banking.
Allow Replies	Indicates if CSRs that are part of a Secure Messaging group can reply to messages sent by end users.
Manage Secure Messaging section (View By Topic option active)	
CSR Name	The name of the CSR that is a member of the Secure Messaging group selected in the top of the page.

Manage Secure Messaging page options (cont'd)

Option	Description
Enrolled	Indicates if a CSR is enrolled in a Secure Messaging group.
Email	The CSR's email address. If necessary, you can add an email address.
Group Description	A description of the Secure Messaging group.



Note: This field may not appear, depending on the system configuration and whether or not the field was selected with the Field Chooser. See "Understanding Secure Messaging group descriptions" on page 307.

Understanding Secure Messaging group descriptions

If your FI provided Secure Messaging group descriptions and Q2 enabled the *EnableMessageRecipientGroupToGroupManagement* property during implementation, you can display group descriptions on the following pages:

- Administration > CSR Users >Message Groups tab
- Administration > Manage Secure Messaging

To display that column, use the Field Chooser and select the *GroupDescription* option .See "Using the Field Chooser" on page 349 for details.

If this functionality was not enabled during implementation, FI staff can contact your Q2 Relationship Manager to request it.

Secure Messaging tasks

This section lists procedures associated with Secure Messaging, including:

- "Editing Secure Messaging groups for FI staff" on page 299
- "Editing or viewing Secure Messaging group membership" on page 299
- "Enrolling CSR Users in Secure Messaging groups" on page 32
- "Secure Message templates overview" on page 299

Additional message-related tasks include:

- "Viewing new secure messages" on page 341
- "Setting up filters for new messages" on page 342
- "Responding to messages" on page 343
- "Forwarding new messages" on page 344
- "Using Secure Message templates" on page 345
- "Sending a secure broadcast message to all end users" on page 310
- "Sending a secure message to all Users in a Group" on page 310
- "Sending a secure message to all Users linked to a Customer" on page 311
- "Sending a secure message to a single user" on page 312
- "Sending a secure message to a login ID" on page 313

Viewing secure messages

To view unread secure messages sent by end users, click **System Alerts > New Messages** in the workspace tree. See "New Messages overview" on page 340.

To view all secure messages sent by end users from within online banking plus outbound messages sent by CSRs to end users and alert-related messages, click **Communication > Secure Messaging** in the workspace tree to open the Secure Messaging page.

Sending secure messages

There are many ways to send a secure message to end users. These messages will appear on the Conversations page that is accessible via the Navigation menu in online banking.

You can create a broadcast message to send to all online banking end users. This is a great way to communicate important FI-related information quickly. See "Sending a secure broadcast message to all end users" on page 310.

You can also send messages to all members of a Group, all members linked to a Customer, a User, or a Login ID. Refer to the following sections for step-by-step instructions:

- "Sending a secure message to all Users in a Group" on page 310
- "Sending a secure message to all Users linked to a Customer" on page 311
- "Sending a secure message to a single user" on page 312
- "Sending a secure message to a login ID" on page 313

Note: Although Q2central does not currently have spell check functionality, you can compose a message in a word processing program such as Microsoft Word, run spell check, and then copy and paste text into Q2central.

Forwarding messages on the Secure Messaging page

In addition to forwarding a message from the **System Alerts > New Messages** page, CSRs can also forward messages from the Secure Messaging page.

Note: A secure message can only be forwarded once to prevent multiple CSRs from replying to the same message. This setting can be changed during the initial implementation or via a request to Q2 Software by the FI.

To forward a message from the Secure Messaging page

1. In the workspace tree, click **Communication > Secure Messaging**.
2. Double-click a row to display the Secure Message page. View details about the message, including the Secure Messaging group at the FI to which the message is directed.
3. Click **Forward Message**.
4. (Optional) Select the **Show all message groups** check box to display all Secure Messaging groups, regardless of whether you are a member of each group or not.
5. Select the new recipient from the **To** list and type a note in the white pane.
6. Click **Save and Close** to send it.

Tip: A shortcut for these steps is to click a message to select it, right-click to access the shortcut menu, and then click **Forward Message** or press Ctrl + F.

Sending a secure broadcast message to all end users

You can send a secure broadcast message to all end users of the system. Like other secure messages, your message arrives via email or SMS (text message) if the recipients are subscribed.

To send a secure broadcast message to all end users

1. In the workspace tree, click **Administration > Broadcast Message**.
2. On the Broadcast Message to All Users page that appears:
   a. In the From box, choose the message group that is originating the message. (Message groups are configuring during implementation.)
   b. In the Subject box, provide a description for the message as you would for an email.
   c. (Optional) To use an existing secure message template:
      i. Click **Select Template**.
      ii. In the Select Template dialog box that appears, select a Category and a Template, then click **OK**.
   d. In the Message Text box, type the message.
3. Click **Send**.

Tip: Although you can attach a file to a message sent to a single user, you cannot send files to multiple users. Instead, upload the file to your FI website, paste a web address into the Message Text box, and instruct recipients to paste that address into a web browser to access the file (for example, a PDF).

Sending a secure message to all Users in a Group

To send a secure message to all Users linked to a selected Group

1. In the workspace tree, click **User Management > Group**.
2. On the Group page, search for and select the Group to which you are sending the message.
3. Right-click the record, and choose **Send Secure Message to Group**.

4. On the Broadcast Message page, follow these steps:
    a. In the From box, choose the message group that is originating the message. (Your FI set these up at implementation.)
    b. In the Subject box, provide a description for the message as you would for an email.
    c. (Optional) To use an existing secure message template:
        i. Click **Select Template**.
        ii. In the Select Template dialog box that appears, select a Category and a Template, then click **OK**.
    d. In the Message Text box, type the message.
5. Click **Send**.



Tip: Although you can attach a file to a message sent to a single user, you cannot send files to multiple users. Instead, upload the file to your FI website, paste a web address into the Message Text box, and instruct recipients to paste that address into a web browser to access the file (for example, a PDF).

Sending a secure message to all Users linked to a Customer

To send a secure message to all Users linked to a selected Customer

1. In the workspace tree, click **User Management > Customers**.
2. In the Customer page, search for and select the Customer to which you are sending the message.
3. Right-click the record, and choose **Send Secure Message to Customer**.



Note: This message will go to all Users linked to the selected Customer.

4. In the Broadcast Message window, complete these steps:
    a. In the From box, choose the message group that is originating the message. Your FI set these up at implementation.
    b. In the Subject box, provide a description for the message as you would for an email.
    c. (Optional) To use an existing secure message template:
        i. Click **Select Template**.
        ii. In the Select Template dialog box that appears, select a Category and a Template, then click **OK**.

d. In the Message Text box, type the message.

5. Click **Send**.

> **Tip:** Although you can attach a file to a message sent to a single user, you cannot send files to multiple users. Instead, upload the file to your FI website, paste a web address into the Message Text box, and instruct recipients to paste that address into a web browser to access the file (for example, a PDF).

Sending a secure message to a single user

To send a secure message to a single User

1. In the workspace tree, click **User Management > Users**. The Users search options appear.
2. Search for and select the User to which you are sending the message.
3. Right-click the User record, and choose **Send Secure Message to User**.
4. In the Send Secure Message window that appears, complete the following steps:
   a. In the From box, choose the message group that is originating the message.
   b. In the Subject box, provide a description for the message as you would for an email.
   c. (Optional) To use an existing secure message template:
      i. Click **Select Template**.
      ii. In the Select Template dialog box that appears, select a Category and a Template, then click **OK**.
   d. In the Message Body box, type the message.
   e. (Optional) To add an attachment to the message, click **Add** in the **Attachment** section. Locate the file you want to attach in the Attach File window, and click **Open**. The file name will appear in the Attachment section.

   > **Tip:** You can only attach one file to a secure message. Also, the file should not exceed 4 MB.

5. Click **Send**.

Sending a secure message to a login ID

To send a secure message to a login ID

1. In the workspace tree, click **User Management > Logins**.
2. Search for and select the Login to which you are sending the message.
3. Right-click the Login record, and choose **Send Secure Message to Login**.
4. In the Send Secure Message window that appears, complete the following steps:
   a. In the From box, choose the Secure Messaging group that is originating the message.
   b. In the Subject box, provide a description for the message, as you would for an email.
   c. (Optional) To use an existing secure message template:
      i. Click **Select Template**.
      ii. In the Select Template dialog box that appears, select a Category and a Template, then click **OK**.
   d. In the Message Body box, type the message.
   e. (Optional) To add an attachment to the message, click **Add** in the **Attachment** section. Locate the file you want to attach in the Attach File window, and click **Open**. The file name will appear in the Attachment section.



Tip: You can only attach one file to a secure message. Also, the file should not exceed 4 MB.

5. Click **Send**.

CHAPTER 21: MARKETING MESSAGES

In Q2central, you can create and maintain various types of Marketing Messages that end users will see while using online banking.

> **Note:** FIs that purchase Q2's digital targeting and marketing platform, Q2 SMART, can target ads based on end user behavior, as well as manage multiple, custom campaigns. Contact your Q2 Relationship Manager for details.

This chapter includes the following sections:

- "Marketing Messages overview" on page 314
- "Ad Elements overview" on page 315
- "System Notifications overview" on page 322
- "Marketing Messages tasks" on page 323
- "Marketing Messages FAQs" on page 328

Marketing Messages overview

You can use Q2central to create Marketing Messages that appear in various places throughout online banking for many purposes, such as:

- Promoting a new product
- Encouraging a particular end-user behavior
- Adding seasonal accents
- Notifying end users about a new online banking feature

Different Marketing Messages can be created for different pages and you can assign different Marketing Messages to different themes. For example, if your FI is planning a series of Spanish-language financial seminars, you can create ads that will appear only in the Spanish-language theme.

> **Note:** To work with Marketing Messages, you must be assigned to a CSR Role that has the *Communication: Manage Marketing Messaging* right enabled.

To display a list of past, current, and future advertisements (ads), click **Communication > Marketing Messages** in the Q2central menu. Ads are listed in the Campaign Name column along with relevant dates, and can be enabled or

disabled at any time. Because of these factors, it is possible that not all ads displayed are active. To view unexpired ads, sort search results by clicking on the End Date and Enabled columns. Use the Field Chooser to display different columns, as necessary.

Ad types

When planning an ad, first consider which type to use:

- Ad Elements are images that may include embedded URL links so when users click an image, they are directed to another web page. Different images can be uploaded for different devices in some cases (for example, the interstitial page that appears briefly after login) and be scheduled for different dates. Ad Elements can be added to the following pages:
  - Home
  - Branches
  - News/Rates
  - Logoff (for Q2online only)
  - Interstitial
- System Notifications are short pieces of text—up to 300 characters—that appear at the top of online banking pages. Typically, they are used to inform end users about planned outages or other events affecting all users. They do not support images, but can be scheduled for specific dates.

Ad Elements overview

This section describes how to add images and links to online banking pages to promote new products, add seasonal accents, etc. Ad Elements can be scheduled for specific dates, allowing you to plan in advance.

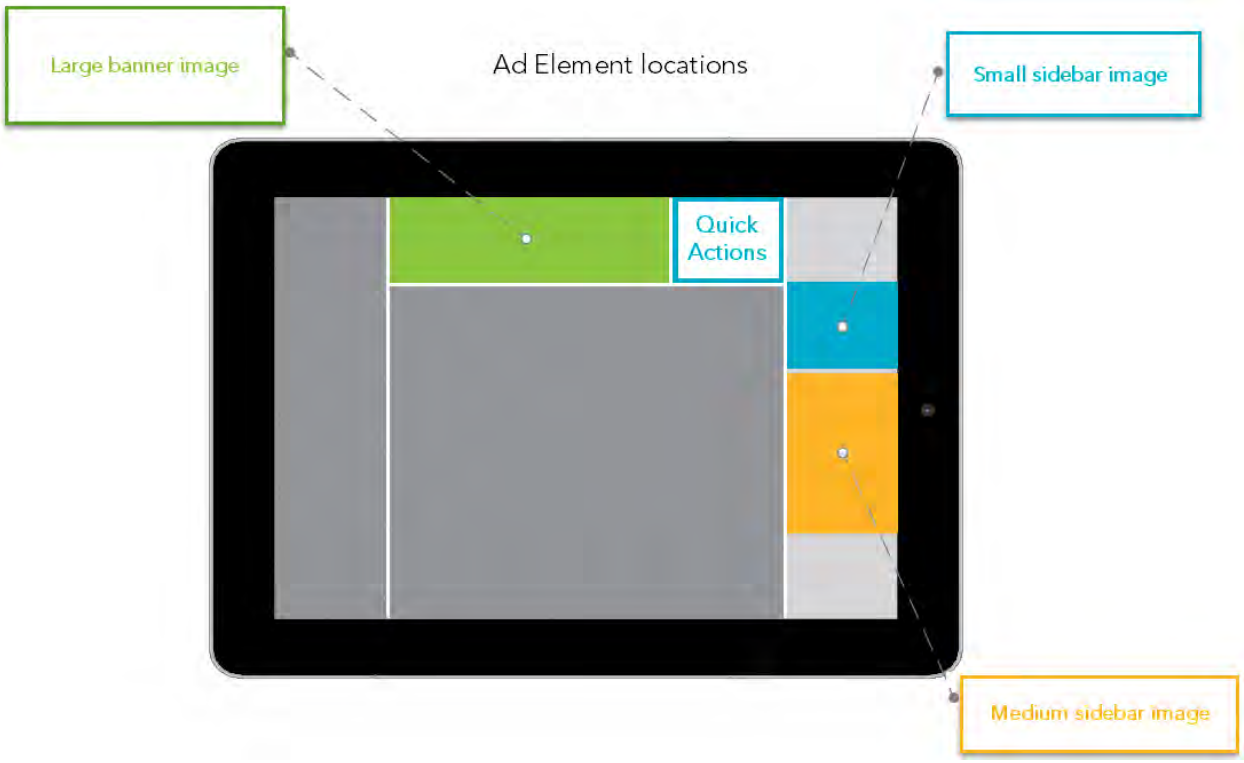
With Ad Elements, you can communicate with end users in many ways in UUX, including:

- Configure ads in the top, wide banner and sidebars of the Home, News, and Branches pages, depending on which layout option—top navigation or left-side navigation—was selected during implementation.
- Update the image on the interstitial page that appears briefly after login.
- Embed a URL to direct end users to an external website (for example, an FI's corporate website) or an online banking page.
- Create a carousel of rotating images.
- Customize Ad Elements that appear only in certain themes (for example, to market Spanish-language seminars to Spanish speakers only.)

Before configuring Ad Elements in Q2central, we recommend that you review this entire section. Then proceed to "Configuring an Ad Element" on page 323 for step-by-step instructions.

Banners and sidebars

You can configure Ad Elements for the banner that appears at the top of the Home, Branches, and News pages in online banking. You can also add images to the small and medium frames that appear in the sidebar.



Note: Banners do not appear on smartphones.

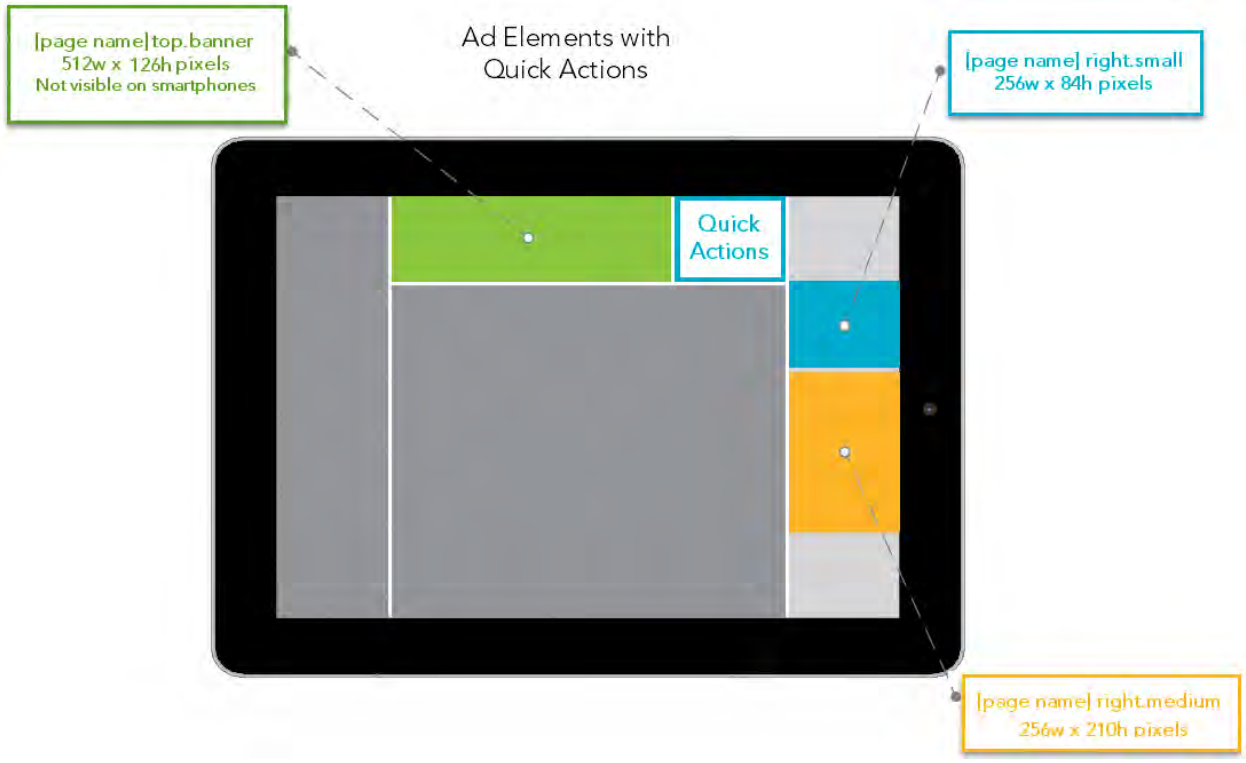
Image sizes

Supported image sizes for banners and sidebars vary, depending on whether or not Quick Actions appear at the top of a page. Quick Actions are shortcuts for common tasks, such as funds transfers, that are configured during implementation.

If Quick Actions do *not* appear on a page, use the following information to configure Ad Elements:

Ad Element requirements without Quick Actions

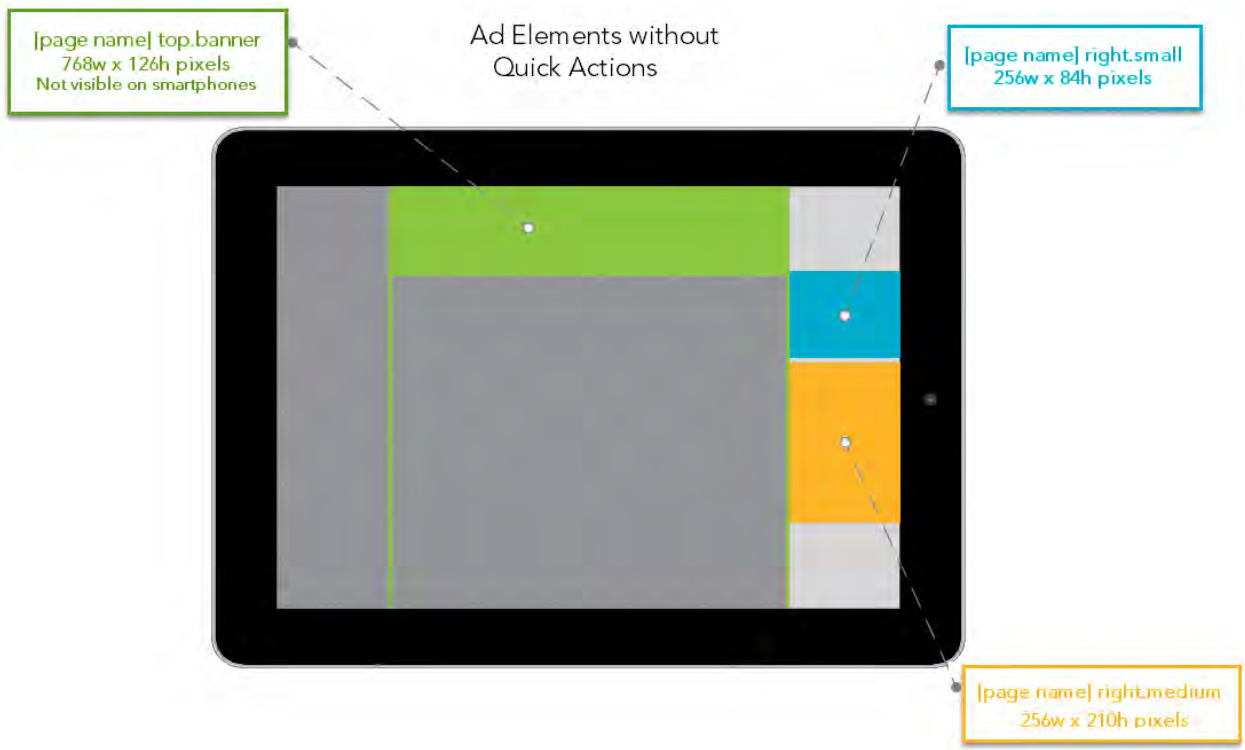
Ad Element	Size (in pixels)	Filename
Large banner image	768 wide x 126 high	[page name] top.banner
Small sidebar image	256 wide x 84 high	[page name] right.small
Medium sidebar image	256 wide x 210 high	[page name] right.medium



If Quick Actions appear on a page, use the following information to configure Ad Elements:

Ad Element requirements with Quick Actions

Ad Element	Size (in pixels)	Filename
Large banner image	512 wide x 126 high	[page name] top.banner
Small sidebar image	256 wide x 84 high	[page name] right.small
Medium sidebar image	256 wide x 210 high	[page name] right.medium



Tip: If you include text in a banner Ad Element image, the recommended font sizes are 18–36 points.

Sidebar

Note the following details about the right sidebar:

- The right sidebar may contain page content or other elements (for example, a Facebook feed) that push down Ad Elements.
- If multiple Ad Elements are enabled for the same target page, page location, and date, they may rotate in a carousel fashion, depending on which theme is selected. Rotating Ad Elements must have identical dimensions.

Tip: If you include text in a sidebar Ad Element image, the recommended font sizes are 16–24 points.

Interstitial page

The interstitial page is a static image that appears, usually very briefly, as account data is downloaded after an end user logs into online banking. During implementation, your FI provided an image for the interstitial page that can be changed later, as necessary.

Note: Load time may be longer for a high-resolution image, but usually only the first time an end user accesses it. After that, the image is typically cached for quick retrieval. For this reason, you should avoid changing high-resolution images frequently, especially for interstitial pages.

Due to the different screen sizes on tablets vs. smartphones, two sizes of the same image are required—one for tablets (also used for desktops), and one for smartphones.

The following figure shows how interstitial images behave on different devices:



When creating a tablet image, note the following details:

- The image size must be 1024 wide x 569 high, in pixels.
- The image will also be used for interstitial pages on desktops.
- The image will occupy the entire screen, except for a 60-pixel-high footer at the bottom of the screen.
- On a tablet in portrait view, the image will expand to occupy the height of the tablet and only the left side of the image will be visible. Be sure to place the most important information on the left.
- In the Ad Element window accessed from the **Communication > Marketing Messages** page, the interstitial image is called *Tablet Interstitial*.
- Use fullscreeninter.png or fullscreeninter.jpg as the filename, depending on the file type.

When creating a smartphone image, note the following details:

- The image width is limited to 320 pixels; it will occupy the entire screen for most smartphones when held vertically.
- On smartphones held horizontally, the image expands to fill available space. The bottom of the image may be hidden by a 60-pixel footer.
- If a smartphone (such as the Samsung Galaxy Note 4) offers more than 768 pixels when held horizontally, the larger tablet/desktop image will be used.
- In the Ad Element window, the smartphone image is called *Device Interstitial*.
- Use *fullscreeninterphone.png* or *fullscreeninterphone.jpg* as the filename, depending on the file type.

For both tablet/desktop and smartphone interstitial images, note these details:

- Use a 72 dots-per-inch (DPI) resolution.
- The interstitial image only appears for a few seconds, so any text included should be brief and concise.
- JPG files are supported, but PNG format is recommended.



Note: After you change an interstitial image in Q2central, log a Q2 Customer Support request to ask Q2 to add the image to the Content Delivery Network (CDN), a backend system that stores large files for quick downloading during login.

To change the interstitial page, see "Configuring an Ad Element" on page 323.

Logoff page

By default, the Logoff page routes end users back to the online banking login page. However, you can configure an Ad Element for the "logoff full size" target page that only includes a target URL for the web page where you want to route users (for example, your FI's corporate home page).

Image recommendations

When using Microsoft Paint or another graphics editor to create images, consider the following recommendations:

- Do not use images with transparency—the gray background color will show.
- To change an image's size, resize it in a graphics editor, and then upload it again. Q2central does not maintain aspect ratio if you change only one dimension of an image in the Ad Elements window. You cannot edit, resize, or rotate images in Q2central.
- High-resolution images take longer to load, but usually only the first time an end user accesses it. After that, the image is typically cached on the device for quick retrieval. For this reason, avoid changing high-resolution images frequently, especially for interstitial pages.
- If you add an image for an interstitial page, you can log a Q2 Customer Support ticket to ask Q2 to add the image to the Content Delivery Network (CDN), a backend system that stores large files for quick downloading during login.

Note: The maximum size for all Ad Element images is 150 KB.

System Notifications overview

You can display a message up to 300 characters long at the top of every page in online banking without sacrificing marketing space. System Notifications are a quick, easy way to let end users know about scheduled maintenance or system downtime.

System Notification layout

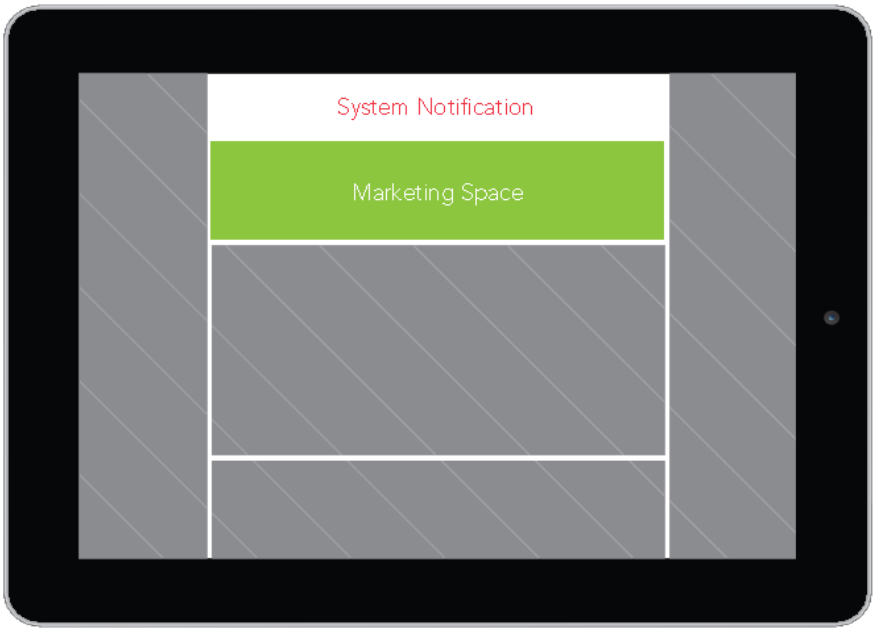


*Illustration represents available layout options and is not to scale.

When working with System Notifications, note the following details:

- For best results, limit each System Notification to 128 characters.
- HTML code is not honored, so any HTML tags you include are visible to end users and formatting is unaffected.
- For optimal results, enable only one System Notification at a time.

For step-by-step instructions, see "Adding a System Notification" on page 326.

Marketing Messages tasks

This section includes some common Marketing Messages tasks:

- "Configuring an Ad Element" on page 323
- "Adding a System Notification" on page 326
- "Setting or editing dates for an ad" on page 327
- "Adding a marketing message object" on page 325
- "Adding a marketing message to a theme" on page 327
- "Deleting an ad" on page 327

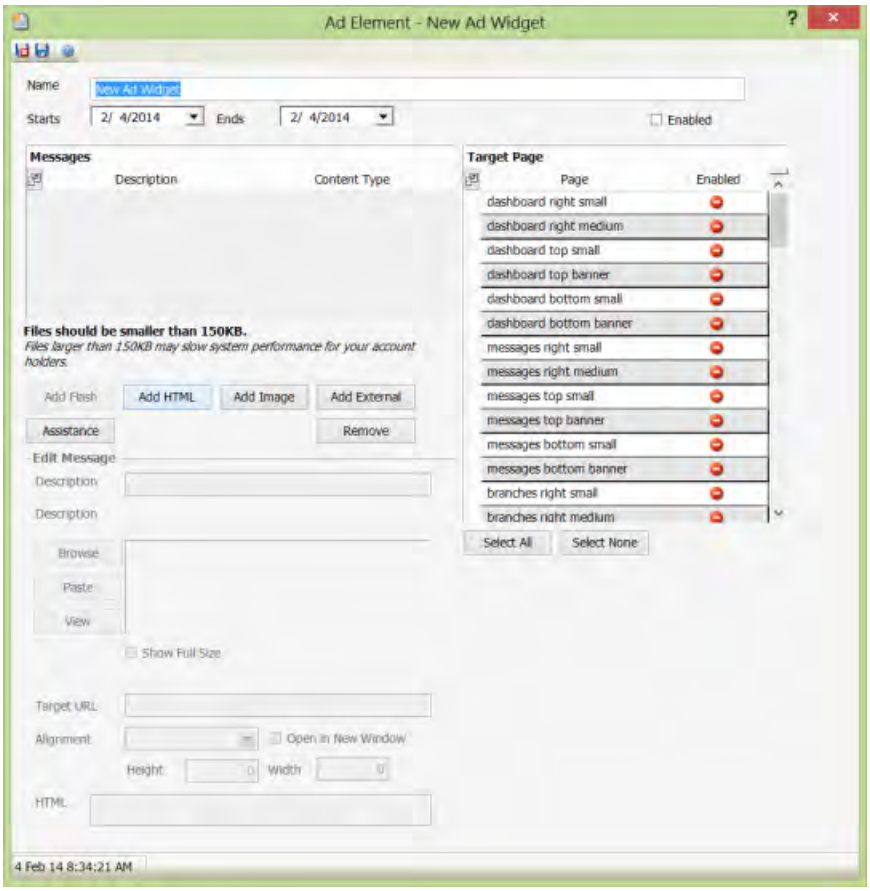
Configuring an Ad Element

Here are some tips to keep in mind while configuring Ad Elements:

- Enable an Ad Element on just one page initially. If you are satisfied with its size and placement, return to the Ad Element window and enable it for additional online banking pages.
- Ad Elements only appear in themes for which they are enabled. This allows you to direct marketing at specific subsets of end users, such as Spanish speakers.
- If you suspect you may want to reuse an ad later, you can hide it from end users without deleting it. Simply clear the **Enable** check box.

To configure an Ad Element

1. In the workspace tree, click **Communication > Marketing Messages**.
2. Right-click in the Marketing Messages list that appears and click **New Ad Element**. The Ad Element window appears.

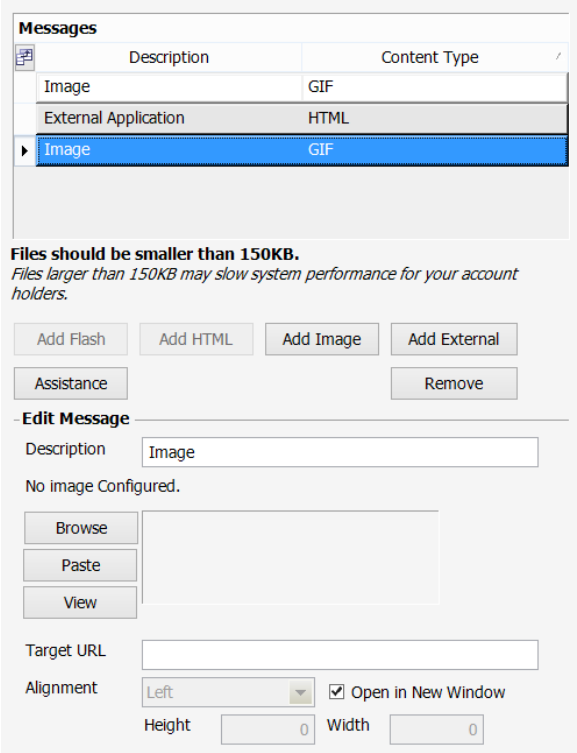


3. Enter a **Name** for the Ad Element.
4. Select the **Starts** and **Ends** Dates for the Ad Element.
5. Select the **Enabled** check box.
6. Select the type of Ad Element being added. (See "Adding a marketing message object" on page 325.)
7. In the **Target Page** pane, click to enable each online banking location where you want the message to appear.
8. Enable one or more **Themes** for the Ad Element.
9. In the toolbar, click **Save**.
10. If you added an image for an interstitial page, log a Q2 Customer Support ticket to ask Q2 to add the image to the Content Delivery Network (CDN), a backend system that stores large files for quick downloading during login.

Adding a marketing message object

An Ad Element can contain different types of child Marketing Messages, as configured in the Ad Element window. Ad Element window options change according to which type of message is active. In the following figure, an image is selected.

Left pane of Ad Element window (Add Image selected)



To add a Marketing Message object

1. In **Description**, provide a name for the object.
2. In the Edit Message section, click **Browse** to find an existing image file on a local drive. (You can also click **Paste** to copy HTML text from the Windows Clipboard.)
3. (Optional) Click **View** to preview the object.
4. (Optional) Enter a **Target URL** to allow end users to click the object to reach another web page. Click **Open in New Window** to open the URL in a new window while the end user remains logged into online banking in the original window.
5. (Optional) Select an **Alignment** option.

Tip: Q2central no longer supports changes to image height and width. To resize an image, use a graphics editor and then upload the image on the Ad Element window.

Adding a System Notification

System Notifications are a good way to let end users know about upcoming scheduled maintenance or system downtime. They will appear at the top of every page, with the exception of the Branches page, on all devices.

To add a System Notification

1. In the workspace tree, click **Communication > Marketing Messages**.
2. Right-click in the Marketing Messages list that appears, then click **New System Notification**. The System Notification page appears.
3. Enter a unique **Name** for the System Notification.
4. In the **Starts** field, select the beginning date for the notification.
5. In the **Ends** field, select the ending date for the notification. For example, if July 4 is the last day of a campaign, choose July 5.
6. Select the **Enabled** check box to display the notification in online banking, assuming that today is within the time frame selected in steps 4 and 5.

   Tip: To use the Enabled check box as an approval method, designate one person to create a System Notification and a second person to review the text and then enable it.

7. In the Messages area, click **Add Text**.

   Note: HTML tags are not supported.

8. Enter a brief **Description** for the System Notification.
9. In the **Text** field, enter the actual text for the notification.
10. In the toolbar, click **Save and Close**.

Setting or editing dates for an ad

A valid time frame must be in effect for each ad.

To set or edit an ad's time frame

1. In the workspace tree, click **Communication > Marketing Messages**.
2. In the Marketing Messages list, search for and select the ad for which you want to define or edit the time frame.
3. Change the **Starts** and **Ends** dates, as necessary.
4. Select the **Enabled** check box to display the ad during the designated dates.

Deleting an ad



Caution: Once you delete an ad, you cannot restore it. To hide an ad from end users temporarily (for example, if you think you may use it again), clear the **Enable** check box.

To delete an ad

1. In the workspace tree, click **Communication > Marketing Messages**.
2. In the Marketing Messages list, search for and select the ad.
3. Right-click the selected ad and click **Delete Campaign**.
4. Click **Yes** in the Confirm Deletion dialog box that appears.

Adding a marketing message to a theme

To add a marketing message to a theme

1. In the **Theme Selection** pane, click to enable each Q2online theme where you want the marketing message to appear. To appear at all, a marketing message must be enabled for at least one theme.
2. In the toolbar, click **Save**.



Tip: Marketing messages only appear in the themes for which they are enabled. This allows you to direct marketing at specific market segments aligned with your FI's themes, such as Spanish speakers or teens, if Users are divided into relevant Groups.

Marketing Messages FAQs

This section includes frequently asked questions (FAQs) about Ad Elements and System Notifications.

Ad Elements

Why won't my Ad Element image appear?

Ad Element images may not be visible if:

- Images sizes do not match those specified in "Banners and sidebars" on page 316.
- Q2 manages Campaigns on behalf of your FI (for example, during an end-user marketing effort). Q2's Ad Elements take precedence over any Ad Elements configured by an FI for the same location.
- Other elements were added outside of Q2central, such as a Facebook feed that was added to the sidebar during implementation.
- Pop-ups are blocked by an end user's Internet browser. The end user must either enable pop-ups or add the online banking URL to the list of allowed sites.



Note: Images added to the wide banner at the top of the Home, Branches, or News page will not appear on smartphones.

Check the dates for which the Ad Element is scheduled and make sure it is enabled by following these steps:

1. In the workspace tree, click **Communication > Marketing Messages**.
2. In the Marketing Message page, search for and double-click the Ad Element to display the Ad Element window.
3. Check the dates.



Note: The **Starts** date is when the Ad Element begins to appear and the **Ends** date is the first day it will not appear. To make sure that an ad's **Starts** date works over multiple time zones, choose a date in the past and the ad will appear immediately.

4. Verify that the **Enabled** check box is selected.

System Notifications

Why doesn't my System Notification appear?

In Q2central, check the dates for which the System Notification is scheduled and make sure the notification is enabled.

1. In the workspace tree, click **Communication > Marketing Messages**.
2. In the Marketing Message page, expand the **Campaign Type: System Notification** group.
3. Double-click the System Notification to display the System Notification dialog box.
4. Check the dates. The **Starts** date is when the notification begins to appear and the **Ends** date is the first day it will not appear.
5. Verify that the **Enabled** check box is selected.

Section V - Daily Processing - System Alerts

The System Alerts menu contains categories of items that are considered part of the CSR's daily processing tasks. These various types of messages may require FI staff's immediate attention or interaction. This section details system alerts that pertain to the end user and FI staff.

CHAPTER 22: SYSTEM ALERTS

This chapter discusses the Q2central System Alerts that may require FI staff's immediate attention or interaction. These alerts pertain to the end user and FI staff. Each alert category appears as an option in the System Alerts section of the Navigation menu.

This chapter also describes how to configure the Home page that most CSRs see when they first log into Q2central. This visual display shows CSRs, at a glance, how they are tracking collectively in several administrative areas, most of which are related to System Alerts.

This chapter contains the following topics:

- "Suspect Transactions overview" on page 331
- "New Postings overview" on page 332
- "Disabled Logins overview" on page 338
- "CSR User Lockouts overview" on page 339
- "CSR Disabled Logins overview" on page 339
- "New Messages overview" on page 340
- "End user alerts overview" on page 345

Suspect Transactions overview

The Suspect Transactions option is useful to FIs that own the Q2 Sentinel product and are in Active Mode. See the *Q2 Sentinel User Guide* to learn more about Active Mode.



Note: This option is accessible via the System Alerts section of the Q2central workspace tree, but you can also access this data via the Home page. See "Home page" on page 41.

Transactions listed here were end-user-approved in online banking and marked suspect by Sentinel. A transaction remains in the Suspect Transaction list until FI staff takes action to either:

- Cancel a transaction after learning from an end user that it is fraudulent
- Approve a transaction based on end-user information that it is valid

Approved transactions move automatically to the To Process list for inclusion the next time the Process Wizard runs. FI staff should clear this list regularly throughout the day, and always before running the Process Wizard. If transactions are not processed promptly, they may become stale-dated, resulting in problems for end users and the FI.

If no transactions appear in this list, it means that Sentinel has not scored any transactions as suspect since the last time the list was cleared.

FI staff cannot see suspect transaction items until rights are granted via the **Administration > CSR Roles** page. The right is named *Transactions: Suspect Transaction Management*.

To process transactions

- Double-click an item in the list to access the Transaction Case Review window.

For details, see the *Q2 Sentinel User Guide*.

New Postings overview

The New Postings page displays transactions that end users approved but that FI staff have not yet processed. These are the same transactions that would appear if you used the Process Wizard to create a batch of all unprocessed items and then viewed batch contents. After a transaction is processed, it will not appear in the New Postings list.

Note: This option is accessible via the System Alerts section of the Q2central workspace tree, but you can also access this data via the Home page. See "Home page" on page 41.

Note: You must perform a search to get records to appear, unless you saved a default search for this option. See "Searching for information in Q2central" on page 348.

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

Locked Logins overview

The Locked Logins option contains a list of end users who are currently locked out of online banking. This may result from too many login attempts by end users who have forgotten or repeatedly mistyped their password, or who are unable to provide a valid security access code (SAC). A Login remains locked until FI staff unlocks the login; see "Restoring end user access" on page 336.

You can view your FI's current Password Policy by double-clicking any item in the list. Select a Login ID on this page, then right-click to access a shortcut menu with options to complete any task listed in the following table:

Locked Logins shortcut menu options

Action	Shortcut (if any)	Description
View User Login		Displays the selected User Login record details.
Show User	Ctrl + Shift + U	Displays the User record associated with the selected Login.
Edit Login		Allows changes to be made to the selected Login.
Delete Login		Deletes the selected Login. Deleting a login only removes the login record; it does not delete the User record from the system.
Change Password	Ctrl + Shift + P	Allows you to set and confirm a new password while viewing the FI's current password policy. You must personally provide this to the end user over the phone because an automated message is not sent.
Enable Login	Ctrl + Shift + E	Returns a disabled Login Status to *Enabled* (that is, normal). This allows end users to log in using their current password.
Disable Login	Ctrl + Shift + D	Changes a Login Status to *Disabled* (FI staff is not prompted for confirmation). A disabled login is not usable until FI staff enable it.

Locked Logins shortcut menu options (cont'd)

Action	Shortcut (if any)	Description
Renew Initial Password	Ctrl + Shift + E	Extends the time that a first-time end user's FI-provided password is valid. Use this option with logins whose status is *New Password Has Expired*. This option is unavailable after the first-time login is successful.
Reset Password to Default	Ctrl + Shift + R	Sets the Login Status to *Normal* and resets the password to the default value specified in the system configuration.
Unlock Pin/Password	Ctrl + Shift + U	Sets the Login Status to *Normal*, to allow an end user to log in with the password they currently use.

Login statuses



Tip: If a user cannot log in but the Login Status does not indicate a problem, check the User Status in the User pane. If the User Status is *Disabled*, all related accounts are blocked. This can occur if an FI suspects fraud is occurring. Escalate the issue to a CSR with Q2central access.

This table describes the possible statuses for a login ID that may appear in the Login pane.

Login ID statuses

Status	Description
Challenge Questions Requested	The end user was prompted to answer a challenge question, but the person attempting to log in did not respond. **Note:** Not all FIs allow end users to use challenge questions instead of secure access codes (SACs) or VIP token codes.

Login ID statuses (cont'd)

Status	Description
Expired Password	The end user does not have an active password. This can occur if the user has never logged into online banking, or begins the Forgot-Your-Password process. This status indicates that a SAC was generated, but the end user has not yet set a password. This status may also appear if an end user does not reset a password before the end of a password's time limit, if one was set by the FI.
Login Disabled	The caller's login ID was actively shut down, either by the FI or by an administrative User. Alternatively, the end user may be part of a Group for which the *New users created through the online channel are disabled* setting is enabled on the Group page's Features tab in Q2central.
New password has expired	FI staff generated a new password for the user, but it was not used to log in and expired. Click **Renew Initial Password** to extend the time period for which this password is valid.
Normal	No system issue prevented the user from logging in. Ask the user to try the **Forgot your Password** link on the Login window. **Note:** A user may still not be able to log in, even if the status is Normal. This can occur if the User record is in an Inactive or Disabled status. Ask a CSR with access to Q2central to check the User record status.
Password Change Required	The system generated a new password for the user, which was not yet used to log in but is still valid.
Temporary Access Code Required	The system sent a SAC to the end user, which has not yet been used to log in.
Token Required	The end user cannot log in because a required VIP token code acquired via a physical VIP Security Token or the VIP Access mobile app was not provided.

Login ID statuses (cont'd)

Status	Description
Login Locked Out	The user cannot log in because the maximum number of unsuccessful attempts was exceeded. **Note:** Being locked out of one channel does not lock the end user out of the other channels (Browsers/Apps, Voice, or Text).
Inactive	This status indicates that an end user is using the Corporate Banking version of online banking and one or both of the following conditions is true: • An administrative user deactivated the user's login ID. • The user is not yet approved to use online banking.

Restoring end user access

FI staff may receive requests from end users to have their access restored. (If this is during your implementation period, check with Q2 staff to see if any special accommodations are in place for high volumes of lockouts.)

For any request, first verify that this end user's login is locked out and not disabled. A locked-out login means the end user forgot or misplaced credentials. Lockouts have a Login Status of Normal. A disabled login (Login Status of Login Disabled) is one whose rights may have been actively removed by the end user or FI staff and probably requires further investigation. New User records in the system may sometimes require verification before FI staff enables them.

To unlock a login without affecting password

1. In the workspace tree, click **System Alerts > Locked Logins**.
2. Locate the login and channel that you want to unlock, and verify that the Login Status is Normal.
3. Right-click the item and click **Unlock Pin/Password**.

Forgotten and first-time passwords

For FIs whose configuration supports it, there is an automated process that end users can use to reset a forgotten password or set a password for the first time (sometimes called password-free migration). This feature saves time, provides service to end users outside of business hours, and enhances password confidentiality.

Note: Forgotten login IDs cannot be retrieved without assistance from FI staff.

The sequence that occurs during this process is as follows:

1. End user clicks on **Forgot Password** or **First-time User** on the Login page.
2. The Multi-factor Authentication (MFA) feature prompts the end user to provide or select a delivery method for a secure access code (SAC).
3. The end user selects a method and receives the code, then the end user's login status changes to *SAC Required*.
4. The end user successfully provides the code and is immediately prompted to select a password. The end user's login status is now *Expired Password*.
5. The end user selects an acceptable password and is granted access. The end user's login status is now *Normal*.

Note: Automated password retrieval does not work if the end user belongs to a Group if the *Authentication: Only allow lost/forgotten password from registered browsers* feature is *Enabled* on the Group page's Features tab.

Resetting an end user's password

To reset an end user's password

1. In the workspace tree, click **User Management > Logins**.
2. Search for and select the correct login record, following your FI's policy for verifying the end user's identity before proceeding.

3. You can search or sort within the Channel column to find Q2voice logins, if necessary.
    - For end users locked out of Q2online, the login ID is usually name-based or is the CIF.
    - For end users locked out of Q2voice, the login ID may be the end user's account number or the Customer CIF number.
4. Double-click the item in the Logins list to display the User Login window.
5. If the end user does not remember the old password, or if the old password was compromised, click **Change Password** to generate a temporary password that you provide to the end user. At this point, the Login Status changes to Password Change Required. The temporary password remains valid until the end user logs in, or until the password reaches the timeout established by the FI.
    - For a Q2online password reset, instruct the end user to log in using the temporary password. In this process, the end user follows the first-time user enrollment path and for this one login session, is not required to provide a secure access code. The end user must accept your FI's Online Banking Agreement and is prompted to update the User Profile. The end user is then prompted for the old password (that is, the temporary password you just issued) and a new password.
    - For a Q2voice password reset, instruct the end user to log in using the password you provided.

Retrieving an end user's secure access code

This report provides the time/date of secure access code expiration, the status of the notification, the delivery method, error message (if any), and the secure access code itself.

To retrieve an end user's secure access code

1. In the workspace tree, click **Reporting > Operations**.
2. Browse to the SAC Lookup Report, if available.
3. Provide the end user's login ID, then click **Submit**.

Disabled Logins overview

The Disabled Logins option displays User logins that are disabled in various channels of the system. This may have occur if the primary account holder disabled the login in online banking, or if FI staff disabled the User login in Q2central (for example, if fraudulent activity is suspected).

Note: This option is accessible via the System Alerts section of the Q2central workspace tree, but you can also access this data via the Home page. See "Home page" on page 41.

In addition, new Login IDs are listed here if new users created through the online channel are disabled or were configured on the **Group > Features** tab for this Group. A message to FI staff appears in the New Messages option alerting them to the new Login ID awaiting authorization. After receiving verbal approval from the end user, FI staff activates the new Login ID by right-clicking the item and selecting *Enable Login*.

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

CSR User Lockouts overview

The CSR User Lockouts option contains a list of FI staff that are currently locked out of Q2central. User lockouts result from too many login attempts by end users who have forgotten or repeatedly mistyped their Q2central password.

Tip: You can view your FI's current Password Policy by double-clicking on any item in the results.

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

CSR Disabled Logins overview

The CSR Disabled Logins option contains a list of FI staff logins that are disabled, preventing access to Q2central. These are typically FI staff who are on vacation for an extended period.

Note: For security purposes, delete CSR User records for staff who are no longer with the FI instead of disabling their login IDs. See"Deleting a CSR User" on page 32

Tip: You can customize most information displayed by using the Field Chooser. See "Using the Field Chooser" on page 349.

For detailed information on tasks associated with disabled CSR Logins, refer to the *Q2central Support Services Guide*.

New Messages overview

The **System Alerts > New Messages** page displays incoming, unread secure messages sent by online banking end users. Each CSR will see messages sent to all queues to which the CSR belongs, as defined on the CSR User page's Message Groups tab.

Note: You can also access this page via the Home page. See "Home page" on page 41 for details.

The tally of new messages shown beside the New Messages option in the workspace tree represents the number of messages that are unread so far by any FI staff.

A message remains in the New Messages queue until opened by a CSR who will, presumably, take action in response to it. Afterward, use the **Communication > Secure Messaging** page to display older messages; see "Viewing secure messages" on page 308.

New Messages tasks

This section lists the tasks available when working with New Messages:

- "Viewing new secure messages" on page 341
- "Setting up filters for new messages" on page 342
- "Responding to messages" on page 343
- "Forwarding new messages" on page 344
- "Using Secure Message templates" on page 345

For information about configuring Secure Messaging groups and setting up Secure Message templates, see "Secure Messaging" on page 297.

Viewing new secure messages

This section describes how to view "unread" secure messages sent by end users, click **System Alerts > New Messages** in the workspace tree.

To view all secure messages sent by end users (both read and unread) along with alerts, click **Communication > Secure Messaging** in the workspace tree to open the Secure Messaging window.

To view a new secure message

1. In the workspace tree, click **System Alerts > New Messages**.
2. Use the Search options to display a list of unread messages, along with the date each was received and a time stamp.
3. Double-click a row to display a specific message in the Secure Message window.
4. (Optional) Use any of the following toolbar options to work with a secure message:
   - Click **Reply to Message** to compose a response in a new window. To send the response, click **Save and Close** on the toolbar.
   - Click **Forward Message** to send the message to another Secure Messaging group within your FI. See "Forwarding new messages" on page 344.
   - Click **Show Customer** or **Show User** to get additional context about the sender.

   Note: End users cannot view internal activity (for example, forwarding) for a message. Only the final "Respond" message is sent to the end user. FI staff may need to summarize the results of forwarded information for the end user.

5. (Optional) Click **History View** to see a multi-message communication thread, if any. In History View, the original message that was selected for viewing is displayed in bold. Attachments (if any) in previous messages appear as hyperlinks.
6. (Optional) Select the **Message does not Expire** check box to prevent the system from automatically deleting this message on the specified date.

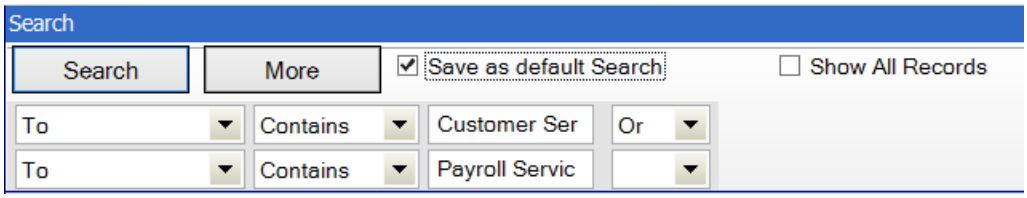
Tip: If an end user claims that they sent a message but it does not appear in the Secure Message window, ask if the message included a file attachment. The maximum file size for attachments is 5 MB.

Setting up filters for new messages

FI staff may wish to set and save a personal filter that is associated with their specific Q2central login ID. Most system-generated messages that are intended for end users do not appear in Q2central, but some outbound messages may still appear on the New Messages list unless a personal filter is established.

For example, FI staff may wish to set up a filter based on the Secure Messages group to which messages are assigned:

- *Assigned to a specific Secure Messages group to which they belong*, by selecting **To**, **Contains**, and a single Secure Messaging group.
- *Assigned to multiple Secure Messaging groups to which they belong*, by creating separate filter criteria for each group, specified by **To**, **Contains**, along with each relevant Secure Messaging group, joined by an **Or** statement.



FI staff may also wish to include only those statuses that occur at a certain place in the workflow, such as *Unresolved*.

To save a filter

1. Select the **Save as default Search** check box.
2. Click **Search**.

Note: To add a field as a filter value in the Search section, first display the associated column in the New Messages window by using the Field Chooser. See "Using the Field Chooser" on page 349.

Responding to messages

There are various ways to respond to messages, including replying, forwarding, and marking as resolved.

Tip: To cancel a response without sending, click **X** in the upper right corner of the message window.

To reply to a message

1. Click **Reply to Message** and accept the prompt, if any.
2. In the white pane, type your response.
3. Click **Save and Close** to send it.

Note: If you or an end user replies to a message that was marked as resolved, the new message will be in an unresolved state.

Tip: When a CSR replies to a message, the CSR's Secure Messaging group will appear as the "From" value in the message. Q2central can be configured to use the CSR's name instead. Contact your Q2 Relationship Manager (RM) for details.

If your FI opted to enable the Secure Message Templates feature, a Select Template button appears on the message window when you respond to a message. See "Using Secure Message templates" on page 345.

To forward a message

1. Click **Forward Message** to send it to another recipient group at your FI.
2. Select the new recipient from the **To** list and type a note in the white pane.
3. Click **Save and Close** to send it.

Tip: To forward a message directly from the New Messages search window, right-click to access the shortcut menu, and then click **Forward Message** or press Ctrl+F.

Note: By default, a message can only be forwarded once. This prevents multiple branches of the same message, which could occur if multiple CSRs responded to the same message. This setting can be changed during implementation or via a support request.

To mark a message as resolved

- Click **Message Resolved** to indicate that no further FI action is needed to respond to this message.

Forwarding new messages

To forward a new secure message

1. In the workspace tree, click **System Alerts > New Messages**.

   Tip: To forward a message directly from the New Messages search window, right-click to access the shortcut menu, and then click **Forward Message** or press **Ctrl+F**.

2. Double-click a row to display the Secure Message window. View details about the message, including the Secure Messaging group at the FI to which the message is directed.
3. Click **Forward Message** to send it to another recipient group at your FI.
4. Select the new recipient from the **To** list and type a note in the white pane.
5. Click **Save and Close** to send it.

Note: By default, a message can only be forwarded once. This prevents multiple branches of the same message, which could occur if multiple CSRs respond to the same message. This setting can be changed during the initial implementation or via a support request.

You can also forward a message on the **Communication > Secure Messaging** page. See "Forwarding messages on the Secure Messaging page" on page 309.

Using Secure Message templates

If your FI opted to include Secure Message templates in their online banking implementation, a Select Template button appears on the message window when you respond to a message.

To use a template when replying to a Secure Message

1. Click the **Select Template** button. The Select Template window appears.
2. Select a **Category** and a **Template**, then click **OK**. The text from the selected template appears in the message window.
3. Edit the text, as necessary.
4. Click **Save and Close** to send the response.

Whether a CSR has the ability to edit the content of templates themselves is controlled in the Administration menu, under CSR Users. On a CSR User record, click the CSR Roles button to display the CSR Role window. See "Secure Message templates overview" on page 299 for details.

End user alerts overview

End users control their own alerts—custom settings are not maintained in Q2central. Instead, end users configure alerts in online banking. For a list of the default alerts available to end users, see the *Q2central Reference Lists* document.

There are several types of alerts that end users may receive:

- Security alerts are notifications to end users regarding events in their online banking profile or accounts, such as changes to password or security options; invalid secure access code provided, new user added, and more. Some of these are mandatory (configurable by the FI) and some are optional. End users select optional alerts in online banking via the **Preferences > Security** menu for delivery by text, phone message, or email.
- Transaction alerts are optional, and are delivered when specific transactional conditions are met, such as a particular check clearing, a specific transaction credit posting to a specific account, and more.
- Date alerts offer end users a convenient reminder of important dates or events.
- History alerts trigger based on details of processed transactions.

End user alerts are:

- Sent in real time, except when a time is specified. End users can select a time to receive a text or voicemail alerts in HH:MM am/pm format.
- Alerts are sent at or after the specified time on any given day. It is recommended that end users specify the earliest time they would be willing to receive an alert; that way, they can be notified throughout the day of any suspicious activity. Your FI may choose to add a clarifying message to the header of the Add Transaction Alert window in Q2online.
- Delivered using an end-user-specified channel, such as SMS (text), phone, and/or email. For end users to receive alerts via Q2text or Q2voice, the FI must own these products.
- Able to be configured as mandatory or optional across the FI's end-user base
- Some end-user alerts, including Non-Sufficient Funds (or Insufficient Funds) alerts, are not part of the core Q2online product and require development services to install.



Tip: Alerts that are sent to CSRs and end users can be modified to include additional information. Contact Q2 Customer Support to pinpoint the alert that you want to customize and determine the fields that are available for use in that alert.

APPENDIX A: HELPFUL TIPS FOR WORKING WITH Q2CENTRAL

This appendix contains useful details for working with search features of Q2central. This information is part of the *Getting Started with Q2central* document, which describes features and functionality in Q2central.

Q2central search techniques

When working with Q2central options and search results, it's important to remember several tips that allow you to customize and fine-tune the information with which you work. These techniques are provided here as reminders, but are explained in more detail in the *Getting Started with Q2central* guide.

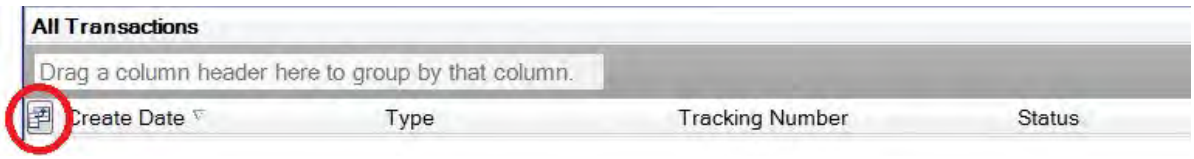
Default searches

For most options in Q2central you must first perform a search so that items appear in the search results pane, unless you saved a default search for the option. See "Searching for information in Q2central" on page 348.

Filtering search results

Options in Q2central that display the Field Chooser ( ) icon allow you to customize the information displayed in your search results.

Field Chooser icon



For more details, see "Using the Field Chooser" on page 349.

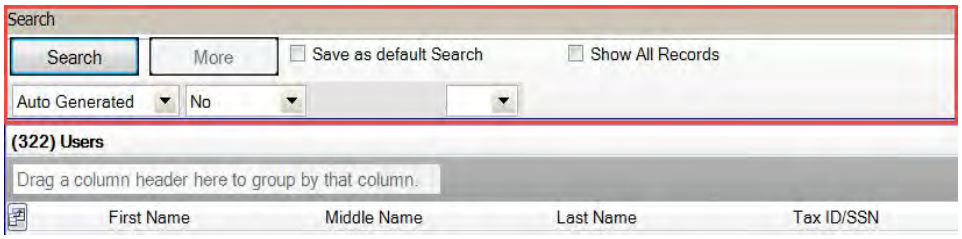
Searching for information in Q2central

Q2central's search functionality allows for the fine tuning of search criteria and results. You can use standard search criteria, such as filters and search operators (for example, AND or NOT), to refine search results and then save the searches.

Tip: Searches are saved for each CSR and persist when that CSR logs into future Q2central session.

Many options in Q2central allow you to group and sort search results. Q2central's search function is similar to a report, allowing you to hone in on those items that meet your specific requirements. For most options, a set of search options appears at the top of the workspace when an option is selected, as shown next:

Q2central search options



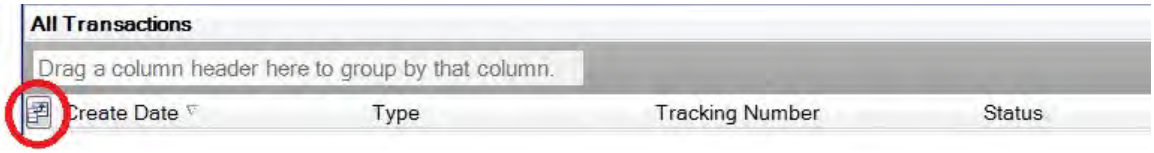
Note the following details about Q2central searches:

- You can enter search criteria in the top bar of any page where a Search button is available, and then click **Search** to display results.
- If the More button appears, click it to display up to 50 more records.
- If your FI uses the Group Access Mapping feature, some data may appear masked (that is, hidden), depending on whether you have permission to display records in a specific Group. See "Group Access Mapping" on page 46.
- Double-click the Search bar to display search options in a new window. Double-click the bar again to close the window.

Using the Field Chooser

Many Q2central pages can be customized to display extra fields of data that are pertinent to your FI's business needs. This option, called the Field Chooser, provides a function that is like a report, allowing you to filter and sort data that meets your search criteria. You can recognize this option by the Field Chooser icon that appears to the left of the sort columns.

Field Chooser icon



To use the field chooser

1. In the workspace, click the Field Chooser icon ( ) to view the data fields available for sorting. Data fields that appear with a check mark beside them are already selected.
2. Select the check box for every data field that you want to include, based on your FI's needs.

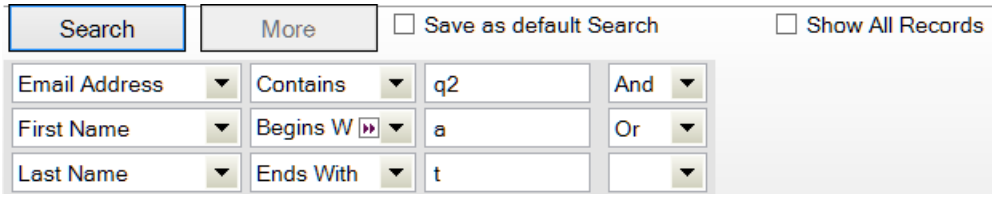
> **Tip:** The duration of a search depends on the number of fields selected, which impacts the number of records being searched.

3. In the Q2central toolbar, click **Refresh**.
4. To group search results, click and drag a column into the **Drag a column header here to group by that column** field.
5. In the Q2central toolbar, click **Refresh** to display records based on the selected grouping. (Data displayed for new fields may vary, appearing as either check boxes, or red and green icons.)
6. Click the Save toolbar button to make this your default view.

Filtering data

You can use the fields listed in the Field Chooser to filter search criteria and fine-tune your search results. These same fields are available as filters from the drop-down box directly below the Search button.

Q2central data filters



After you select a field to search by, the options that appear to the right allow you to filter that information. By using the final drop-down box containing **And**, **Or**, and other options, you can add multiple selections to fine tune search criteria even further.

To filter for specific attributes

1. In the left-most drop-down box below the Search button, begin by selecting the attribute on which you want to search in the left-most box. (For example, *Email Address*, *First Name*, or *Last Name*.)

   Note: The fields you select in the Field Chooser are the same fields that you can use in searches.

2. In the next box to the right, select the relationship you want your results to have with the first selection. (For example, *Begins with* or *Contains*.)
3. In the next box, enter the value you want the system to match when compiling results. (For example, *S*.)
4. In the last box, you can continue to add search attributes by selecting **And** or **Or**.

And	Specifies a list of items that meet both the previous attribute and the next attribute.
Or	Specifies a list of items that match at least one of either the previous attribute or the next attribute.

5. Repeat and complete the drop-down boxes to define all the search attributes you may need to narrow your search results.
6. When all of your filters are set, click **Search** to display the results.

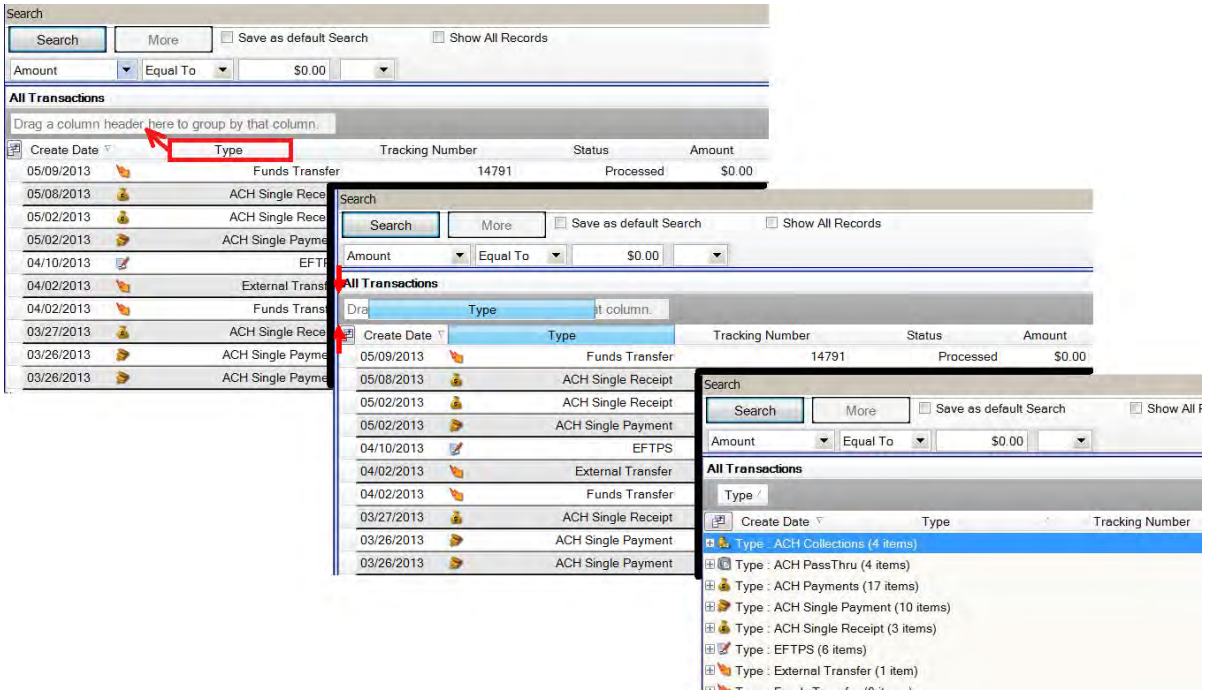
Tip: To save a search for future use when you access a page, click **Save as default Search** before clicking **Search**. You will still need to click **Search** to access results, but you will not need to enter search criteria again.

Grouping data columns

Group data by clicking and dragging the name box of a column into the field labeled "Drag a column header here to group by that column".

To group by column

1. Filter results so that they fit on one page, if possible.
2. Make sure the column by which you want to group is displayed. You may need to drag the column header to the left so that it displays without scrolling.
3. Click and drag the column header upward into the **Drag a column header here to group by that column** box.



4. The system sorts search results (visible on this page only) by the attribute for the column you selected and groups those with common values.



Tip: To undo the groupings, drag the column header name back into the main workspace.

Q2central Documentation

All Q2central guides are available in PDF format from the Q2central menu bar. Click **Help > User Guide** to display the list of Q2central user documentation.