CO OP Solutions℠

LEADER GUIDE

My Co-op Client Leader Guide

Contents

My Co-op overview

My Co-op is a single launching point for all Co-op applications. It simplifies the way users log in to many applications, while employing the latest security technology, including Security Access Markup Language (SAML) and multifactor authentication (MFA). This guide offers information that will help you roll out My Co-op to your employees.

My Co-op URL

The My Co-op main page is https://sso.my.coop.org/mycoop

My Co-op documentation

Additional resources can be found in the Knowledge Center within My Co-op.

Pre-rollout and admin guides

- **My Co-op Pre-rollout Checklist** – An overview of steps to help your organization plan a successful rollout of My Co-op.
- **My Co-op Client Leader Guide** (this guide) – A detailed overview for staff at your organization who will lead the rollout and the use of My Co-op. The **Application User Group Matrix** lists the user groups and the applications assigned to each user group. A **sample email script** can be used as a starting point for the message to new users when they have access to My Co-op.
- **My Co-op Delegated Admin Console Guide** – Detailed information and procedures for your Power Users of the Delegated Admin Console, who manage My Co-op users by creating and deleting them, assigning users to groups, and resetting passwords. The **Application User Group Matrix** lists the user groups and the applications assigned to each user group. A **sample email script** can be used as a starting point for the message to new users when they have access to My Co-op.
- **My Co-op Delegated Admin Console Quick Reference Guide** – A shorter guide containing procedures for your administrators. A **sample email script** can be used to notify users of their access.

End-user guides

- **My Co-op End-User Guide** – Detailed procedures and FAQs to guide your staff as they access and use My Co-op.
- **My Co-op End-User Quick Reference Guide – Initial Sign-On** – A shorter guide to assist users as they sign on to My Co-op for the first time.

Rollout steps

Co-op recommends following a structured rollout program, which is described in the My Co-op Pre-rollout Checklist.

1. **Log in the first time.**
    a. Sign on and set up multifactor authentication (MFA). MFA setup is part of the initial sign-on process.
    b. Launch applications.
2. **Determine your staff's user groups** and assign access rights.
    a. Navigate to the Delegated Admin icon on your dashboard.
    b. Follow procedures in the My Co-op Delegated Admin Console Guide to determine the user groups and access rights as you set up new users of My Co-op.
    c. Securely share credentials with your staff.
3. **Validate your staff users.**
4. **Decide how you will communicate.**
5. **Test the registration process.**
6. **Communicate with your staff.**

Email for new users

The sample email script on the next page can be used as a starting point for the message that the My Co-op administrators at your credit union will send to new users after each user is set up with access to My Co-op.

- The sample provided is the *first* email that My Co-op admins (Power Users) send to new users after setting up their access to My Co-op.
- In a *separate* email, provide the temporary password that the admin has set up for the new user.

The sample email script can be tailored to fit your organization's specific needs and approach. For example, will you permit staff to receive authentication passcodes on a personal cell phone? If so, as part of the initial registration process, consider requiring users to select a backup device. Doing so can mitigate risk in cases where staff forget their phone, or battery issues arise. The My Co-op End-User Guide contains instructions for adding additional devices for MFA.

Sample email script:

Subject: You Can Now Access My Co-op

Welcome to My Co-op, the single sign-on (SSO) portal launching point for all Co-op applications!

My Co-op includes multifactor authentication (MFA), which means you will receive a one-time use authentication code each time you go to My Co-op. You can use your email address or smartphone to receive the code via *[state here what is available to users: text and/or email]*.

Before using My Co-op, perform a one-time registration by going to the URL provided in this email and following the first-time sign-on steps in the attached My Co-op End-User Guide.

Here's a quick overview of what you'll need to do:

- **Access My Co-op.** Go to the following URL to log in, using your e-mail address as the username:

  https://sso.my.coop.org/mycoop

  Please note: *The password will be supplied in a separate e-mail.*

- **Create your password.** An essential part of the registration process is creating your own password.

- **Set up multifactor authentication (MFA).** You will be prompted to set up your device to send a one-time use authentication code for multifactor authentication when you use My Co-op.

  As mentioned in the end-user guide, do not use the phone pairing option for multifactor authentication.

- **After registering in My Co-op, you can sign on to My Co-op and access all the Co-op applications.**

  For some applications, you will need to enter your username and password for only the *first* time you access the app. On subsequent sign-ons, the portal remembers you and auto-fills the details in the sign-in screen (also referred to as "password replay").

Thank you!

First-time sign-on overview

When users arrive to the My Co-op main page for the first time, the process typically takes minutes to complete. For detailed instructions for users, see the My Co-op End-User Guide. The following is a summary of the process.

Sign on and set up multifactor authentication (MFA)

Multifactor authentication setup is part of the initial sign-on process that users are guided through.

> **Important**
> Encourage users to read the My Co-op End-User Guide or the My Co-op End-User Quick Reference Guide before completing the sign-on process the first time.

1. **Open My Co-op.** Use the link https://sso.my.coop.org/mycoop to launch My Co-op.
2. **Enter credentials.** The system prompts the user for a valid username and password.
   - **Username** is the user's work email address.
   - **Initial password** is provided by the My Co-op admin at your credit union. Passwords are valid for five days.
3. **Reset initial password.** After users enter their username and initial password to sign on, and follows the steps for multifactor authentication, the system prompts users to replace the initial password with a new one of their choice. The new password is valid for up to 90 days. The system will prompt users at sign on to reset their password five days prior to the password's expiration.

   Password requirements

   - At least 8 characters
   - At least 1 special character
   - At least 1 number
   - At least 1 lowercase letter
   - At least 1 uppercase letter
   - Password not used previously in the last year
   - No more than 2 duplicate characters

About multifactor authentication (MFA)

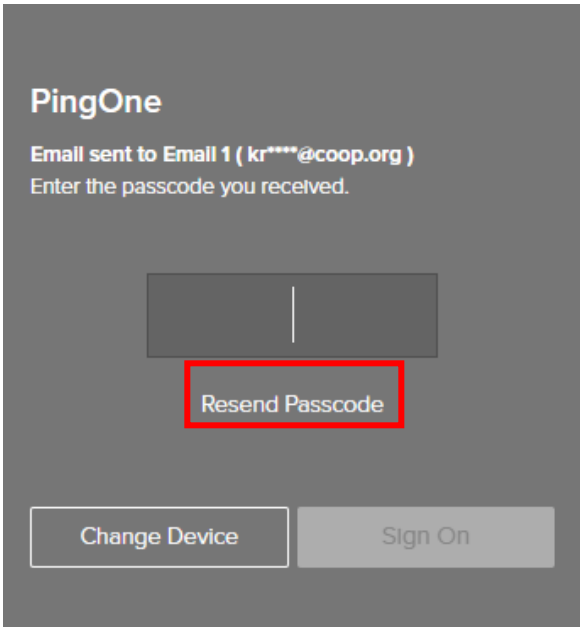
As a user proceeds through their initial sign-on, they will be prompted to set up a device for MFA.

> **Warning**
> Registering only one device puts a user at risk. Users should set up at least two devices to receive passcodes (one acting as the primary and the other as a backup). If the primary device becomes unavailable, account reset is the only way to designate a different device to receive MFA passcodes.

Users will need a new authorization passcode each time they sign on to My Co-op, as well as when they change their own password, or change information about an MFA device. MFA passcodes are sent to the primary device on record, which users designate during the registration process. Ask your staff to register at least two devices so that a backup device exists should the primary device become unavailable (for example, the user leaves their cell phone at home, cell phone battery runs down, email goes down, etc.).

Instructions for adding additional devices are in the My Co-op End-User Guide.

MFA passcodes expire if you do not enter the passcode within a limited period (30 minutes). If a passcode does not arrive before it expires, click **Resend Passcode** on the Authentication screen.



Launch applications

Important notes about browsers

Some applications work only in specific browsers.

The following applications are browser-specific:
- **BlueZone** – Can be accessed only in IE.
- **Extranet** – Can be accessed only in IE.
- **StarView** (inside Desktop Director) – Can be accessed only in Chrome and Edge.

These applications work only in the browsers specified in this section, whether or not My Co-op is used to access them. If the specified browser is not used, some of these apps may not work at all, and some may lose functionality. If a login screen appears for these apps in another browser, copy and paste the URL into the specified browser to access them. For all applications not specified in this note, you can use any browser.

Additional Note

My Co-op can be used in *multiple* browsers at the same time.
You do not need to log out of My Co-op and close one browser in order to open it in another browser. Typically a user prefers a favorite browser they are most comfortable with. If you open another session of My Co-op in a different browser (for example, you're working in Chrome but want to also open My Co-op in IE), you don't need to log out of My Co-op in the first browser (Chrome) or even close that browser. You can just open another browser and sign on to My Co-op there as well.

Launch an application in My Co-op

Note
The My Co-op main screen stays open when you launch an application. The application opens in a separate window.

On the My Co-op main page, perform the following for an application you have existing credentials to use:

- **Select the application.**
  - **The application opens in a new window.**
    (Some applications allow you to sign on without entering your credentials. These applications are connected via technology called SAML.)

    -OR-

  - **If prompted by the application, enter your username and password for that app.**
    (If a pop-up from your browser offers to save your password for the app, select **Never**. This is the best practice for your information security.)

  You can begin working in the app.

Manage My Co-op users

Your My Co-op admins will use the Delegated Admin Console application within My Co-op to create and manage your users. Refer to instructions in the My Co-op Delegated Admin Console Guide for creating and deleting users, assigning groups to users, changing the group a user is assigned to, and resetting passwords. A shorter My Co-op Delegated Admin Console Quick Reference Guide is also available for admins.

Create users

Your admins will create users for your financial institution by using the Delegated Admin Console. They can also create other admins.

User group assignments

My Co-op offers several user groups, each enabling access to a different set of applications. You can tailor the user group assignments based on the function of your staff.

This guide contains an Application User Group Matrix, which is a table that lists all the user groups and the applications assigned to each group. Admins at your organization will use this table as they assign users to groups. This table is also in the My Co-op Delegated Admin Console Guide.

Applications display on the My Co-op main page based on user group assignment (and not based on the individual user). Consequently, icons may appear for an application that a user does not have the credentials to use. A user can only access applications they have existing credentials to use.

> **Note**
> During setup of My Co-op and if applicable for the financial institution and users, users should be asked to identify which is their primary FIS ID. That ID is connected directly to the FIS applications through the icons on their dashboard. They can access FIS applications, like Data Navigator, Cardholder Maintenance, etc. by clicking on any of those icons. Or they can go to the green Desktop Director icon and navigate to the application they want to use.
>
> To use their secondary FIS ID, the credit union's My Co-op admin should assign the user to the DesktopDirectorSecondary access group.* After this access group is assigned, users should select the purple Desktop Director icon and navigate to the applications through the menu. The secondary FIS ID will not allow access to any applications assigned under the primary ID.
>
> **The DesktopDirectorSecondary access group does not appear in the Application user group matrix because it is only a subset of My Co-op.*

Application user group matrix

The table in this section provides a list of user groups and the applications assigned to each user group. Use this list as you determine which groups to assign to users.

Applications with an asterisk (*) are SAML-enabled and launch without the need for credentials when a user signs in to My Co-op. Co-op is working to transition all applications to open this way, without the need for credentials.

Important!
The first Power Admin at your organization will be assigned to the Delegated Admin Console group. **If you create additional Power Admins, be sure to assign them to this group** so they can access the Delegated Admin Console after they sign on to My Co-op.

Application user group matrix

	Legacy Co-op Groups								Legacy TMG Groups			Both Legacy Co-op & TMG Groups			
Application Name	**Front Office** (Front Line)	**Back Office** (Operations)	**Supervisor/ Admin**	**ATM**	**Marketing**	**Miscellaneous** (ecom, prepaid gift, cmc)	**Shared Branching**	**Network Access Only**	**Springboard**	**Star Station**	**Legacy TMG**	**Delegated Admin Console**	**Insights Center**	**Insights Center Admin**	**Developer Portal**
Arcot											x				
Atira CardWiz											x				
ATM Visual Control	x	x	x	x											
Augeo (Rewards) Admin			x		x										
BackOffice			x			x									
Binload			x	x				x							
Blue Zone											x				
Cardholder Maintenance*	x	x	x												
CardPro Connect*		x	x												
CardWiz Gift Cards			x			x									
CIMple Access Admin			x	x			x								
CIMple Teller			x				x								

	Legacy Co-op Groups								Legacy TMG Groups			Both Legacy Co-op & TMG Groups			
Application Name	**Front Office** (Front Line)	**Back Office** (Operations)	**Supervisor/ Admin**	**ATM**	**Marketing**	**Miscellaneous** (ecom, prepaid gift, cmc)	**Shared Branching**	**Network Access Only**	**Springboard**	**Star Station**	**Legacy TMG**	**Delegated Admin Console**	**Insights Center**	**Insights Center Admin**	**Developer Portal**
CIMple Teller Admin			x				x								
CST, customer support tool			x			x									
Dashboard											x				
Data Navigator*	x	x	x	x			x	x							
Delegated Admin												x			
Desktop Director (eACCESS)*	x	x	x	x			x								
Desktop Director Secondary			x												
Developer Portal															x
Dispatch Manager Self Service (DMSS)*			x	x											
Dispatch Manager Web Workstation (DMWW)*			x	x											
Expanded Co-op Springboard			x						x		x				
Extranet	x	x	x	x			x	x							
ezAdmin			x	x		x	x	x							
File Transfer*		x	x				x	x							
Hot Card*	x	x	x												
InfoLink			x			x									
Insights Center													x		
Insights Center Admin													x	x	
LendingTools											x				
Loanliner			x			x									

	Legacy Co-op Groups								Legacy TMG Groups			Both Legacy Co-op & TMG Groups			
Application Name	**Front Office** (Front Line)	**Back Office** (Operations)	**Supervisor/ Admin**	**ATM**	**Marketing**	**Miscellaneous** (ecom, prepaid gift, cmc)	**Shared Branching**	**Network Access Only**	**Springboard**	**Star Station**	**Legacy TMG**	**Delegated Admin Console**	**Insights Center**	**Insights Center Admin**	**Developer Portal**
Mail Express											x				
Marketing Portal					x						x				
mConsole Connex	x	x	x												
mConsole Omaha											x				
MemberView			x			x									
MoveIT		x	x	x	x										
PaymentsOne			x	x											
Revelation		x	x	x	x										
Secure Suite (RSA)		x	x												
Secure Suite (RSA) Admin		x	x												
Secure Transfer Folder		x	x												
SmartLook											x				
SpendTrend											x				
Springboard*			x						x		x				
Star Station										x	x				
Xnet											x				

Initial password

After you set up your users, they will need to log in with the temporary password you provide them and create a new one. Login instructions are in the My Co-op End-User Guide.

> **Reminder**
> For security purposes, provide the username and password to each user individually.

Resources and contact information

Resources

Additional resources can be found in the Knowledge Center application within My Co-op.

Contact information

If you have any questions or problems, contact:

Email: clientservicecenter@coop.org

Phone: Client Care at 800-782-9042, option 5.

Common user questions

Devices

Are smartphones and other touch devices supported?

Users can use smartphones (as your organization permits), tablets, and other mobile devices to receive MFA authentication passcodes. However, these devices are not supported for My Co-op use.

Why should I add a backup device to receive passcodes?

Adding an extra device will allow you to have multiple verification options in case you are unable to access a certain device at any time. For instructions on adding a multifactor authentication (MFA) device, see the My Co-op End-User Guide.

My Co-op applications

Can users add, delete, or rearrange icons?

No. A fixed set of applications appears in alphabetical order on the My Co-op main page.
My Co-op uses machine learning to dynamically place each user's most frequently accessed application in the top section of the user's page. If your organization does not have rights to use one or more of the applications that are included in the grouping, users cannot access the application(s).

Why do applications appear that our staff does not use?

My Co-op offers various user group options. Each user group option has a fixed set of applications that appear on the My Co-op main page. Your organization and/or an employee may not have rights to use all of the applications that are included in the user group. Although staff will see all application icons, only credentialed users can access and use applications.

Why do some users see two Desktop Director icons, and which should they use?

Most users see only one icon, the green Desktop Director icon. However, Data Navigator requires different FIS IDs for signature and PIN chargebacks if performed by the same user, so some of your users will have two FIS IDs. These users will see two Desktop Director icons: the green icon for primary FIS ID access, and the purple icon for secondary FIS ID access. For additional instructions on how to assign attributes, see *User attributes* in the My Co-op Delegated Admin Console Guide.

Why can't I access some applications in certain browsers?

Some applications work *only in a certain browser,* even when accessed from My Co-op. So be sure to use the browser that those applications work in when you're using My Co-op. For example, when using BlueZone and the Extranet, use My Co-op in Internet Explorer. When using StarView (inside Desktop Director), use Chrome or Edge. For more information, see *Launch applications*.

My Co-op password

What should users do if they forget their My Co-op password?

On the My Co-op login screen, users should contact their financial institution's My Co-op admin.

Password requirements

- At least 8 characters
- At least 1 special character
- At least 1 number
- At least 1 lowercase letter
- At least 1 uppercase letter
- Password not used previously in the last year
- No more than 2 duplicate characters

What do users do if an error message displays after they reset their password?

After submitting the new password request, if an error message displays, users should:

1. Sign on again (use the link https://sso.my.coop.org/mycoop); and
2. Enter their username and new password.

Passcodes (authentication tokens)

Why does an authorization screen time out sometimes before a passcode arrives?

- **Codes sent to office phone.** Users who choose to receive MFA passcodes via a phone should answer the call to access the first verification code. If the call goes to voicemail, users may not be able to retrieve the message before the passcode times out. If the passcode times out, the user should click **Re-select Authentication Preference** (during first-time sign-on) or **Resend Passcode** (during subsequent sign-ons).
- **Codes sent to email.** For users who set their email address as the authentication device, Spam filters can delay the arrival of passcodes and in some cases, prevent them from arriving at all. Check your local spam filter and add the domain "@pingidentity.com" to your safe senders list. Users can request another passcode by selecting **Re-select Authentication Preference** (during first-time sign-on) or **Resend Passcode** (during subsequent sign-ons).

What if users leave their cell phone at home or the battery runs out during the workday?

Users unable to access their primary device can receive passcodes on a secondary device by selecting **Change Device** on the Authentication screen. The change device option works *only if a user has established at least two devices*. If only one device is on record, users will need to contact Co-op to reset their account. Resetting will require users to re-register. Encourage your staff to set up at least two devices to receive passcodes, one that acts as a primary device and one that acts as a backup.

Passwords for applications

Will application passwords expire?

Passwords to the individual applications are handled within the applications just as they are today with an additional step required within My Co-op. If a user needs to reset or wants to change a password in a particular application, they must change the password in the application.

Why are some users unable to access all applications that appear on the My Co-op main page?

Not all users will have access to all applications that display on their My Co-op main page. Applications appear based on user group assignment (and not based on the individual user). Consequently, icons may appear for an application that a user does not have the credentials to use. A user can only access applications they have existing credentials to use.

Sign on

Why do some users get an error message or see a blank page when using a favorite to sign on?

After a user enters the My Co-op URL to the browser bar, the page redirects to a different URL. Users who receive an error message instead of the sign-on page may have inadvertently saved a wrong URL to their favorites. The correct URL is: **https://sso.my.coop.org/mycoop**

After users complete the registration process, how do they sign on again?

Users can sign on to My Co-op by entering the URL (https://sso.my.coop.org/mycoop) into the browser or choosing the link from favorites (assuming it is saved with an accurate URL). They will experience multifactor authentication every time they sign on.

> **Tip**
> Users should save the following My Co-op URL as a favorite:
> https://sso.my.coop.org/mycoop

Sign off

How should I tell staff to sign off of My Co-op?

Users can sign off of My Co-op by going to the Profile icon on and clicking Sign Off.

Timeouts

Is there a timeout for My Co-op?

The timeout is 12 hours for My Co-op. This is a hard session timeout and not an inactivity timeout.

Is there a timeout for applications?

Each application follows its existing time-out schedule. If an application times out, users should close the application window, go back to My Co-op, and click on the application to sign on again.

Application Glossary

Arcot
Used by credit unions to manage member passwords for Verified by Visa and Mastercard SecureCode. Credit unions can also pull reports on those programs from the site.

Atira CardWiz
Web-based credit union admin site for the Atira Reloadable, Prepaid and Gift Card Program.

ATM Visual Control
Includes three modules: Content Manager, for the creation of customized ATM screens; Electronic Journal, to remotely pull EJ files from ATMs; Remote Manager, to remotely distribute software to the ATM.

Augeo (Rewards) Admin
Tool used by credit unions to manage their Rewards program offered by Augeo.

BackOffice
Reporting and support ticketing.

Binload
Other EFT processors and credit unions who drive their own ATMs download the Co-op BIN File each week so they know which BINs belong to the Co-op Network. By knowing that, they'll know which transactions are surcharge-free at their ATMs.

Blue Zone
Applications that provide real-time access to card account information on the First Data system. This system is used to perform many of the services credit union staff perform each day: create new accounts, control card program parameters, and more.

Cardholder Maintenance
A web-based tool that credit unions can use to add, edit, or delete cardholder records from the Co-op database in real-time.

CardPro Connect
A web-based application for credit unions with CardPro to view and track their plastic collateral, inventory and card issuance from transmission through production and shipment.

CardWiz Gift Cards
A web-based credit union admin site for Card in a Box gift card program.

CIMple Access Admin
Provides tools for user management and reporting on Shared Branch express transactions.

CIMple Teller
A solution for credit unions whose core processor doesn’t support a shared branching interface. It enables those credit unions to service guest members in the shared branching network.

CIMple Teller Admin
Application that allows credit unions using CIMple Teller to manage user access, login credentials, and passwords.

CST, customer support tool
Support tool for payment issues for ecom.

Dashboard
A client-facing website that provides easy access to Co-op processing and solution information. Information contained within the dashboard includes the following: trending industry topics, consumable blog content, details on Co-op solutions, interactive products page, training materials and manuals, product enhancements and announcements, insider stories, a personalized client dashboard and much more.

Data Navigator
An application used internally and by credit union staff to research transactions in real-time (ATM, PIN POS, Signature, Shared Branching), perform ATM adjustments, review ATM statuses and cash positions, and manage disputes and chargebacks.

Delegated Admin Console
My Co-op administrative tool.

Desktop Director (eACCESS)
Main portal access for FIS tools (eACCESS).

Developer Portal
An enterprise-level API management system that houses all Co-op APIs in one library, organized in a way that makes it easy to browse and find ways to integrate with Co-op. In addition to providing access to APIs and documentation, the platform also supports developers with environments for testing and mocking services.

Dispatch Manager Self Service (DMSS)
A web browser interface that allows users to change, add, or delete their existing ATM contact information. The user can view or request Dispatch Manager changes at any time.

Dispatch Manager Web Workstation (DMWW)
Enables a user to remotely monitor their ATM fleet. Users can access open tickets, ticket history, as well as any call logs associated with the tickets.

Extranet
Site for credit unions to receive Co-op notices, Notice of Action information for disputes, risk reports, fraud forum access, update contact and ATM information. Credit unions are also able to access Co-op Concierge to load travel notes, upload dispute forms for the Dispute Resolution Center and view their invoices.

ezAdmin
Ensenta's web-based product used by credit union staff for daily proofing and validation of deposited items. Admin level functions are also available.

File Transfer
Allows a credit union to download its legacy Co-op reports, as well as upload cardholder data files to the Co-op switch.

Hot Card
A web-based tool that credit unions can use to add blocked card information to the warning bulletins at Visa and Mastercard. They can also select certain area of the world in which the cards should be blocked.

InfoLink
A website for Co-op Member Center clients to pull reports related to their call center activity.

Insights Center
This web-based platform is Co-op's custom-built, data analytics warehouse and dashboard tool that simplifies complex portfolio information, providing credit unions with the technology to analyze cardholder and ATM data, understand the health of their portfolio, and make decisions to grow their portfolio.

Lending Tools
This application is used to upload ACH files to the FED.

Loanliner
A CUNA Mutual application that is used as a loan application entry tool.

Mail Express
Mail Express is an FTP application from legacy TMG that enabled users to send files that contained sensitive cardholder information.

Marketing Portal
Web-based access for credit unions to view, use and purchase marketing collateral on Co-op products and services.

mConsole Connex
Web-based access for credit unions to assist members with CardNav Control and Alert issues on Connex platform. This site is also used to pull CardNav reports.

mConsole Omaha
Web-based access for credit unions to assist members with CardNav Control and Alert issues on Omaha platform. This site is also used to pull CardNav reports.

MemberView
CMC Access into Symitar's Member Service module to assist members with more detailed core information.

MoveIT
Provides Connex clients with access to reports for their Automated Consumer Notifications product.

PaymentsOne
Online servicing application that provides access to multiple back-end applications for processing different payments types. Available functions include Managing Currency Conversion rate, Remote Balancing (TTF), and Issuers Clearinghouse Service.

Revelation
Web-based data analytics tool used internally and by credit unions. Transactions include ATM, PIN POS, Signature, FSC, IHC and Shared Branch Express and Shared Branching information. Other functions include campaign management, fraud forensics which includes Compromise Card Manager and Breached Merchant, as well as, ATM Profitability.

Secure Suite (RSA)
Used by credit unions to manage their members' passwords for Verified by Visa and Mastercard SecureCode. Credit unions can also pull reports on those programs from the site.

Secure Suite (RSA) Admin
An application used by credit unions to manage user IDs, login credentials, and passwords for their staff that access the Secure Suite.

Secure Transfer Folder
Enables credit unions to securely share card and transaction information files with Co-op staff that satisfies PCI requirements. This is used during certification, testing, and implementation tasks.

SmartLook
This web-based application is Co-op's custom-built, data analytics warehouse and dashboard tool for First Data Credit and Debit issuers. The SmartLook platform simplifies complex portfolio information, giving Co-op staff and clients the technology to analyze cardholder data to create marketing campaigns that deliver the right offer at the right time to the right cardholders and provide for better overall portfolio management. Dashboards include Product P&L information, New Account Acquisition, TRIP Analysis, Month-On-Books Reporting, Merchant Analysis, Credit Score "bands", Rewards Program analytics, and more.

SpendTrend
A web-based application that allows financial institutions to access standard and customized reports to analyze fraud trends. SpendTrend enables clients to identify immediately fraud trends affecting their card portfolio. It takes the information gathered during suspicious transactions and pools it into a consortium file.

Springboard
An application that offers real-time access to card account information and reports for credit unions processing on the Optis platform. The web-based system automates many of the services credit union staff perform each day: create new accounts, control card program parameters, manage plastic inventory, and more.

Springboard Expanded / Expanded CO-OP Springboard
A back-office platform designed to streamline member servicing and program management for credit and debit programs into a single application. This unified, web-based platform delivers secure access to cardholder account information, real-time access to transaction details, and reporting on Connex and Optis platforms. Additional program management capabilities exist for clients on Optis platform; additional functionality for Connex will be added.

STAR Station
A web-based tool used to research transactions on the Wilmington platform. Also used to process adjustments and disputes that routed over the STAR Network, and to report transactions as fraudulent.

StarView
Located within Desktop Director. A repository for reports. If credit unions need to access an old report that they did not save internally, they can go into StarView and retrieve a copy.

Xnet
A website that provides reporting for the FIS prepaid card programs.

Also see the General Glossary beginning on the next page.

General Glossary

credentials
The username and password a user must enter for an application.

Identity as a Service (IDaaS)
An emerging solution category for managing and simplifying access to applications. IDaaS will enable clients to meet the PCI 3.2 requirement in a single pass from a central location, rather than app by app.

multifactor authentication (MFA)
Multifactor authentication (MFA), a requirement for 2018 PCI 3.2, is an important piece of My Co-op, ensuring that your data—and your members'—is safe. Users will receive a one-time token (called a passcode) to authenticate each time they log in to My Co-op. This token can be sent via email or via SMS text to a user's phone. The user chooses these options when registering for My Co-op.

My Co-op
My Co-op is a new single launching point for all things Co-op. It simplifies the way you and your staff log in to Co-op applications, while using the latest security technology, including IDaaS, SAML, and multifactor authentication (MFA).

My Co-op main page
The landing page of all Co-op applications available to your organization.

passcode
The one-time authorization code generated when you first log in. The code is delivered to your designated device (email, SMS text message, or desktop phone). Enter the code in the authorization screen. The code is valid for:

- Up to 30 minutes when you sign on to the My Co-op portal.
- For up to 4 minutes when you add a new device and are required to validate that device.

PingOne
PingOne powers My Co-op. A cloud-based identity as a service (IDaaS) framework for secure identity access management, providing users secure, simplified access to My Co-op cloud applications.

Security Access Markup Language (SAML)
A programming language that allows a user to sign on once for affiliated but separate websites. It provides a single point of authentication as a secure identity provider. User credentials will never leave the firewall boundary. This eliminates the need for storing or synchronizing credentials, reducing the potential for data to be breached or stolen. It means that there is no more password expiration by application. Another advantage is that users will not have to enter individual credentials per application upon first visit to My Co-op. For more information, click:
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

SAML-enabled App
Applications, such as Springboard and FIS, that launch without a need to sign on with a username and password, even on the first visit to the My Co-op portal.